

**UNIVERSIDAD AUTÓNOMA “GABRIEL RENE MORENO”  
FACULTAD DE INGENIERÍA EN CIENCIAS DE LA  
COMPUTACIÓN Y TELECOMUNICACIONES**

**“UAGRM SCHOOL OF ENGINEERING”**



**MAESTRÍA EN AUDITORIA Y SEGURIDAD INFORMÁTICA  
“MODELO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO  
BASADO EN LA NORMA ISO 22301 PARA EL GRUPO  
EMPRESARIAL DE INVERSIONES NACIONAL VIDA S.A.”**

TRABAJO FINAL DE GRADO BAJO LA MODALIDAD DE TESIS PARA OPTAR  
AL TÍTULO DE MAESTRO EN CIENCIAS

**AUTOR:**  
Ing. Alexis Andrés García Sandoval

**DIRECTOR DE TRABAJO FINAL DE GRADO:**  
Alida Nersa Paneque Ginarte Ph.D.

Santa Cruz, Bolivia  
Marzo, 2019

## **Cesión de derechos**

Declaro bajo juramento que el trabajo aquí descrito, titulado “**Modelo de Gestión de Continuidad del Negocio basado en la norma ISO 22301 para el Grupo Empresarial de Inversiones Nacional Vida S.A.**” es de propia autoría; que no ha sido previamente presentado para ningún grado de calificación profesional; y, que se ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaro que cedo mi derecho de propiedad Intelectual correspondiente a este trabajo, a la UAGRM Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

**Ing. Alexis Andrés García Sandoval**

## **Dedicatoria**

A mis padres por enseñarme a vencer los obstáculos de la vida con esfuerzo y perseverancia.

A la memoria de mi hermano Juan Alejandro a quien recordaré por siempre.

A mi amada esposa y amiga Carola, por acompañarme y ayudarme a formar un proyecto de vida.

A mis hijos Melissa, Eduardo y Andrés por el tiempo que estuve ausente mientras trabajaba y elaboraba el presente trabajo, el cual espero los pueda inspirar para formarse profesionalmente.

## Agradecimiento

A Dios por ser mi fuente de inspiración y darme cada día una nueva oportunidad.

A la escuela de Ingeniería de la Universidad Autónoma Gabriel Rene Moreno por abrirme sus puertas y darme la oportunidad de realizar mi maestría.

Al Grupo Empresarial de Inversiones Nacional Vida por facilitarme un entorno donde logré contribuir y realizar el proyecto.

A todos mis colegas y amigos que me han ayudado aportando consejos sobre el camino apropiado a seguir en mi desarrollo profesional.

A la profesora Alida Paneque Ginarte PhD. directora de tesis, por dedicarme su tiempo y compartir sus conocimientos en el área de metodología de la investigación para realizar la presente investigación.

Al personal del área de IT de TECorp S.A., por ayudarme en la ejecución de la investigación, gracias por su compromiso y aporte para la culminación del proyecto.

## **RESUMEN**

La presente investigación responde al problema científico ¿Cómo mejorar el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica afectado por los nuevos Riesgos y Amenazas de Ciberseguridad que impactan las Tecnologías de Información y Comunicaciones del Grupo Empresarial de Inversiones Nacional Vida S.A.? y define como Objetivo General: Diseñar un Modelo de Gestión de Continuidad basado en la norma ISO 22301 para mejorar el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica en el contexto mencionado.

Se sistematiza los planteamientos de diferentes autores y a través del método de Análisis Documental, se caracterizan los riesgos, amenazas y ciberseguridad, abordando las tendencias de las amenazas de ciberseguridad. Así también, las definiciones de tiempo objetivo de recuperación y sus tendencias.

Mediante la aplicación de instrumentos de investigación: entrevista y encuesta se evalúan los procesos de misión crítica en el contexto investigado para identificar el tiempo Objetivo de Recuperación. Se identifica como problema crítico “Los tiempos objetivos de recuperación de incidentes no responden a la meta definida por la alta dirección”.

Con un enfoque de sistemas, se estructura del Modelo de Gestión de Continuidad del Negocio. Se desarrollan, a partir de la aplicación de la norma ISO 22301, las diferentes cláusulas y sus objetivos: Contexto de la Organización, Liderazgo, Planificación, Recursos y Operación.

Finalmente, se valida metodológicamente y estadísticamente la mejora en el Tiempo objetivo de recuperación después de aplicar el Modelo de Gestión de Continuidad de Negocio propuesto, con la aplicación de la prueba Chi Cuadrada de Pearson.

## **ABSTRACT**

*The purpose of this research work is to answer the question to the scientific problem: "How to improve the Recovery Time of the Critical Mission Services affected by the new Cybersecurity Risks and Threats that impact the Information and Communications Technologies of the Nacional Vida S.A. Investment Group? In addition, establish a General Objective, which will outline a Continuity Management Model based on the ISO 22301 standard to improve the Recovery Time of the Critical Mission Services in the aforementioned context.*

*The explanations of different authors are systematized through the method of Documentary Analysis, characterizing the risks of cybersecurity threats, as well as the definitions of objective time of recovery and its trends.*

*Through the application of research tools such as interviews and surveys, the critical mission processes in the research are evaluated to identify the Recovery Time Objectives. A critical problem is identified if the objective times of recovery of incidents do not respond to the goal defined by senior management".*

*The Business Continuity Management Model is structured along a systems approach. Based on the application of the ISO 22301 standard, the different clauses and their objectives are developed: Context of the Organization, Leadership, Planning, Resources and Operation. Finally, the improvement in the Target Recovery Time is validated methodologically and statistically after applying the proposed Business Continuity Management Model, with the application of Pearson's Chi Square test.*

## ÍNDICE GENERAL

INTRODUCCIÓN.....	1
1. Antecedentes del Problema .....	3
2. Planteamiento del problema .....	5
2.1 Objeto de Estudio .....	5
2.2 Campo de Acción .....	5
3. Objetivos.....	5
3.1 Objetivo General.....	5
3.2 Objetivos específicos .....	5
4. Idea Científica a Defender.....	6
5. Justificación .....	6
6. Delimitación de la investigación .....	8
7. Diseño Metodológico .....	9
7.1. Tipo de Investigación .....	9
7.2. Métodos de Investigación .....	9
7.3. Técnicas e Instrumentos de Investigación .....	10
7.4. Población y Muestra .....	11
CAPÍTULO I. MARCO TEÓRICO Y CONCEPTUAL.....	13
1.1 Riesgos y Amenazas de Ciberseguridad.....	13
1.1.1. Riesgo .....	13
1.1.2. Amenazas.....	15
1.1.3. Ciberseguridad.....	18
1.1.4. Tendencias de las amenazas de Ciberseguridad .....	21
1.2 Tiempo Objetivo de Recuperación .....	25
1.2.1. Definiciones Principales.....	25
1.2.2. Tendencias.....	28
1.3 Norma ISO 22301.....	28
1.3.1. Origen.....	28
1.3.2. Características Principales .....	31

1.3.3. Tendencias de la Gestión de Continuidad .....	33
1.4 Norma ISO 31000.....	36
1.4.1. Evolución .....	37
1.4.3. Características Principales .....	38
1.4.4. Tendencias de la Gestión de Riesgos de Ciberseguridad.....	41
1.5 Gestión de Continuidad del Negocio (BCM) .....	43
1.6. Análisis de Riesgo .....	44
1.7. Análisis de Impacto (BIA: <i>Business Impact Analysis</i> ).....	44
1.8. Estrategias de Recuperación.....	45
1.9. Plan de Continuidad del Negocio (BCP).....	46
CAPITULO II. DIAGNÓSTICO .....	48
2.1 Acercamiento al contexto que se investiga.....	48
2.1.1 Estructura organizacional de la empresa .....	49
2.2 Procedimiento para el Diagnóstico.....	49
2.2.1 Definición conceptual. ....	50
2.2.2 Definición operacional de las variables.....	51
2.2.3 Instrumentos de investigación .....	51
2.3 Análisis de los resultados de la aplicación de los instrumentos .....	52
2.3.1 Resultados de la aplicación del Cuestionario de Encuesta .....	52
2.3.2 Resultados de la aplicación del Cuestionario de Entrevista .....	59
2.3.3 Guia de Observación.....	61
2.4 Triangulación de los resultados de los instrumentos e identificación de los problemas	62
CAPÍTULO III. PROPUESTA .....	64
3.1 Estructura del Modelo de Gestión de Continuidad del Negocio .....	64
3.1.1 Por qué la ISO 22301.....	66
3.2 Contexto de la Organización (Cláusula 4).....	68
3.2.1 Descripción de la Organización.....	68
3.2.2 Necesidades y expectativas de las partes interesadas .....	75
3.2.3 Alcance del Modelo de Gestión de Continuidad del Negocio.....	79
3.3 Liderazgo (Cláusula 5) .....	82

3.3.1 Responsabilidades y Empoderamiento .....	82
3.4 Planificación (Cláusula 6) .....	90
3.4.1 Direccionar Riesgos, Oportunidades .....	90
3.4.2 Objetivos y planes para Alcanzarlos.....	91
3.5 Recursos (Cláusula 7).....	92
3.5.1 Competencia .....	93
3.5.2 Toma de conciencia .....	95
3.5.3 Comunicación .....	97
3.6 Operación (Cláusula 8) <i>Disaster Recovery Institute (DRI)</i> .....	104
3.6.1 P01 Planificación y Control Operacional .....	105
3.6.2 P02 Evaluación de Riesgos.....	119
3.6.3 P03 Análisis de Impacto al Negocio (BIA) .....	153
3.6.4 P04 Estrategias de Continuidad de Negocio.....	174
3.6.5 P06 Desarrollo e Implementación del Plan de Continuidad del Negocio (BCP) .	196
3.7 Validación metodológica y estadística del proceso pre-experimental.....	217
3.7.1 Soporte metodológico y estadístico .....	217
CONCLUSIONES.....	223
RECOMENDACIONES .....	224
REFERENCIA BIBLIOGRÁFICA.....	225
BIBLIOGRAFÍA .....	229
ANEXOS .....	232

## ÍNDICE DE CUADROS

<b>Cuadro No. 1.</b> Desglose del Tiempo de Inactividad.....	2
<b>Cuadro No. 2.</b> Ejemplos de Estrategia de la Gestión del Riesgo .....	15
<b>Cuadro No. 3.</b> Instrumentos de Investigación .....	51
<b>Cuadro No. 4.</b> Encuestados por Cargo .....	52
<b>Cuadro No. 5.</b> Encuestados por Edad.....	53
<b>Cuadro No. 6.</b> Encuestados por Antigüedad .....	54
<b>Cuadro No. 7.</b> Encuestados por Nivel de Estudio .....	54
<b>Cuadro No. 8.</b> Explicación del Modelo PHVA .....	65
<b>Cuadro No. 9.</b> Sistemas Informáticos.....	72
<b>Cuadro No. 10.</b> Fuentes de Información .....	74
<b>Cuadro No. 11.</b> Lineamiento estratégico .....	75
<b>Cuadro No. 12.</b> Dominios de Trabajo .....	80
<b>Cuadro No. 13.</b> Criterios de Seguridad .....	90
<b>Cuadro No. 14.</b> Identificación de Grupos de interés y partes interesadas .....	97
<b>Cuadro No. 15.</b> Matriz de Poder.....	98
<b>Cuadro No. 16.</b> Principales entregables del proyecto .....	108
<b>Cuadro No. 17.</b> Estimación Resumida de Tiempos.....	110
<b>Cuadro No. 18.</b> Nivel Sigma aplicado a la Estimación de Tiempo .....	111
<b>Cuadro No. 19.</b> Estimación Resumida de Costos.....	113
<b>Cuadro No. 20.</b> Nivel Sigma aplicado a la Estimación de Costos .....	113
<b>Cuadro No. 21.</b> Matriz de asignación de responsabilidades del proyecto BCM.....	116
<b>Cuadro No. 22.</b> Responsabilidades de Equipos en el proyecto BCM .....	116
<b>Cuadro No. 23.</b> Criterios de valoración de riesgo cualitativo .....	123
<b>Cuadro No. 24.</b> Activos de información catalogados.....	127
<b>Cuadro No. 25.</b> Valoración de dependencia de activos.....	129
<b>Cuadro No. 26.</b> Listado de amenazas sobre los activos de información .....	130
<b>Cuadro No. 27.</b> Identificación, Motivación y Beneficio del Atacante .....	134
<b>Cuadro No. 28.</b> Dominios de Amenazas .....	136

<b>Cuadro No. 29.</b> Valoración por Dominio de Amenaza .....	136
<b>Cuadro No. 30.</b> Tabla de valoración de impactos .....	137
<b>Cuadro No. 31.</b> Evaluación de impactos acumulados .....	138
<b>Cuadro No. 32.</b> Niveles de Madurez .....	139
<b>Cuadro No. 33.</b> Resumen de evaluación de Controles existentes .....	139
<b>Cuadro No. 34.</b> Mapa de Calor.....	143
<b>Cuadro No. 35.</b> Resumen de riesgos Totales.....	145
<b>Cuadro No. 36.</b> Nivel de Tolerancia al Riesgo (figura) .....	146
<b>Cuadro No. 37.</b> Calculo del riesgo Individual y del Riesgo tratado.....	150
<b>Cuadro No. 38.</b> Valor por periodo de impacto .....	156
<b>Cuadro No. 39.</b> Valor por tipo de Actividad .....	157
<b>Cuadro No. 40.</b> Nivel del Criticidad por Tipo de Impacto.....	157
<b>Cuadro No. 41.</b> Categorías de procesos .....	158
<b>Cuadro No. 42.</b> Análisis del proceso crítico de gestión Comercial.....	162
<b>Cuadro No. 43.</b> Análisis del proceso crítico de gestión de Cobranzas.....	163
<b>Cuadro No. 44.</b> Análisis del proceso crítico de Gestión de Siniestros .....	164
<b>Cuadro No. 45.</b> BIA- Denominación general del Activo de Información .....	165
<b>Cuadro No. 46.</b> BIA- Disponibilidad del Elemento de Servicio .....	165
<b>Cuadro No. 47.</b> BIA- Parámetros de Recuperación .....	166
<b>Cuadro No. 48.</b> BIA- Niveles de Impacto .....	166
<b>Cuadro No. 49.</b> BIA - Interrupción del Servicio .....	167
<b>Cuadro No. 50.</b> BIA - Línea de Tendencia (Siguientes 12 meses) .....	167
<b>Cuadro No. 51.</b> Objetivos de recuperación (MTD, WR, RTO, RPO).....	168
<b>Cuadro No. 52.</b> Análisis de Impacto sobre los activos de información (FOINLP)...	170
<b>Cuadro No. 53.</b> Análisis de Impacto en el Tiempo .....	172
<b>Cuadro No. 54.</b> División de los ambientes en función de los sitios. ....	180
<b>Cuadro No. 55.</b> Resumen de Propuestas financieras HPE, Dell, Lenovo .....	199
<b>Cuadro No. 56.</b> Valores percentiles para la distribución Chi Cuadrada.....	219
<b>Cuadro No. 57.</b> Calculo del $\chi^2$ de la variable dependiente.....	221

## ÍNDICE DE FIGURAS

<b>Figura No. 1.</b> Razones que causan inactividad o interrupción del Negocio .....	1
<b>Figura No. 2.</b> Realización del valor de un ciberataque.....	20
<b>Figura No. 3.</b> Relación entre un <i>RTO</i> y <i>RPO</i> .....	27
<b>Figura No. 4.</b> Evolución de los estándares en Continuidad del Negocio .....	30
<b>Figura No. 5.</b> Ciclo PDCA aplicado al proceso de Continuidad del Negocio.....	32
<b>Figura No. 6</b> Organigrama corporativo del holding de Inversiones .....	49
<b>Figura No. 7.</b> Muestra por Cargos .....	53
<b>Figura No. 8.</b> Encuestados por Género.....	53
<b>Figura No. 9.</b> Pregunta 1 – Encuesta .....	55
<b>Figura No. 10.</b> Pregunta 2 – Encuesta .....	55
<b>Figura No. 11.</b> Pregunta 3 – Encuesta .....	56
<b>Figura No. 12.</b> Pregunta 5 – Encuesta .....	56
<b>Figura No. 13.</b> Pregunta 6 – Encuesta .....	57
<b>Figura No. 14.</b> Pregunta 7 – Encuesta .....	57
<b>Figura No. 15.</b> Pregunta 8 – Encuesta .....	58
<b>Figura No. 16.</b> Pregunta 9 – Encuesta .....	58
<b>Figura No. 17.</b> Pregunta 10 – Encuesta .....	59
<b>Figura No. 18.</b> Jerarquización de los problemas .....	63
<b>Figura No. 19.</b> Grafico del Ciclo de Mejora Continua PHVA aplicado al SGCN .....	64
<b>Figura No. 20.</b> Estructura de Trabajo del ciclo Planificar .....	65
<b>Figura No. 21.</b> Estructura de Trabajo del ciclo Hacer-Verificar-Actuar .....	65
<b>Figura No. 22.</b> Ciclo de vida BCM y BCMS basado en el modelo PDCA .....	66
<b>Figura No. 23.</b> Mapa de procesos .....	71
<b>Figura No. 24.</b> Distribución de las oficinas y agencias regionales en Bolivia .....	74
<b>Figura No. 25.</b> Proceso para definir el alcance y límite del contexto de estudio. ....	79
<b>Figura No. 26.</b> Poder de influencia de los <i>stakeholders</i> .....	98
<b>Figura No. 27.</b> Estimación de Tiempo aplicado a la curva de Distribución Normal.	112
<b>Figura No. 28.</b> Cronograma de Trabajo.....	112

<b>Figura No. 29.</b> Estimación de Costos aplicado a la curva de Distribución Normal ..	114
<b>Figura No. 30.</b> Organigrama funcional del Proyecto BCM.....	115
<b>Figura No. 31.</b> Proceso de Gestión del Riesgo .....	120
<b>Figura No. 32.</b> Proceso de Evaluación del Riesgo .....	125
<b>Figura No. 33.</b> Secuencia de tareas en la etapa de Identificación de Riesgos .....	126
<b>Figura No. 34.</b> Diagrama de Colaboración y visibilidad con dependencias.....	129
<b>Figura No. 35.</b> Relación Amenaza, Vulnerabilidad, Activo e Impacto.....	137
<b>Figura No. 36.</b> Secuencia de la etapa de Análisis de Riesgos .....	140
<b>Figura No. 37.</b> Secuencia de la etapa de Valoración de Riesgos.....	144
<b>Figura No. 38.</b> Matriz de Riesgos totales .....	145
<b>Figura No. 39.</b> Matriz de Nivel de Riesgos .....	147
<b>Figura No. 40.</b> Secuencia de la etapa de Tratamiento de Riesgos .....	148
<b>Figura No. 41.</b> Secuencia de Actividades para el Tratamiento del Riesgo .....	149
<b>Figura No. 42.</b> Alcance de la técnica de Análisis de Impacto al Negocio.....	154
<b>Figura No. 43.</b> Secuencia de tareas de Análisis de Impacto al negocio (BIA).....	155
<b>Figura No. 44.</b> Matriz de calor por periodo de impacto .....	156
<b>Figura No. 45.</b> Matriz de calor por tipo de Actividad .....	157
<b>Figura No. 46.</b> Mapa de ubicación del Sitio Principal.....	159
<b>Figura No. 47.</b> Proceso para desarrollar la Estrategia de Continuidad.....	174
<b>Figura No. 48.</b> Escenario de una interrupción y recuperación del servicio.....	175
<b>Figura No. 49.</b> Mapa de ubicación del Sitio Alterno.....	176
<b>Figura No. 50.</b> Diagrama de Configuración del Sitio Templado (Warm Site).....	177
<b>Figura No. 51.</b> Diagrama de Configuración del Sitio Caliente ( <i>Hot Site</i> ).....	178
<b>Figura No. 52.</b> Diagrama de Configuración del Sitio Espejo ( <i>Mirror Site</i> ) .....	179
<b>Figura No. 53.</b> Diagrama de Red actual del Sitio Principal y Alterno .....	189
<b>Figura No. 54.</b> Diagrama de Red mejorado para el Sitio Principal y Alterno .....	191
<b>Figura No. 55.</b> Diagrama de Red mejorado del Sitio Principal y Regionales .....	192
<b>Figura No. 56.</b> Secuencia de tareas para la Adquisición de la Solución (BCP) .....	197
<b>Figura No. 57.</b> Cuadrante Mágico de Gartner para Servidores Modulares .....	200
<b>Figura No. 58.</b> Arquitectura de la solución HPE .....	203

<b>Figura No. 59.</b> Arquitectura de la solución Dell.....	206
<b>Figura No. 60.</b> Arquitectura de la Solución mixta HPE/Lenovo.....	208
<b>Figura No. 61.</b> Diagrama Solución de Servidores, Sitio Principal y Alterno.....	209
<b>Figura No. 62.</b> Transformación de los criterios de observación.....	222

## ÍNDICE DE ILUSTRACIONES

<b>Ilustración 1.</b> Configuración del <i>Backup</i> en el repositorio.....	211
<b>Ilustración 2.</b> Configuración de un trabajo semanal ( <i>JOB</i> ) de <i>backup</i> a disco .....	211
<b>Ilustración 3.</b> Configuración de un trabajo mensual ( <i>JOB</i> ) de <i>backup</i> a Cinta.....	212
<b>Ilustración 4.</b> Configuración de tareas semanales ( <i>Task</i> ) de <i>backup</i> de Servidores...	212
<b>Ilustración 5.</b> Distribución de Pool de servidores de <i>backup</i> .....	213
<b>Ilustración 6.</b> Pruebas de restauración de trabajos de <i>backup</i> .....	213

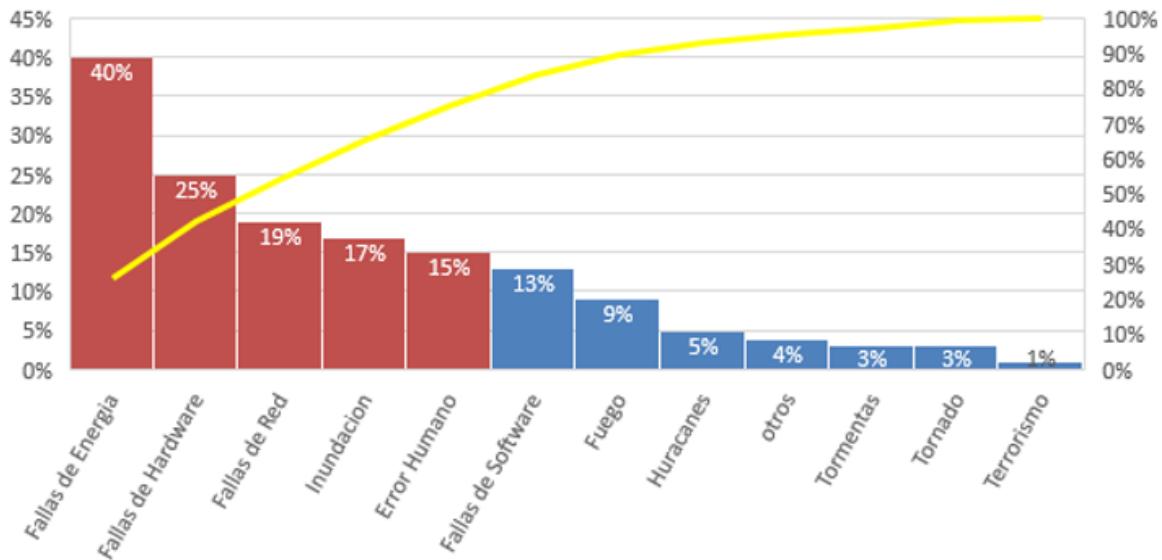
## ÍNDICE DE ANEXOS

<b>Anexo No.</b>	<b>1.</b>	Guía de análisis Documental .....	232
<b>Anexo No.</b>	<b>2.</b>	Guía de Observación.....	234
<b>Anexo No.</b>	<b>3.</b>	Cuestionario de Entrevistas a Directores y Gerentes Generales .....	236
<b>Anexo No.</b>	<b>4.</b>	Cuestionario de Encuestas a Gerentes de Línea y Ejecutivos.....	239
<b>Anexo No.</b>	<b>5.</b>	Operacionalización de las variables .....	244
<b>Anexo No.</b>	<b>6.</b>	Resultado de la Guía de Observación ( <i>Pre-Test</i> ).....	245
<b>Anexo No.</b>	<b>7.</b>	Triangulación de los instrumentos .....	246
<b>Anexo No.</b>	<b>8.</b>	Restricciones de la autoridad de supervisión ASFI .....	247
<b>Anexo No.</b>	<b>9.</b>	Restricciones de la autoridad de supervisión APS .....	248
<b>Anexo No.</b>	<b>10.</b>	Acta de Constitución del Proyecto ( <i>Project Charter</i> ).....	249
<b>Anexo No.</b>	<b>11.</b>	Lista de Actividades.....	251
<b>Anexo No.</b>	<b>12.</b>	Estimación de Tiempos .....	252
<b>Anexo No.</b>	<b>13.</b>	Estimación de Costos .....	253
<b>Anexo No.</b>	<b>14.</b>	Activos críticos identificados.....	256
<b>Anexo No.</b>	<b>15.</b>	Grado de Dependencia de Activos.....	258
<b>Anexo No.</b>	<b>16.</b>	Valoración de las amenazas sobre la plataforma tecnológica.....	261
<b>Anexo No.</b>	<b>17.</b>	Identificación de Vulnerabilidades .....	267
<b>Anexo No.</b>	<b>18.</b>	Valoración de las consecuencias (Impactos) .....	272
<b>Anexo No.</b>	<b>19.</b>	Subconjunto de Amenazas definido por MAGERIT .....	278
<b>Anexo No.</b>	<b>20.</b>	Evaluación de Controles Existentes.....	282
<b>Anexo No.</b>	<b>21.</b>	Matriz de Determinación de Riesgos Cualitativos.....	289
<b>Anexo No.</b>	<b>22.</b>	Formulario de Registro de Riesgos .....	293
<b>Anexo No.</b>	<b>23.</b>	Matriz de Riesgos con prioridad .....	295
<b>Anexo No.</b>	<b>24.</b>	Plan de Tratamiento de Riesgos.....	298
<b>Anexo No.</b>	<b>25.</b>	FRM de Análisis de Elementos de Servicios Críticos para el BIA...302	302
<b>Anexo No.</b>	<b>26.</b>	Cotización Enlace Inter-Sitio con Fibra Oscura 40Gbps/80Gbps ....305	305
<b>Anexo No.</b>	<b>27.</b>	Acta de entrega y aceptación del Proyecto BCM .....	306
<b>Anexo No.</b>	<b>28.</b>	Resultados de la Prueba del Plan de Continuidad del Negocio .....	308
<b>Anexo No.</b>	<b>29.</b>	Procesamiento estadístico con la corrección de Yates.....311	311

## INTRODUCCIÓN

El control de Seguridad sigue siendo un inconveniente para los responsables de Tecnología de la Información (TI) de la mayoría de las organizaciones del medio, el clásico ejemplo es cuando un virus o gusano informático infecta a los equipos de cómputo de la organización. Los profesionales de TI deben dejar todas sus actividades destinando esfuerzo para actualizar y escanear los equipos, y en algunos casos, reiniciar todo el proceso de instalación (preparar los servidores y reconfigurar servicios críticos desde el inicio), lo que causa una inversión importante de tiempo y la interrupción de los servicios críticos del negocio.

En la **Figura No. 1**, se presentan las principales razones que causan la inactividad o interrupción de la continuidad del Negocio. Ocupa los primeros lugares: Fallas de energía, de *hardware* y problemas en la red.



**Figura No. 1.** Razones que causan inactividad o interrupción del Negocio  
**Fuente:** (BCI, 2018)

En Bolivia muy pocas empresas han implementado un modelo de Gestión de Continuidad del Negocio (BCM) y en las empresas que sólo han elaborado un Plan de Continuidad del negocio (BCP) no existen evidencias de que lo hayan probado debidamente. Las nuevas regulaciones de la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS) para el Sector Seguros, han fijado requerimientos mínimos para la continuidad del negocio, desde la perspectiva de TI, habiendo tomado en cuenta los siguientes aspectos: a) La seguridad de la información y b) La gestión de continuidad del negocio.

Las nuevas amenazas deben permitir preparar una debida Gestión de continuidad del Negocio (BCM), tal que permita a los procesos críticos de la organización y al personal de TI, ser proactivos y tener las previsiones necesarias para accionar de forma eficiente cada vez que suceda el incidente.

En el **Cuadro No. 1**, se presentan la relación del tiempo, considerando la disponibilidad del negocio expresada en porcentaje.

**Cuadro No. 1.** Desglose del Tiempo de Inactividad

Uptime	Min	Hrs	Días
99.9994%	3.15	0.05	0.00
99.9990%	5.26	0.09	0.00
99.9900%	52.56	0.88	0.04
99.9500%	262.80	4.38	0.18
99.9000%	525.60	8.76	0.36
99.5000%	2,628.00	43.80	1.83
99.0000%	5,256.00	87.60	3.65
98.0000%	10,512.00	175.20	7.30
97.0000%	15,768.00	262.80	10.95
96.0000%	21,024.00	350.40	14.60
95.0000%	26,280.00	438.00	18.25

Fuente: (BCI, 2018)

Las empresas de clase mundial tienen un nivel de disponibilidad igual o superior al 99.9000%, es decir, pudieran sufrir tan solo una caída (menor a 8.76 hrs) al año, con una indisponibilidad medida menor a 4 horas.

## 1. Antecedentes del Problema

En muchas empresas de la ciudad de Santa Cruz de la Sierra, no es posible llevar a cabo un Procedimiento de Recuperación del Negocio de forma rápida (recuperar y restaurar los sistemas críticos), dentro de un Tiempo Objetivo de Recuperación (RTO) razonable sin tener impactos adversos para el negocio.

No se evidencian la toma de acciones posteriores a los incidentes, para determinar, por ejemplo: cómo ingresó el virus (*malware*), o cómo se suscitó el incidente (a través de alguna vulnerabilidad no identificada), y cómo identificar la naturaleza o la exposición del riesgo y si además fue posible minimizar el impacto del inconveniente al negocio.

A través de un análisis causa-efecto, se manifiesta que entre las principales causas que no permiten reaccionar al área de TI y Seguridad de manera oportuna ante un desastre, y recuperar los servicios críticos en un tiempo razonable:

- **Mano de Obra**
  - Insuficiente capacitación y preparación para la identificación de Riesgos y Amenazas de Ciberseguridad
  - Falta de preparación para la detección de vulnerabilidades en la infraestructura tecnológica
  - Escasa capacitación y preparación para la ejecución del Plan de Continuidad
  - Incapacidad de reacción ante eventos adversos de tecnología y seguridad

- Recursos Humanos insuficientes para poder segregar debidamente las funciones y garantizar la rendición de cuentas
- **Métodos**
  - Falta de adecuación e integración de las Políticas de Seguridad, Riesgos y Continuidad
  - Procesos y procedimientos de TI, Seguridad y Continuidad desactualizados
  - Incumplimiento de las políticas establecidas por la alta dirección
  - Ausencia de una estrategia de continuidad
  - Ausencia de procedimientos de preparación y respuesta de incidentes disruptivos
- **Entorno**
  - Desconocimiento de la naturaleza y complejidad del perfil de riesgo inherente de la organización
  - Falta de inclusión de las restricciones que afectan a la organización
  - Desconocimiento de los nuevos Riesgos y Amenazas de Ciberseguridad
  - Falta de definición del nivel de impacto que puede afectar al negocio (Pérdida Financiera, Reputación e Imagen, Normativo, Operativo y Legal).
- **Mediciones**
  - Tiempo Objetivo de Recuperación no definido
  - Tiempo de Caída Máxima Tolerable no definida
- **Infraestructura**
  - Desconocimiento de vulnerabilidades en la infraestructura tecnológica
  - Obsolescencia Tecnológica (equipamiento que cumplió su ciclo de vida)
  - Infraestructura no redundante para contingencias

- Bajo presupuesto para el área de Tecnología, Seguridad y Continuidad

## **2. Planteamiento del problema**

¿Cómo mejorar el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica afectado por los nuevos Riesgos y Amenazas de Ciberseguridad que impactan las Tecnologías de Información y Comunicaciones del Grupo Empresarial de Inversiones Nacional Vida S.A.?

### **2.1 Objeto de Estudio**

Riesgos y amenazas de Ciberseguridad.

### **2.2 Campo de Acción**

Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica del Grupo Empresarial de Inversiones Nacional Vida S.A.

## **3. Objetivos**

### **3.1 Objetivo General**

Diseñar un Modelo de Gestión de Continuidad basado en la norma ISO 22301 para mejorar el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica del Grupo Empresarial de Inversiones Nacional Vida S.A.

### **3.2 Objetivos específicos**

1. Caracterizar Amenazas y Vulnerabilidades de Ciberseguridad para tratar las fuentes de riesgo que impactan las Tecnologías de Información y Comunicaciones.
2. Evaluar los procesos de misión crítica para identificar los Objetivos de Tiempo de Recuperación en el Grupo empresarial de inversiones Nacional Vida.

3. Elaborar un Modelo de Gestión de Continuidad para Mejorar el Tiempo Objetivo de Recuperación de los servicios de misión crítica que afectan los objetivos del negocio.
4. Validar el Modelo de Gestión de Continuidad propuesto para medir si el tiempo objetivo de recuperación evidencia mejoras.

#### **4. Idea Científica a Defender**

Existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la aplicación de un Modelo de Gestión de Continuidad.

#### **5. Justificación**

##### **Relevancia Social**

El presente trabajo puede ser aplicado en cualquier empresa a través de los diseños elaborados como modelos y en especial permitirá a las empresas de diferentes sectores adoptar y aplicar metodologías de análisis de riesgo, análisis de impacto y de gestión de incidentes para fortalecer la continuidad del negocio.

Los problemas e incidentes de seguridad que se generan a diario en las empresas son una gran preocupación, participar en la resolución de los problemas derivados de la inseguridad el mismo permitirá aportar a las empresas del sector de seguros.

##### **Justificación Técnica**

En Bolivia, existen experiencias numerosas de incidentes de seguridad en empresas, que como resultado han afectado significativamente las finanzas y la imagen institucional, habiendo recibido multas y/o sanciones por el incumplimiento normativo.

Los componentes, modelos, diseños y actividades desarrolladas en el presente trabajo pueden ser aplicados por cualquier tipo de empresa, independiente del tamaño, complejidad, rubro o sector.

La Autoridad de Fiscalización y Control de Pensiones y Seguros (APS), así como, la Autoridad de Supervisión del Sistema Financiero (ASFI), han emitido nuevas circulares y, definido nuevos requisitos de auditoria al procesamiento electrónico de datos, por lo que las empresas reguladas deben adecuarse a las nuevas normativas y regulaciones.

### **Justificación Práctica**

Esta investigación se realiza porque existe la necesidad de:

- Diferenciar al Grupo empresarial de Inversiones Nacional Vida de la Competencia Mejorando la imagen y credibilidad ante sus clientes y proveedores, al adoptar e implementar un modelo de Gestión de Continuidad basado en la norma ISO 22301
- Identificar los principales riesgos en materia de Seguridad y Continuidad y establecer controles para gestionarlos o eliminarlos.
- Disminuir gastos relacionados con eventos de Riesgos e Incidentes de Seguridad de la información (Impacto al Negocio: Financiero, Imagen, Operativo, Legal, Procesos, Recursos Humanos)
- Proteger la reputación de la empresa y conseguir ventaja competitiva ante los competidores.
- Cumplir con las leyes, normas, requisitos y regulaciones pertinentes (APS, ASFI) reduciendo así la posibilidad de enfrentar multas y sanciones.

El proyecto subsanará estas deficiencias y permitirá a las empresas definir un grado razonable de seguridad tanto en la arquitectura de Seguridad y Continuidad del ambiente de Tecnología de la Información (TI) y en los sistemas críticos de información en producción

### **Justificación Personal**

El presente proyecto de investigación es importante porque forma parte de la culminación práctica del proceso de aprendizaje y especialización que culminará con el grado académico de Maestro en Ciencias.

El trabajo permitirá analizar los problemas y definir controles de aseguramiento desde distintas perspectivas: desde la perspectiva del Auditor de Seguridad (CISA, LA ISO 27001, LRM ISO 31000), desde el punto de vista del Especialista en Aseguramiento de Seguridad (CISM), desde el punto de vista del Testeador de Seguridad e Intrusión (OPST), así como también del Especialista de Redes (CCNA), el conocimiento de todas estas especialidades entre sí, podrán identificar debilidades, amenazas, vulnerabilidades y los riesgos informáticos de las distintas tecnologías que son implementadas en las empresas hoy en día.

El proyecto ayudará a interpretar el “QUE”, propuesto por las Normas Internacionales y Buenas prácticas de la industria. Logrando aportar con la realización del “COMO” a través de modelos de evaluación de riesgos, análisis de impacto, diseños de controles de seguridad, y estrategias de continuidad.

### **6. Delimitación de la investigación**

**Delimitación espacial:** El lugar donde se realiza y aplica el estudio de la presente investigación es el Grupo Empresarial de Inversiones Nacional Vida S.A., en la ciudad de Santa Cruz de la Sierra, Bolivia

**Delimitación temporal:** El presente trabajo se considera desde junio del 2018, el estudio tendrá una duración de seis meses y finalizará en diciembre del 2018.

**Delimitación sustantiva:** El presente trabajo se enmarca en el área de Seguridad y Auditoría Informática.

En el análisis documental y algunos aspectos donde se aplique, se utilizarán los estándares internacionales de Riesgos, Continuidad y Seguridad:

- NB/ISO 22301:2012 Sistema de Gestión de Continuidad del Negocio – Requisitos
- NB/ISO 22313:2015 Sistema de Gestión de Continuidad del Negocio – Directrices
- NB/ISO/IEC 27001:2013 Sistema de Gestión de Seguridad - Requisitos.
- NB/ISO 31000:2014 Gestión del Riesgo

## **7. Diseño Metodológico**

### **7.1. Tipo de Investigación**

El presente trabajo de investigación es de tipo propositiva y aplicada, en tanto se podrá caracterizar las Amenazas y Vulnerabilidades para tratar las fuentes de riesgo y amenazas de Ciberseguridad, identificando los objetivos de recuperación; lo que permite plantear como solución al problema, con un enfoque de sistemas, un modelo Gestión de Continuidad del Negocio evaluando los procesos de misión crítica, para ser implementado en el Grupo empresarial de inversiones Nacional vida S.A., basado en la norma internacional ISO 22301.

### **7.2. Métodos de Investigación**

- **Método Histórico – lógico:** Permitirá ordenar la información, a partir de la sistematización a diferentes autores, del fundamento teórico del objeto de estudio,

identificando Riesgos y Amenazas de Ciberseguridad, para el desarrollo del marco teórico.

- **Método Análisis documental:** Basado en una guia elaborada por el autor, se caracterizarán los principios normativos en el campo de trabajo a través de las normas internacionales, considerando además los requisitos legales, resoluciones administrativas regulatorias y las buenas prácticas de la industria.
- **Método Enfoque de Sistema:** Para estructurar los procesos de Gestión de Continuidad del Negocio, caracterizando los componentes, funciones y las interacciones entre los procesos críticos del negocio.
- **Método experimental en su variante pre-experimental:** Permitirá comparar el estado actual (*Pre-Test*) con el estado deseado (*Post-Test*) y validar la propuesta de diseño; verificando la trasformación que ocurre después de aplicar la solución al problema en el campo de acción Tiempo Objetivo de Recuperación.

### 7.3. Técnicas e Instrumentos de Investigación

#### Técnicas

- **Entrevista** a Directores y Gerentes Generales, para caracterizar el contexto del negocio, las expectativas de las partes interesadas e identificar el Tiempo Objetivo de Recuperación deseado por la alta dirección y la estrategia de recuperación adoptada por las empresas del Grupo Empresarial de Inversiones.
- **Encuesta** a Gerentes de Línea, Ejecutivos y personal de puestos críticos para caracterizar las vulnerabilidades, amenazas y recopilar información de las restricciones que afectan a las empresas del Grupo de Inversiones.

## **Instrumentos**

- Guía de Análisis Documental, **Anexo No. 1**
- Guía de Observación, **Anexo No. 2**
- Cuestionario de Entrevista a Directores y Gerentes Generales, **Anexo No. 3**
- Cuestionario de Encuesta a Gerentes de Línea y Ejecutivos, **Anexo No. 4**

Los datos obtenidos de las encuestas serán procesados aplicando la estadística descriptiva a partir de los indicadores, para luego agruparlos a través de las dimensiones definidas de cada variable.

Finalmente, se realizará la triangulación de los resultados obtenidos a partir de la aplicación de los instrumentos de investigación, para determinar los problemas en el contexto donde se investiga y la validación de la propuesta de solución al problema de investigación.

### **7.4. Población y Muestra**

#### **Población**

Para las entrevistas se considera como población a los Directores y Gerentes Generales del grupo empresarial, siendo un total de 7 personas del Grupo empresarial de Inversiones Nacional Vida.

Para las encuestas se considera como población a los Gerentes de líneas, Ejecutivos y puestos críticos de las empresas, siendo un total aproximado de 44 funcionarios.

#### **Muestra**

El muestreo para las entrevistas se aplicará a un total del 100% de la población de Directores y Gerentes Generales.

El muestreo para las encuestas se aplicará al menos a un total del 95% de la población de Gerentes de líneas, Ejecutivos y funcionarios de puestos críticos de las empresas.

## CAPÍTULO I. MARCO TEÓRICO Y CONCEPTUAL

En este capítulo, a partir del método histórico lógico, se organiza y fundamenta el sustento teórico necesario sobre el objeto de estudio de la investigación: "Riesgos y amenazas de Ciberseguridad", y el campo de Acción: "Tiempo Objetivo de Recuperación". Se revisa información relevante, bajo la sistematización de las definiciones de los teóricos y a través del instrumento Guía de Análisis Documental, se caracterizan los Riesgos, Amenazas y Ciberseguridad, abordando las tendencias de las amenazas de Ciberseguridad. Se transita por las definiciones principales de tiempo objetivo de recuperación y sus tendencias.

Finalmente se analizan los principios normativos a través de las normas internacionales, resoluciones administrativas y buenas prácticas de la industria.

### 1.1 Riesgos y Amenazas de Ciberseguridad

#### 1.1.1. Riesgo

El riesgo es inherente a toda actividad humana, las personas evalúan los riesgos y adoptan un conjunto de acciones. Estas opciones se hacen al instante, casi de forma inconsciente y con un mínimo de análisis formal.

Se pone en práctica la gestión del riesgo todo el tiempo, consciente o inconscientemente, al tomar decisiones:

- Cruzar las calles (Seguridad Personal o de Bienestar)
- Invertir en acciones (Seguridad Financiera)
- Cambio de empleador (Seguridad Laboral)
- Ir de Vacaciones (Seguridad Personal o de Bienestar)

- Practicar deportes (Cuidado de la Salud)

El riesgo proviene de la palabra italiana *risico*, que significa peñasco o roca, utilizada por las principales compañías de seguros para describir el peligro en el mar (LRM 31000, 2008, p. 20).

La primera definición de riesgo fue dada en 1738 por el matemático Daniel Bernoulli en *Specimen theoriae novae de mensura sortis*. “El Riesgo es la expectativa matemática de una función de probabilidad de los sucesos” (LRM 31000, 2008, p. 22).

Cuando un evento se considera que sucederá con una probabilidad menor al 100%, entonces hay un riesgo.

Según el investigador británico Allan Lavell, PhD, afirma que el riesgo es: "Probabilidad de daños y pérdidas futuras: una condición latente y predecible en distintos grados, marcada por la existencia de AMENAZAS (naturales, socio naturales y antrópicos), VULNERABILIDAD (propenso a perder o ser dañado) y EXPOSICIÓN al daño; resultado de PROCESOS determinados de desarrollo de la sociedad" (Bankoff, Frerks, & Hilhorst, 2004)

De acuerdo a la (ISO 27005, 2010, pág. 2) cláusula 2.1, define el Riesgo en la Seguridad de la Información como “Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias”.

El autor asume la posición de la definición de la norma ISO 31000, la que define el Riesgo como “Efecto de la incertidumbre sobre el logro de los objetivos” (ISO 31000, 2014, pág. 4).

Según las notas la (ISO Guia 73, 2009, pág. 1) refiere lo siguiente: Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

Los objetivos pueden tener diferentes aspectos como: financieros, de salud y seguridad, o ambientales y se pueden aplicar a diferentes niveles como: nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa.

El riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

El **Cuadro No. 2**, muestra los ejemplos de la estrategia de la Gestión de Riesgos de una organización. Una Gestión de Riesgo eficaz permite prever los riesgos y tomar los riesgos relacionados a las oportunidades

**Cuadro No. 2.** Ejemplos de Estrategia de la Gestión del Riesgo

Tipo de Riesgo	Estrategia de la Gestión del Riesgo	Ejemplos
<b>Positivo</b> (Oportunidad)	Maximizar el retorno de la inversión teniendo en cuenta la prima de riesgo	Asumir el Riesgo de invertir en proyectos con alto potencial de rendimiento mediante el control de riesgos
<b>Neutral</b> (Incertidumbre)	Calcular las probabilidades de distintos escenarios de riesgo y prever las tendencias	Estudio de la tecnología, así como el seguimiento y revisión de los riesgos
<b>Negativo</b> (Amenaza)	Evitar, transferir, reducir o mantener los riesgos identificados	Evitar las tecnologías, que son inseguras, aplicación de los controles, seguro contra incidentes

Fuente: (LRM 31000, 2008, p. 26)

### 1.1.2. Amenazas

En el sentido de la seguridad de la información, son las actividades que representan un posible peligro a su información. “El peligro puede ser pensado como algo que afectaría negativamente a la confidencialidad, integridad o disponibilidad de sus activos, sistemas o

servicios. Por lo tanto, si el riesgo es el potencial de pérdida o daño, las amenazas pueden ser consideradas como agentes de riesgo” (GIAC Information Security, 2002).

Las amenazas pueden venir en muchas formas diferentes y provienen de múltiples fuentes. Hay amenazas físicas, como incendios, inundaciones, actividades terroristas, y los actos vandálicos. Hay amenazas electrónicas como los *hackers* y los virus. El conjunto particular de las amenazas, dependerá en gran medida de su situación. Qué es la empresa, dónde se encuentra, quiénes son sus socios y enemigos, lo valioso que es su información, cómo se almacena, mantiene y se asegura, quién tiene acceso a ella, y una serie de otros factores.

El autor asume la definición de «amenaza» de la norma ISO 31000, que cita a la amenaza como una «fuente de riesgo» y la define como “Elemento que solo o combinado posee potencial intrínseco para originar el riesgo” (ISO 31000, 2014, pág. 7).

Según la norma ISO 27005 las fuentes de amenazas se dividen en dos categorías: (ISO 27005, 2010, pág. 48)

- **Amenazas Comunes:**

Algunas de las amenazas comunes identificadas en la norma, considerando su origen:

- Accidentales (A): Fuego, Daño por agua, falla en el Sistema de A/C, Datos provenientes de fuentes no confiables, entre otros.
- Deliberadas (D): Destrucción de equipos o medios, Espionaje remoto, Hurto de equipos, entre otros.
- Ambientales o Naturales (E): Polvo, corrosión, congelamiento, fenómenos meteorológicos, radiación térmica, entre otros.

- **Amenazas Humanas:**

Las amenazas humanas por su fuente se pueden categorizar en:

- Pirata informático, intruso ilegal
- Criminal de la computación
- Terrorismo
- Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)
- Intrusos (empleados con entrenamiento deficiente, descontentos; malintencionados, negligentes, deshonestos o despedidos).

Las características de las fuentes de amenazas humanas definidas en la norma, se categorizan por Fuente de amenazas, Motivación y Acciones amenazantes: Pirata informática, intruso ilegal, criminal de la computación, terrorismo, espionaje industrial e intrusos.

Existen dos maneras de categorizar los ataques de red, (Stephen Northcutt 2001) indica que los ataques de red pueden llegar por varias vías. La siguiente lista muestra los ataques categorizados por vectores de amenazas principales:

- Ataque exterior desde la red pública
- Ataque exterior desde un teléfono
- Ataque interior desde una red o subred local
- Ataque interior desde una red inalámbrica
- Ataque interior desde un sistema local
- Ataque con un código malicioso

La segunda forma de categorizar los ataques de red, es basándose en la naturaleza del ataque (Capite 2007). Las categorías de ataques a redes incluyen los siguientes:

- Virus informático (*Malware*)
- Gusanos Informáticos (*Worm*)
- Caballos de Troya (*Trojan Horse*)
- Denegación de Servicios (*Denial of Service*)
- Denegación de Servicios Distribuida (*Distributed Denial of Service*)
- Programas espías (*Spyware*)
- Pesca de usuarios (*Phishing*)
- Desbordamiento de memoria (*Buffer Overflow*)
- Explotación de vulnerabilidades (*Exploit*)
- Ingeniería social (*Social Engineering*)

### **1.1.3. Ciberseguridad**

El significado de Ciberseguridad puede asociarse a muchos términos similares como ciberespacio, ciberamenazas, ciberataques, ciberguerra, cibercrimen, ciberincidentes, ciberdelincuentes. Término que en la actualidad ha comenzado a ser ampliamente utilizado.

Seguridad informática, Seguridad de la red, Seguridad de información, Ciberseguridad. Todos estos términos se utilizan para describir la protección de los activos de información. (CSX Cybersecurity Nexus, 2015, p. 5).

Entendiendo como activos de información a los “conocimientos o datos que tienen valor para una organización” (ISO IEC 27001, 2013). Los activos de información, además, incluyen, la información financiera, la propiedad intelectual y los detalles de los empleados, o la información que les confíen los clientes o terceros. (ISO IEC 27000, 2018, p. 5)

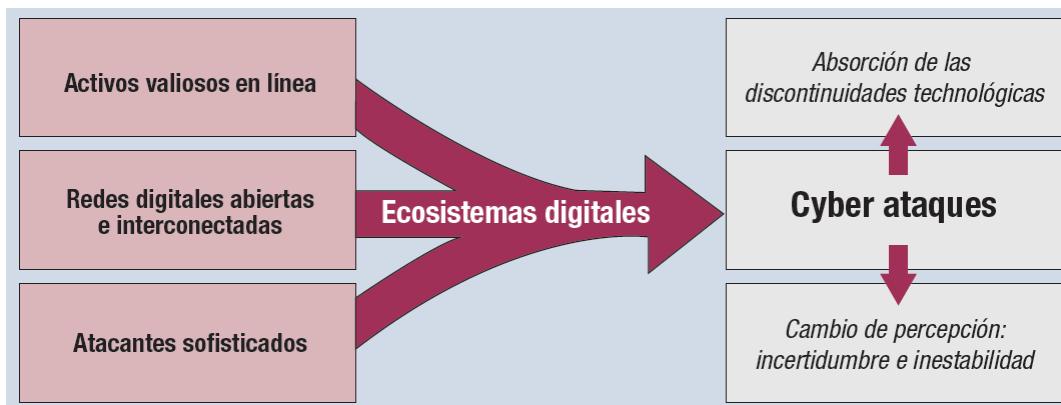
Los términos «Ciberseguridad» y «Seguridad de la información» comúnmente se usan de manera indistinta. Algunos utilizan el término Ciberseguridad como sinónimo de seguridad de la información, seguridad de TI y gestión de riesgos de la información. En los círculos gubernamentales, han adoptado definiciones más técnicas relacionadas con la defensa nacional, incluyendo la ciberguerra y la protección de las infraestructuras críticas. Aunque diferentes grupos tienden a adaptar la terminología para sus propios fines, hay algunas diferencias importantes entre la Ciberseguridad y la Seguridad de la Información.

La seguridad de la información trata con la información, independientemente de su formato: incluye los documentos en papel, propiedad digital e intelectual en las mentes de las personas, y las comunicaciones verbales o visuales. La ciberseguridad, por otro lado, se ocupa de la protección de los activos digitales, desde las redes al *hardware* y la información que es procesada, almacenada o transportada a través los sistemas de información interconectados.

Además, conceptos tales como ataques patrocinados por naciones-estados y amenazas avanzadas persistentes (APTs) pertenecen casi exclusivamente a la ciberseguridad. Es útil pensar en la ciberseguridad como un componente de la seguridad de la información.

El autor asume la definición de ciberseguridad de ISACA (*Information Systems Audit and Control Association*), citada en CSX Cybersecurity, donde “La ciberseguridad se encarga de amenazas internas y externas a los activos de información digital de una organización, centrándose en los procesos críticos de datos electrónicos, procesamiento de señales, análisis de riesgo y la ingeniería de seguridad de los sistemas de información” (CSX Cybersecurity Nexus, 2015, p. 5).

De acuerdo al profesor investigador Jeimy Cano Ph.D, un ciberataque, como se ilustra en la **Figura No. 2**, un ejercicio de “creación y aprovechamiento de vulnerabilidades, que considerando los activos de información en línea, las redes digitales abiertas e interconectadas y las capacidades de los atacantes, son capaces de producir cambios de percepción en el entorno, que resultan difíciles de detectar y enfrentar”.



**Figura No. 2.** Realización del valor de un ciberataque

Fuente: (Jeimy J. Cano, 2016)

Un ciberataque confirma la responsabilidad que se advierte por la convergencia entre la tecnología de información y la tecnología de operaciones. Esto es, que tanto los encargados de mantener el control de los procesos industriales o de fabricación, es decir, aquellos que aseguran que las fallas de la operación no afecten el mundo exterior, así como los profesionales de seguridad de la información, cuyas actividades están concentradas en evitar que entes externos comprometan los equipos internos, no comparten un nuevo dominio de protección denominado resiliencia digital.

El autor asume la definición de resiliencia digital del investigador Jeimy Cano Ph.D, citado en ISACA *Journal*. “Combina lo mejor de la disciplina operativa con la resistencia de las protecciones perimetrales, articulando las personas, los procesos, la tecnología y el marco

normativo, es capaz de crear un esfuerzo conjunto que defienda el valor de los procesos de negocio”.

Mientras el ciberataque encuentre una vista especializada o parcial de la defensa y anticipación en la estrategia de protección, la efectividad de sus acciones hará evidente la falta de comunicación entre las áreas, la debilidad de las interfaces disponibles, la inexperiencia del directorio, la desalineación de los objetivos estratégicas y sobre manera, la ausencia de lecciones aprendidas por condiciones semejantes sobre la infraestructura o información relevante para la organización.

#### **1.1.4. Tendencias de las amenazas de Ciberseguridad**

La Ciberseguridad juega un papel significativo en el panorama cibernético actual en constante evolución. Nuevas tendencias en movilidad y conectividad presentan más variedad de desafíos que nunca antes, ya que los nuevos ataques continúan desarrollándose junto con las tecnologías emergentes. Los profesionales de la ciberseguridad deben estar informados y ser flexibles para identificar y gestionar nuevas amenazas potenciales, tales como las amenazas persistentes avanzadas (*Advanced Persistent Threat*), con eficacia.

Los APTs son los ataques de un adversario que posee niveles sofisticados de experiencia y recursos significativos, los cuales permiten al atacante crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataque (CSX Cybersecurity Nexus, 2015, p. 5).

El informe de predicciones de amenazas de *McAfee Labs* 2018. Indica que “La Ciberseguridad se encuentra en una etapa altamente volátil, con nuevos dispositivos, riesgos desconocidos y nuevas amenazas que aparecen todos los días, incluido el aprendizaje

automático, *ransomware*, aplicaciones sin servidor y problemas de privacidad” (McAfee, 2017).

La empresa de seguridad informática *McAfee*, considera que los principales riesgos para la seguridad informática en 2018 se centran en estos puntos:

- Evolución del *ransomware* hacia nuevos sectores. Las predicciones de McAfee señalan que los ataques de *ransomware* buscarán objetivos menos tradicionales, individuos de alto poder adquisitivo, servicios con un gran número de usuarios y dispositivos conectados IoT (*Internet of Things*).
- *Machine learning* e Inteligencia Artificial (IA). Según la empresa de ciberseguridad, las empresas deberán aumentar la inteligencia de las máquinas y su capacidad de respuesta para evitar una nueva generación de ciberataques con la IA como objetivo.
- Aplicaciones *serverless*. Estas aplicaciones informáticas sin servidor basadas en las posibilidades de la Nube también son vulnerables a los ataques de denegación de servicio (DDoS) que se traducen en costosas interrupciones de las funciones prestadas al usuario.
- Gestión y uso de los datos personales. Desde el punto de vista de los internautas, uno de los principales focos de atención va a estar centrado en las políticas de privacidad, uso y gestión de los datos personales; en especial tras la entrada en vigor del nuevo Reglamento.
- General de Protección de Datos de la UE y sus implicaciones, por ejemplo, en redes sociales, aplicaciones o plataformas de contenido digital que podrían ver condicionada su reputación *online* por infracciones en esta materia.

Según el informe de Kaspersky de Amenazas para la seguridad de la información, se indica lo siguiente: “Vivimos en un mundo conectado, donde las tecnologías digitales tienen a convertirse en parte de la existencia cotidiana de las personas y organizaciones. Esto ha introducido nuevas vulnerabilidades y amenazas. Algunas industrias son actualmente objetivos para el ataque cibernetico” (Kaspersky Lab).

Para las predicciones de la industria y tecnología se han elegido varias áreas; presentando algunos de los riesgos claves que podrían estar por venir y su impacto potencial.

- Predicciones de Amenazas para el sector Automotriz.
  - Vulnerabilidades introducidas por falta de atención del fabricante
  - Vulnerabilidades introducidas a través de un producto y servicio en crecimiento
  - Ningún código de *software* es 100% libre de errores, y donde hay errores puede haber *exploits*
  - *Software* escrito por diferentes desarrolladores, instalado por diferentes proveedores, y a menudo informando a diferentes plataformas de gestión
  - Las aplicaciones significan felicidad para los cibercriminales con componentes cada vez más conectados por las empresas más familiarizado con el *hardware* y *software*
- Predicciones de Amenazas para el sector de la Salud conectado (*e-health*).
  - Ataques contra equipos médicos con el objetivo de extorsión, interrupción maliciosa
  - Ataques dirigidos en el robo de datos
  - Ataques de *ransomware* contra instalaciones de salud
  - El concepto de un perímetro corporativo claramente definido continuará

- Datos confidenciales transmitidos
- Datos de pacientes sin encriptar
- Datos que generalmente están mínimamente protegidos
- Ataques disruptivos, en forma de denegación de servicio
- Ataques a través de *ransomware* que simplemente destruye los datos (como *WannaCry*)
- Tecnologías emergentes como extremidades artificiales, implantes para mejoras fisiológicas inteligentes, realidad aumentada incorporada.
- Predicciones de Amenazas para el sector financiero.
  - Desafíos de pago en tiempo real (*Real-time payment*)
  - Ataques de ingeniería social (*Social engineering*)
  - Amenazas móviles (*Mobile threats*)
  - Violaciones de datos (*Data breaches*)
  - Objetivos de criptomoneda (*Cryptocurrency targets*)
  - Adquisición de cuenta (*Account takeover*)
  - Fraude como servicio (*Fraud as a Service*)
  - Ataques ATM
- Amenazas en el sector industrial.
  - Aumento en las infecciones de *malware* general y accidental
  - Mayor riesgo de ataques de *ransomware* dirigidos
  - Más incidentes de ciberespionaje industrial
  - Ataques a sistemas industriales
  - Nuevos tipos de *malware* y herramientas maliciosas

- Cambios en las regulaciones nacionales
- Los delincuentes aprovecharán los análisis de amenazas publicados por los investigadores de seguridad
- Creciente disponibilidad e inversión en seguros cibernéticos industriales
- Predicciones de Amenazas para criptomonedas.
  - Los ataques de *ransomware* obligarán a los usuarios a comprar criptomonedas
  - Ataques dirigidos con minería
  - Aumento de minería continuará e involucrará a nuevos actores
  - Minería *web* (*Web-mining*)
  - Caída de ICO (oferta inicial de monedas)

Las tecnologías conectadas tienen el poder de mejorar la vida, pero traen consigo nuevas vulnerabilidades que los ciberataques podrán rápidamente explotar. Seguiré viendo numerosos incidentes, ataques, vulnerabilidades y nuevas tendencias.

## 1.2 Tiempo Objetivo de Recuperación

### 1.2.1. Definiciones Principales

El autor asume la definición de MAO, MBCO, RPO y RTO citados en la norma ISO 22301.

- **Interrupción Máxima Aceptable (MAO: Maximum Acceptable Outage).**

El tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto/servicio o realizar una actividad, para convertirse en inaceptable. Conocido también como Periodo máximo tolerable de Interrupción (MTPOD: *Maxium Tolerable Period of Disruption*) (ISO 22301, 2012, pág. 8).

- **Objetivo mínimo de Continuidad del Negocio (MBCO: *Minimum Business Continuity Objective*).**

Nivel mínimo de servicios o productos que es aceptable para que una organización pueda lograr sus objetivos de negocio durante una interrupción (ISO 22301, 2012, pág. 9).

- **Punto Objetivo de Recuperación (RPO: *Recovery Point Objective*).**

Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación. También se puede denominar como "Perdida máxima de datos". (ISO 22301, 2012, pág. 11)

De acuerdo al manual de CISA (*Certified Information Systems Auditor*) de ISACA, “El RPO se determina sobre la base de la pérdida de datos aceptable en caso de una interrupción de operaciones”. Ello indica el punto más anticipado en el tiempo en el que es aceptable recuperar los datos. Por ejemplo, si el proceso puede permitirse perder los datos hasta 24 horas antes del desastre, entonces la última copia de respaldo debería ser hasta 24 horas antes de la interrupción y, por tanto, las transacciones durante RPO y la interrupción deberán ser ingresadas después de la recuperación (conocido como “*catch-up-data*” o puesta al día de los datos).

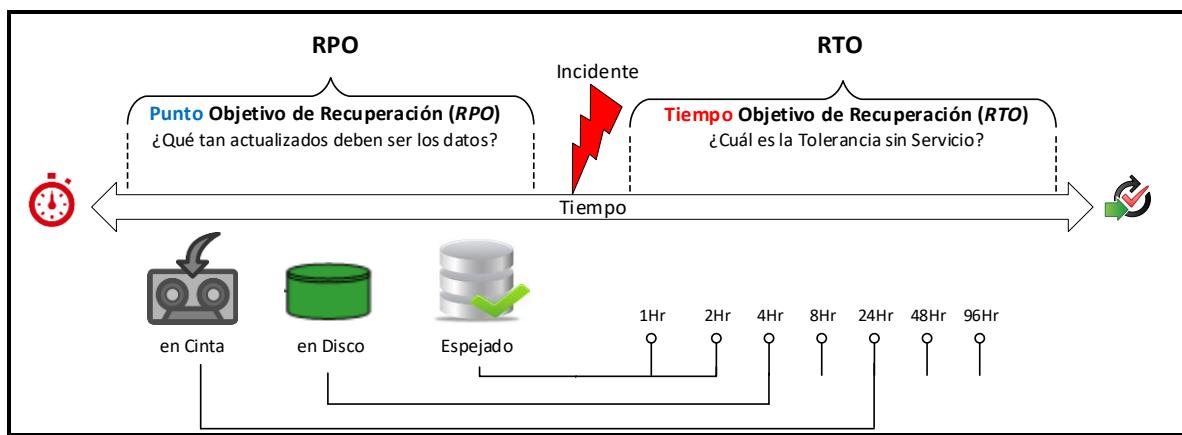
RPO cuantifica efectivamente la cantidad permitida de pérdida de datos en el caso de interrupción, Es casi imposible recuperar la totalidad de los datos. Incluso después de recuperar los datos faltantes, algunos todavía se perderán y a ellos se hace referencia como datos huérfanos (Meadows, Rolling, 2009, pág. 529) .

- **Tiempo Objetivo de Recuperación (RTO: Recovery Time Objective).**

El autor asume la definición del Tiempo Objetivo de Recuperación de la norma ISO 22301 “Periodo de tiempo después de un incidente, en el que el producto o servicio deber ser reanudado, o la actividad debe reanudarse, o los recursos deben ser recuperados” (ISO 22301, 2012, pág. 11).

De acuerdo al manual CISA (*Certified Information Systems Auditor*) de ISACA, “El RTO se determina sobre la base de tiempo de inactividad aceptable en caso de una interrupción de operaciones. Ello indica el punto más anticipado en el tiempo en el que las operaciones de negocio deben retomarse después del desastre.” (Meadows, Rolling, 2009, pág. 530).

En la **Figura No. 3**, se muestra la relación entre el Punto Objetivo de Recuperación (RPO) y el Tiempo Objetivo de Recuperación (RTO). Ambos conceptos están basados en parámetros de tiempo. Cuanto más bajo sea el tiempo de recuperación requerido, más elevado será el costo de las estrategias de recuperación.



**Figura No. 3.** Relación entre un *RTO* y *RPO*

Fuente: (Meadows, Rolling, 2009)

### 1.2.2. Tendencias

De acuerdo a ISACA (*Information Systems Audit and Control Association*), además del RTO y RPO, hay algunos parámetros adicionales que son importantes para definir estrategias de recuperación, estos incluyen:

- **Ventana de Interrupción (IW: *Interruption Window*).**

El tiempo que una organización puede esperar desde el punto de falla hasta la restauración de servicios/aplicaciones críticas. Después de ese tiempo, las pérdidas progresivas causadas por la interrupción no son aceptables.

- **Objetivo de Prestación del Servicio (SDO: *Service Delivery Objetive*).**

El nivel de servicio a proveer durante el modo de proceso alterno hasta que se restaure la situación normal. Esto está directamente relacionado con las necesidades del negocio.

- **Cortes máximos tolerables.**

El tiempo máximo que la organización puede soportar en modo alterno. Después de este punto, pueden surgir diferentes problemas, en especial, si el SDO alterno es más bajo que el SDO habitual, y la información pendiente de ser actualizada puede tornarse no manejable. (Meadows, Rolling, 2009, pág. 530).

## 1.3 Norma ISO 22301

### 1.3.1. Origen

La norma internacional ISO 22301 especifica los requisitos para el establecimiento y la gestión de un efectivo Sistema de Gestión de Continuidad del Negocio (SGCN). (ISO 22301, 2012)

La continuidad del negocio contribuye a una sociedad más resiliente, la comunidad general y el ambiente organizacional incluidos. Es por esta razón que otras organizaciones deben involucrarse en el proceso de recuperación.

La norma ISO 22301 surge debido al desarrollo de buenas prácticas, lineamientos y normas de continuidad de negocio como:

- **1995:** *NFPA 1600*, es el lineamiento más antiguo. En él se establecieron unos criterios para gestionar los desastres, emergencias y programas de continuidad de las organizaciones.
- **1997:** *Disaster Recovery Institute International* (DRII), se establecieron las Prácticas Profesionales para la Gestión del Negocio.
- **2002:** Las Buenas Prácticas para la Continuidad del Negocio, publicado por el *Business Continuity Institute*.
- **2003:** se publicó el lineamiento PAS 56, define el proceso, principios y terminología del sistema de continuidad del negocio.
- **2006:** se publicó el BS 25999-1, establece el ciclo de vida de la continuidad del negocio.
- **2007:** se publica el BS 25999-2:2007, primer estándar internacional que podía ser auditado y certificado. Su objetivo era especificar los requerimientos necesarios para el enfoque de sistemas de gestión.
- **2007:** se publicó el ISO/PAS 22399, consiguiendo lineamientos genéricos para establecer un sistema de gestión para el desarrollo de la continuidad operacional e incidentes potenciales.

- **2008:** ISO/IEC 24762, dispuso guías para el abastecimiento de información y comunicación útiles para la recuperación de desastres.
- **2008:** BS 25777, contempla un código de buenas prácticas para la gestión de la continuidad del negocio.
- **2010:** ASIS/BSI *Business Continuity Management Standard*, es un lineamiento basado en BS 25999, y concreta los requerimientos necesarios para un SGCN.
- **2011:** PAS 200, Gestión de Crisis – Lineamiento y Buenas Prácticas.
- **2011:** surge ISO/IEC 27031, define los conceptos y principios de tecnología de información y comunicación requeridos para que una organización se prepare para la continuidad de negocio.
- **2012:** se publica la ISO 22301 “Sistema de Continuidad del Negocio”, la planificación, implementación, establecimiento, operación, revisión, monitoreo, mantenimiento y la mejora continua de su efectividad está basado en el ciclo PHVA.

La **Figura No. 4**, muestra la evolución de los estándares en Continuidad del Negocio explicado anteriormente.



**Figura No. 4.** Evolución de los estándares en Continuidad del Negocio

Fuente: (Gestión, 2012)

### **1.3.2. Características Principales**

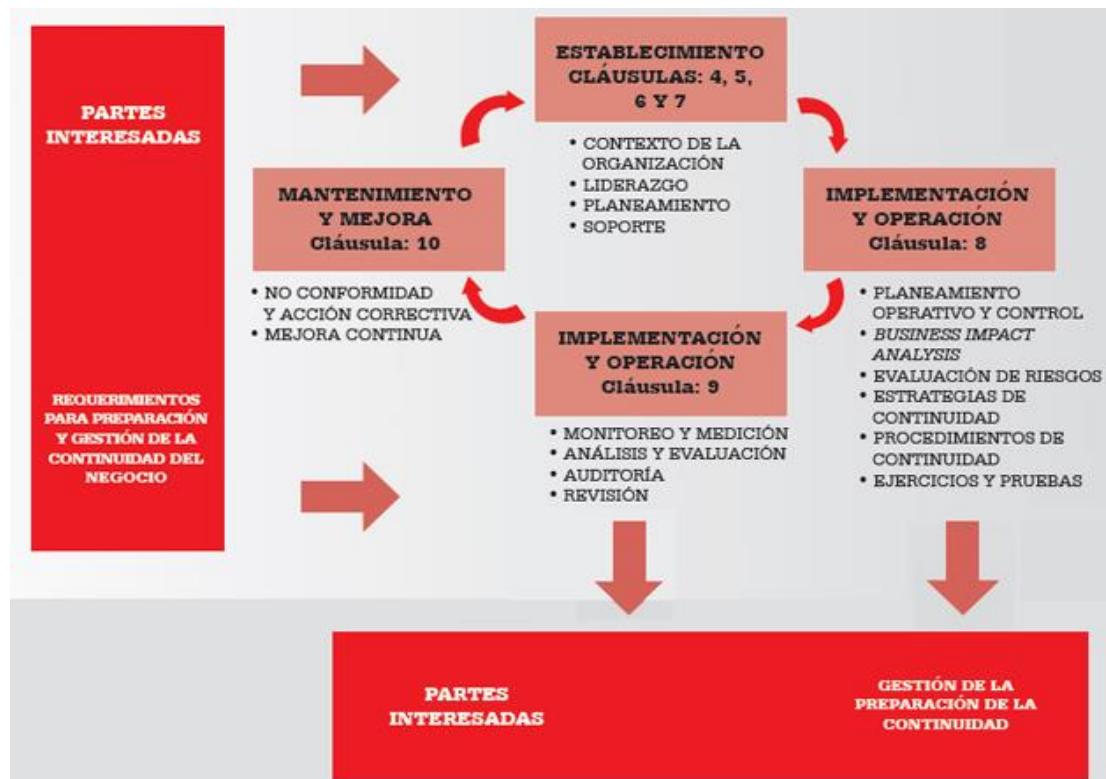
De acuerdo a la norma ISO 22301 (ISO 22301, 2012, p. 1), Un SGCN hace énfasis en la importancia de:

- Entender las necesidades de la organización y la necesidad de establecer una Gestión de Continuidad de negocio, sus objetivos y política
- Implementar y operar los controles y medidas para administrar la capacidad general de una organización en responder a incidentes
- Hacer el seguimiento y revisión de la eficacia del SGCN
- Mejora continua basada en mediciones objetivas

El SGCN, como todos los sistemas de gestión, contiene los siguientes componentes claves:

- a) Una Política
- b) Personas con responsabilidades definidas
- c) Gestión de los procesos relativos a:
  1. Política
  2. Planeación
  3. Implementación y Operación
  4. Evaluación de desempeño
  5. Análisis de la Gestión, y
  6. Mejoramiento
- d) Documentación que proporcione evidencia auditable. y
- e) Cualquier proceso de Gestión de la Continuidad de Negocio relevante para la organización.

La Figura No. 5, muestra el Ciclo PDCA aplicado al proceso de Continuidad del Negocio, se puede apreciar como el SGCN toma insumos de las partes interesadas, requerimientos para la gestión de la continuidad, y a través de las necesarias acciones y procesos produce resultados de continuidad para cumplir con los requerimientos (ISO 22301, 2012).



**Figura No. 5.** Ciclo PDCA aplicado al proceso de Continuidad del Negocio

Fuente: (Gestión, 2012)

El establecimiento es el «Plan». Donde se aprecian los principales requerimientos. Las secciones 4, 5, 6 y 7 de la norma corresponden al establecimiento. Seguidamente se tiene la «implementación y operación», el cual es el «Do»; esta etapa del proceso está compuesta por los requerimientos de la sección 8. Luego se tiene la fase «monitoreo y revisión», la cual representa al «Check». Allí se pueden apreciar los principales requerimientos de esta sección. Esta fase comprende los requerimientos de la sección 9 de la norma. Finalmente, se tiene la

fase de «mantenimiento y mejora», representando a la fase «Act», la que engloba todos los requerimientos de la cláusula 10 de la norma.

### **1.3.3. Tendencias de la Gestión de Continuidad**

Con la llegada del nuevo milenio, ha habido una mayor necesidad de garantizar el cumplimiento de políticas, procesos y controles relacionados con ciberseguridad. Las organizaciones ya están comenzando a gestionar los nuevos riesgos de ciberseguridad, adecuando sus políticas, procesos y controles para afrontar la ciberseguridad.

El público en general también está reconociendo que *Internet* se está volviendo cada vez más intimidante y un lugar destructivo, no solo para la información personal que está en línea (en las redes sociales), también para los datos del mundo corporativo. Cualquier violación de los datos personales impactan al público directamente, como los datos personales residen dentro de las agencias gubernamentales, empresas privadas e instituciones financieras.

Después de la gestión de continuidad, el equipo de respuestas a incidentes deberá entrenarse y prepararse para la gestión de crisis.

## **Gestión de Crisis**

De acuerdo al artículo «Cómo prepararnos para enfrentar la crisis en las organizaciones», una crisis se define como cualquier suceso inesperado y adverso, natural o artificial, que impacta las operaciones y reputación de una organización. Se involucran usualmente, las autoridades, los reguladores, los medios y el público (Acosta, 2018).

Típicamente, en una crisis hay información limitada o bien, ahora en exceso y distorsionada por las redes sociales también, extrema presión de tiempo y poca experiencia en la gestión de las situaciones de emergencia.

Los riesgos operacionales que se pueden enfrentar y que pueden convertirse en crisis son, por ejemplo: fenómenos naturales (terremotos, inundaciones, incendios, huracanes); acción humana (fraudes, sabotajes, huelgas, saqueos, secuestros, epidemias); colapso tecnológico (cortes de energía, fallas informáticas).

De acuerdo al artículo «Gestión de Crisis»: elemento vital para la continuidad del negocio, las crisis son inevitables, pero el estar preparados para gestionarlas hará la diferencia entre el éxito y el fracaso (Néstor Garrido, 2018).

La Gestión de Crisis requiere una serie de factores diseñados para prevenir o aminorar los resultados negativos de una crisis y que estén orientados a proteger a la organización y sus partes interesadas contra daños, lo que además brinda una perspectiva única y crítica sobre las nuevas habilidades de gestión y los tipos de organizaciones que se necesitan en estos días. El proceso de Gestión de Crisis comprende cuatro fases interrelacionadas: Prevención, Respuesta, Recuperación y Aprendizaje.

- **Prevención**

Es el mejor estado para evitar que una crisis se desarrolle y para ello la Gestión de Riesgos, así como la intervención oportuna de las señales o advertencias tempranas que anuncian la probable ocurrencia de una crisis, tales como: quejas por la calidad de productos o servicios por parte de consumidores y/o clientes, fallas recurrentes en la producción o despacho de productos clave, observaciones de auditorías internas y externas, así como aquellas resultantes de una inspección de la autoridad regulatoria.

También considera el desarrollo de los planes de Gestión de Crisis que contemplen objetivos y acciones a tomar para cada tipo de crisis potencial, la selección y entrenamiento del equipo de Gestión de Crisis con roles y tareas específicas, la selección e implementación

de una sala principal y otra alterna para desarrollar las sesiones de simulación y atención de las crisis reales por parte del equipo y por último, definir las estrategias de comunicación durante la crisis, definiendo los canales adecuados.

- **Respuesta**

Es la aplicación de los planes por parte del equipo, los que deben ser probados regularmente en ejercicios de simulación lo que ayudará a que en una situación real se actúe con rapidez para tomar el control, incluso con información insuficiente, para ello es importante comunicar los hechos que existen. Los objetivos de esta etapa son:

- Contener la crisis.
- Elevar moral de empleados.
- Tranquilizar a clientes, consumidores y socios estratégicos.
- Evitar los vacíos de información dejando menos lugar al rumor y la especulación.

- **Recuperación**

Una vez que la crisis concluye es necesario reactivar la normalidad en las actividades del negocio lo más pronto posible. El tiempo de inactividad de una crisis causa problemas financieros. Mientras más rápido pueda una organización regresar a las operaciones normales, menores serán las pérdidas financieras en las que incurrirá. Para ello, es crítico reconocer la importancia de la preparación, conocer las implicancias de la crisis y activar el plan de continuidad de negocio, de ser necesario.

- **Aprendizaje**

Esta etapa envuelve la evaluación de la prevención y respuesta de la organización ante la crisis, determina qué se hizo bien, qué se hizo mal y qué faltó hacer. Toda esta información debe ser organizada y documentada para actualizar el sistema de gestión de

riesgos e intervención de señales tempranas, los planes de Gestión de Crisis y que sirva de insumo para los ejercicios de simulación que el equipo debe desarrollar periódicamente.

También es importante tomar en cuenta las crisis que diversas organizaciones del mismo giro de negocio hayan podido experimentar a fin de analizar las implicancias, reacción e impacto. Lo más importante de esta etapa es tener la capacidad de tomar la experiencia como una oportunidad de sacar ventaja a través de la mejora de procesos, productos y como resultado de ello la percepción de los grupos de interés.

La Gestión de Crisis es un proceso continuo que requiere la participación de todas las áreas de una organización, en especial de aquellas que tienen relación directa con los grupos de interés, por lo que la intervención y atención efectiva de las cuatro fases es crucial para garantizar la continuidad de las operaciones del negocio.

#### **1.4 Norma ISO 31000**

Cada día la inseguridad está más generalizada en la gestión empresarial. Los riesgos empresariales son cambiantes y cada vez evolucionan. Por lo que, las organizaciones deben aprender a gestionar todo tipo de riesgos empresariales y considerar además los riesgos no identificados o no detectados.

La norma ISO 31000 es un estándar internacional muy utilizado por las empresas para gestionar sus riesgos; Por ello, se ha convertido en un referente para la gestión de riesgos, indica que: las organizaciones de todo tipo y tamaño enfrentan influencias y factores internos y externos que tornan incierto el logro de sus objetivos y el momento en que los alcanzarán. El efecto que esa incertidumbre tiene sobre los objetivos de la organización se llama "riesgo".

Todas las actividades de una organización implican un riesgo. Las organizaciones gestionan el riesgo, identificándolo, analizándolo y luego valorando si el riesgo debe ser modificado mediante su tratamiento con el propósito de satisfacer los criterios de riesgo. A lo largo de este proceso, se comunica, se consulta con las partes interesadas y se realiza seguimiento y control, revisión del riesgo y los controles que lo modifican a fin de asegurar que no es necesario tratamiento adicional del riesgo. (ISO 31000, 2014, pág. 1)

#### **1.4.1. Evolución**

De acuerdo a (ISO Tools, 2019) , en los últimos años las empresas se han esforzado en implantar sistemas de gestión de riesgos, apoyados en diferentes metodologías, entre las que se destaca la norma ISO 31000, siendo la más aceptada. Para realizar esta tarea se han realizado inversiones que van desde la creación de áreas especializadas hasta la compra de herramientas de *software*, pasando por el pago a consultores y tipos para establecer un Modelo de Gestión de Riesgos sobre las necesidades de la organización.

A veces, todos los elementos no son suficientes para ser exitosos en la misión, muchas veces se dejan de lado o no se realizan los esfuerzos suficientes para involucrar a todo el personal que se encuentra realizando la operación, quién es el responsable de ejecutar los controles definidos y de reportar posibles materializaciones de riesgos. No siempre conscientes de la importancia de generar una cultura real del riesgo en las empresas, cada persona debe reflexionar sobre su papel dentro del sistema, deberá ser consciente de la necesidad de realizar seguimiento a los riesgos de los procesos, según la oportunidad en el registro de los eventos, la revisión permanente de la efectividad de los controles, identificando las claves y mitigando los riesgos.

Los aspectos se convierten en factores críticos para implantar con éxito un Sistema de Gestión de Riesgos en las empresas. En ese momento encuentro un desafío que va a permitir a una empresa conseguir beneficios a través de diferentes frentes, incluyendo el estratégico, el táctico y el operativo.

#### **1.4.3. Características Principales**

##### **Gestión de Riesgos (*Risk Management*)**

- Identificación en Gestión de Riesgos:

Es necesario hacer mucho énfasis en la definición de objetivos:

- Línea de negocio, procesos y subprocesos
- Procesos críticos
- Aspectos metodológicos
- Riesgo inherente
- Asignación de responsabilidad

La identificación del riesgo se ha de realizar mediante un grupo multidisciplinario de expertos en la materia. En ella se ha de reconocer todas las amenazas posibles, dentro de cada uno de los procesos o ítems.

- Análisis en Gestión de Riesgos:

El análisis se mide en función a la probabilidad del impacto que pueda ocasionar cualquier tipo de riesgo inherente a un proceso:

- Metodología acorde al grado de madurez.
- Cualitativa o cuantitativa.
- Registro de eventos o incidentes.
- Controles y su grado de efectividad.

- Evaluación en Gestión de Riesgos:

Una vez que se han establecido los objetivos de priorización, se procede a la evaluación:

- Criterios de riesgo
- Apetito de riesgo
- Priorización de riesgos

- Tratamiento en Gestión de Riesgos:

Es necesario tener en cuenta el riesgo y la cobertura que se establece según el apetito de riesgo establecido por la organización:

- Planes de acción
- Seguimiento de cumplimiento de plan de acción
- Razonabilidad del control y medidas de tratamiento
- Asignación de presupuesto
- Indicadores de efectividad

- Comunicación y consulta en Gestión de Riesgos:

Los planes de comunicación pueden ser internos o externos:

- Reportes internos o externos
- Informar y consultar
- Nivel y evolución indicadores de riesgo
- Seguimiento al perfil de riesgo
- Mantener eficiencia

- Revisión y monitoreo en Gestión de Riesgos:

Se lleva a cabo según los indicadores establecidos previamente:

- Cumplimiento de políticas y procedimientos
- Efectividad del sistema
- Seguimiento al perfil de riesgo
- Periodicidad
- Responsabilidad

La Gestión del Riesgo no hay que ver como algo aislado, sino como un modelo que debe involucrar todos los procesos de la empresa. La norma ISO 31000 contribuye a la toma de decisiones (ISO Tools, 2019).

### **Principios de la gestión del Riesgo**

Para que la Gestión del Riesgo sea eficaz, la norma ISO 31000 recomienda cumplir los siguientes principios (ISO 31000, 2014, págs. 10-11):

- La gestión del riesgo protege y crea valor
- Es una parte integral de todos los procesos de la organización
- Es parte de la toma de decisiones
- Aborda explícitamente la incertidumbre
- Es sistemática, estructurada y oportuna
- Se basa en la mejor información disponible
- Está hecha a medida
- Tiene en cuenta factores humanos y culturales
- Es transparente e inclusiva
- Es dinámica, iterativa y capaz de reaccionar ante los cambios
- Permite la mejora continua de la organización

#### 1.4.4. Tendencias de la Gestión de Riesgos de Ciberseguridad

De acuerdo al informe Gartner citado en (Gartner, 2018), Se apunta a seis tendencias emergentes que ya se están empezando a vislumbrar en el mercado de la seguridad y las previsiones sobre su evolución en el futuro. Conociendo estas tendencias las organizaciones podrán gestionar el riesgo de forma más eficiente.

Ante la proliferación de las ciberamenazas, de su sofisticación y de su impacto en los negocios, conocer las amenazas que se ciernen sobre ellos y las consecuencias que puede acarrearles resulta clave para minimizar su impacto. Gartner apunta a seis tendencias para mejorar la capacidad de recuperación y elevar su posición.

- 1) Cada vez más, los directivos de las organizaciones son conscientes del impacto de la ciberseguridad en sus negocios, en sus capacidades para conseguir sus objetivos de negocio y a la hora de proteger su reputación corporativa. Esto está haciendo que la seguridad TI forme parte de cualquier estrategia empresarial digital sólida y, aunque los directivos no han sido muy receptivos inicialmente, cada vez más cambia este sentimiento. Casos como la violación de datos de Equifax (El proveedor de servicios de crédito de Estados Unidos, su incumplimiento afectó a 143 millones de usuarios), ataques como *Wannacry*, entre otros, han causado daños tan grandes que están concienciando cada vez más de los peligros a los que están expuestos.
- 2) Los temas legales y reglamentos sobre la protección de datos están afectando a los planes de negocio digitales. Los datos y su protección cobran cada vez mayor relevancia y escándalos como el de *Cambridge Analytica*, han llevado a que los entornos regulatorios sean más complejos y las sanciones cada vez más elevadas. Ante

- el creciente valor de los datos y sus infracciones, los programas de gestión de datos se tornan esenciales.
- 3) Las nuevas tecnologías de detección de amenazas, las actividades y modelos de autenticación requieren de grandes cantidades de datos, lo que está impulsando la adopción de productos de seguridad en la nube (modo *cloud*). Estos permiten utilizar los datos casi en tiempo real para proporcionar soluciones más ágiles y adaptativas. Buscar proveedores que proporcionen servicios de seguridad en la nube con gran manejo en la gestión de datos y «*machine learning*», y una alta protección de datos será clave.
  - 4) El «*machine learning*», o aprendizaje de máquina, proporciona un alto valor, especialmente a la hora de resolver múltiples problemas de seguridad, como el *malware*, las amenazas internas y los ataques avanzados. Gartner prevé que, para 2025, el «*machine learning*» será una parte normal de las soluciones de seguridad y compensará las capacidades crecientes y la escasez de personal.
  - 5) Cada vez más, las decisiones de compra de seguridad se basan en factores geopolíticos que se suman a las consideraciones de compra tradicionales. Las recientes prohibiciones del gobierno estadounidense contra empresas rusas y chinas son ejemplos de esta tendencia.
  - 6) Ante la concentración de tecnologías, como la computación en la nube, es importante tener en cuenta los riesgos que también puede conllevar en lo que a seguridad se refiere. Es clave evaluar las implicaciones de seguridad en la centralización, en disponibilidad, confidencialidad y flexibilidad de los planes de negocio digital. Si los

riesgos de la centralización pueden amenazar los objetivos de la organización, será necesario explorar una arquitectura alternativa y descentralizada.

## **1.5 Gestión de Continuidad del Negocio (BCM)**

El autor asume la definición de Continuidad del Negocio, Gestión de Continuidad del Negocio, Sistema de Gestión de Continuidad del Negocio y Plan de Continuidad del Negocio, definidos en la norma ISO 22301. (ISO 22301, 2012).

**Continuidad del Negocio (BC):** Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

**Gestión de Continuidad del Negocio (BCM):** Proceso de gestión integral que identifica las amenazas potenciales para la organización y los impactos para la empresa. Si las amenazas ocurren, debe proporcionar un marco para la construcción de la resiliencia de la organización con la capacidad de una respuesta eficaz que salvaguarde los intereses de sus grupos de interés clave, reputación, marca y las actividades que crean valor.

**Sistema de Gestión de Continuidad del Negocio (BCMS):** Parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio. El sistema de gestión incluye estructura organizativa, las políticas, actividades de planificación, responsabilidades, procedimientos, procesos y recursos.

**Plan de Continuidad del Negocio (BCP):** Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción. Normalmente, esto incluye los recursos, servicios y actividades necesarias para garantizar la continuidad de las funciones críticas del negocio.

## 1.6. Análisis de Riesgo

En su tesis de maestría (Peña Castro, 2016, p. 57) señala que la evaluación y control de riesgos permite: “identificar las amenazas internas y externas, incluyendo concentraciones de riesgos, que pueden causar la interrupción o pérdida de las actividades críticas de la organización, así como la probabilidad o frecuencia de que ocurra una amenaza.”

A manera de conclusión (González Villalobos, 2015, p. 44) indica que: “los entornos globalizados representan riesgos mucho más complejos debido al cambio de paradigma en las operaciones, para mitigar la posibilidad de materialización de amenazas que impacten el negocio, se deben implementar mecanismos como procesos de Gestión de Continuidad del Negocio”

## 1.7. Análisis de Impacto (BIA: *Business Impact Analysis*)

De acuerdo a la publicación especial del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST SP 800-34 Rev. 1, 2010) El propósito del *BIA* es: “identificar y priorizar los componentes del sistema correlacionándolos con los procesos de misión / negocio que el sistema soporta, y usar esta información para caracterizar el impacto en los procesos si el sistema no estuviera disponible”.

(González Villalobos, 2015, p. 44) concluye que uno de los principales elementos para modelar los Sistemas de Continuidad del Negocio es: “la correcta elaboración de un *BIA*, en dónde se determinen los procesos críticos para el negocio y las dependencias necesarias para continuar brindando los servicios acordados a un nivel aceptable”.

## 1.8. Estrategias de Recuperación

El autor asume las estrategias de recuperación basadas en el manual de CISA (*Certified Information Systems Auditor*) de ISACA. “Una estrategia de recuperación identifica la mejor forma de recuperar un sistema en caso de interrupción, incluyendo desastre, y provee orientación basada en qué procedimientos detallados de recuperación se pueden desarrollar” (Meadows, Rolling, 2009, pág. 531).

Se deben presentar todas las alternativas a la alta dirección. La alta dirección debe seleccionar la estrategia más apropiada de las alternativas ofrecidas y aceptar el riesgo residual inherente. Las estrategias elegidas deben ser usadas para desarrollar el Plan de continuidad del negocio.

La selección de una estrategia de recuperación depende de:

- La criticidad del proceso de negocio y las aplicaciones que soportan los procesos
- Costo
- El tiempo requerido para recuperarse
- Seguridad

Existen diversas estrategias para recuperar los recursos críticos de información. La estrategia apropiada es la que tiene un costo para un tiempo aceptable de recuperación que también es razonable con el impacto y la probabilidad de ocurrencia que se determinó en el análisis de impacto sobre el negocio (BIA).

El costo de recuperación es el costo de prepararse para posibles interrupciones (por ejemplo, los costos fijos de compra, mantenimiento y prueba regular de las computadoras redundantes, y mantenimiento de la configuración para el direccionamiento alterno de la red)

así como también los costos variables de poner todos estos elementos en uso en el caso de una interrupción.

En general, cada plataforma de TI en la que corra una aplicación que soporte una función crítica del negocio necesitará una estrategia de recuperación. Hay muchas estrategias alternativas. Se debe seleccionar la alternativa más apropiada en términos de costos de recuperación y de costos del impacto identificado en el análisis de impacto sobre el negocio (BIA) y basado en el nivel de riesgo (*Risk Assessment*). Las estrategias de recuperación basadas en el nivel de riesgo identificado para la recuperación deben incluir el desarrollo de:

- Sitio Caliente (*Hot Sites*)
- Sitio templado (*Warm Sites*)
- Sitio Frío (*Cold Sites*)
- Instalaciones de procesamiento de información duplicada (*Mirror Sites*)
- Sitios Móviles (*Mobile Sites*)
- Acuerdos recíprocos con otras organizaciones (*Reciprocal agreements*)

### **1.9. Plan de Continuidad del Negocio (BCP)**

El Plan de Continuidad se ha convertido en un dominio crítico en la gestión de conocimiento de una organización; en los últimos años se han experimentado muchos acontecimientos que han quedado marcados en la memoria del mundo, como son: el terrorismo, los terremotos, los huracanes, los tsunamis e inundaciones.

En su tesis de maestría (Peña Castro, 2016, p. 12) concluye que el Plan de Continuidad: “Es la última línea de defensa de una entidad, cuando los controles han fallado. El BCP es el control final, que puede prevenir eventos drásticos, como lesiones, pérdidas de vida o el fracaso de una organización”

El autor (González Villalobos, 2015, p. 8) indica en su tesis de maestría que: “El aumento de las exigencias en la forma de hacer negocios, representa, para las organizaciones modernas, la necesidad de adquirir capacidades estratégicas y tácticas para responder de manera eficiente ante incidentes que afecten la operación y las obligaciones adquiridas”.

En su investigación (Sarabia Zapata, 2015, p. 17) indica que los Planes tiene como finalidad: “recuperar la operación de los servicios en producción, mitigando riesgos y afectación al negocio con consecuencias como pérdida de ingresos o mala imagen para la Compañía”.

“El BCP debe ser considerado como un proceso fundamental dentro de una organización, ya que de éste depende su supervivencia o continuidad, permitiendo que la empresa continúe brindando sus servicios cuando ocurra un desastre o una interrupción de las actividades” (Romero Romero, 2014, p. 28).

Según la publicación especial de la Guía de Planificación de Contingencias para Sistemas de Información Federales del Instituto Nacional de Estándares y Tecnología de Estados Unidos, indica que el Plan de Continuidad (BCP): “Es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para desarrollar la capacidad de dar una respuesta efectiva, que permita proteger los intereses, imagen y valor de las actividades” (NIST SP 800-34 Rev. 1, 2010)

En opinión del autor de la investigación, el BCP permite soportar la misión de una organización y los procesos de negocio durante y después de una interrupción. Un ejemplo de un proceso de misión del negocio puede ser, el proceso de gestión comercial, gestión de siniestros o el proceso de gestión de cobranzas de una organización.

## CAPITULO II. DIAGNÓSTICO

El presente capítulo tiene por objetivo analizar el estado actual de los Riesgos y Amenazas de Ciberseguridad y el estado actual del Tiempo Objetivo de Recuperación del Grupo Nacional de Inversiones Nacional Vida S.A., se aplican diferentes instrumentos de investigación como la entrevista y encuesta. Se analizan los resultados de la aplicación de los instrumentos y se triangulan los resultados para analizar los problemas que serán abordados en la propuesta de solución al problema.

### 2.1 Acercamiento al contexto que se investiga

El Grupo Empresarial de Inversiones Nacional Vida S.A. es un Holding empresarial de inversiones que asegura la sinergia entre sus empresas, velando por la rentabilidad y valor agregado de sus accionistas, contribuyendo al desarrollo económico del país.

El Grupo Empresarial de Inversiones Nacional Vida S.A. tiene oficinas distribuidas en varias ciudades de Bolivia, los sistemas informáticos de la compañía se brindan bajo un esquema centralizado, es por ello que el diagnóstico se enfocará en la ciudad de Santa Cruz, principalmente en la oficina central ubicada en Av. Paraguá de la ciudad.

El holding está conformado por 4 compañías en el territorio de Bolivia:

- Nacional Seguros Vida y Salud S.A.
- Nacional Seguros Patrimoniales y Fianzas S.A.
- Conecta Redes y Servicios S.A.
- Tecnología Corporativa Tecorp S.A.

Por su giro de negocio las empresas del Holding del Grupo Empresarial de Inversiones, son empresas reguladas por:

- Autoridad de Fiscalización y Control de Pensiones y Seguros (APS)

Dado que las empresas también cotizan en la Bolsa Bolivia de valores, razón por la cual son reguladas por:

- Autoridad de Supervisión del Sistema Financiero (ASFI)

### **2.1.1 Estructura organizacional de la empresa**

En la **Figura No. 6**, se muestra el organigrama corporativo del Grupo empresarial de Inversiones Nacional Vida S.A.



**Figura No. 6** Organigrama corporativo del holding de Inversiones

Fuente: (Grupo Nacional Vida, 2018)

### **2.2 Procedimiento para el Diagnóstico**

Para el diagnóstico del campo de acción se aplican diferentes instrumentos de investigación, tales como: Guía de observación, y Cuestionario de entrevistas dirigido a Directores y Gerentes Generales, y del cuestionario de encuestas dirigido a Gerentes de

Línea, Ejecutivos y Funcionarios del área de TI para analizar el estado actual de los Riesgos y Amenazas de Ciberseguridad de las empresas.

### **2.2.1 Definición conceptual.**

A partir de la sistematización de diferentes núcleos teóricos realizada en el capítulo 1 a los diferentes investigadores, el autor de este trabajo asume las siguientes definiciones:

Para la variable independiente, el autor asume la definición de la norma ISO 31000, la que define el Riesgo como “Efecto de la incertidumbre sobre el logro de los objetivos”. (ISO 31000, 2014, pág. 4). Y para la amenaza, de la norma ISO 31000, la que cita a la amenaza como una “fuente de riesgo” y la define como “Elemento que solo o combinado posee potencial intrínseco para originar el riesgo”. (ISO 31000, 2014, pág. 7).

La definición de ciberseguridad se asume de ISACA (*Information Systems Audit and Control Association*), donde “La ciberseguridad se encarga de amenazas internas y externas a los activos de información digital de una organización, centrándose en los procesos críticos de datos electrónicos, procesamiento de señales, análisis de riesgo y la ingeniería de seguridad de los sistemas de información” (CSX Cybersecurity Nexus, 2015, pp. 5-6).

En el caso de la variable dependiente, el autor asume la definición del Tiempo Objetivo de Recuperación de la norma ISO 22301 “Periodo de tiempo después de un incidente, en el que: el producto o servicio deber ser reanudado, o la actividad debe reanudarse, o los recursos deben ser recuperados” (ISO 22301, 2012, pág. 11).

### **2.2.2 Definición operacional de las variables.**

Con la definición conceptual de las variables se realiza la derivación en dimensiones e indicadores que se encuentran en el **Anexo No. 5** del documento, y que sirve como base para la elaboración de los instrumentos de investigación para la recolección de información.

Variable independiente: Riesgos y amenazas de ciberseguridad, se deriva en seis dimensiones (Fuentes de Riesgo, Amenazas de Ciberseguridad, Identificación, Análisis, Evaluación, Política) y sus respectivos indicadores (11).

Variable dependiente: Tiempo Objetivo de Recuperación, se deriva en dos dimensiones (Compromiso y apoyo de la dirección, Estrategia de Tecnología, Seguridad y Continuidad) y tres indicadores.

### **2.2.3 Instrumentos de investigación**

A continuación, se identifican los instrumentos que se aplican, las unidades evaluativas y los objetivos de cada uno, resumidos en el **Cuadro No. 3**.

**Cuadro No. 3.** Instrumentos de Investigación

INSTRUMENTO	UNIDAD EVALUATIVA	OBJETIVOS
Guía de Análisis Documental	Normas internacionales	Asumir una postura en las definiciones valorando los documentos normativos, requisitos legales, resoluciones administrativas regulatorias y las buenas prácticas de la industria
Guía de Observación	Personal Operativo	Contrastar el cumplimiento de las características de las Instalaciones del Sitio principal y alterno
Cuestionario de Entrevista	Directores y Gerentes Generales	Caracterizar el contexto del negocio, las expectativas de las partes interesadas e Identificar el Tiempo Objetivo de Recuperación deseado por la Alta Dirección y la estrategia de recuperación adoptada por las empresas del Grupo Empresarial de Inversiones
Cuestionario de Encuesta	Gerentes de Línea y Ejecutivos	Caracterizar las vulnerabilidades, amenazas y recopilar información de las restricciones que afectan a las empresas del Grupo de Inversiones

**Fuente:** Elaboración Propia, 2018

## 2.3 Análisis de los resultados de la aplicación de los instrumentos

### 2.3.1 Resultados de la aplicación del Cuestionario de Encuesta

Con los indicadores obtenidos en la etapa de operacionalización se diseña la encuesta que se encuentra en el **Anexo No. 4.**

#### Caracterización de la muestra

La encuesta se aplica en el Grupo Empresarial de Inversiones, Nacional Seguros Patrimoniales y Fianzas, Nacional Seguros Vida y Salud, Tecnología Corporativa, Conecta Redes y Servicios.

La caracterización de los encuestados se detalla en el **Cuadro No. 4.**

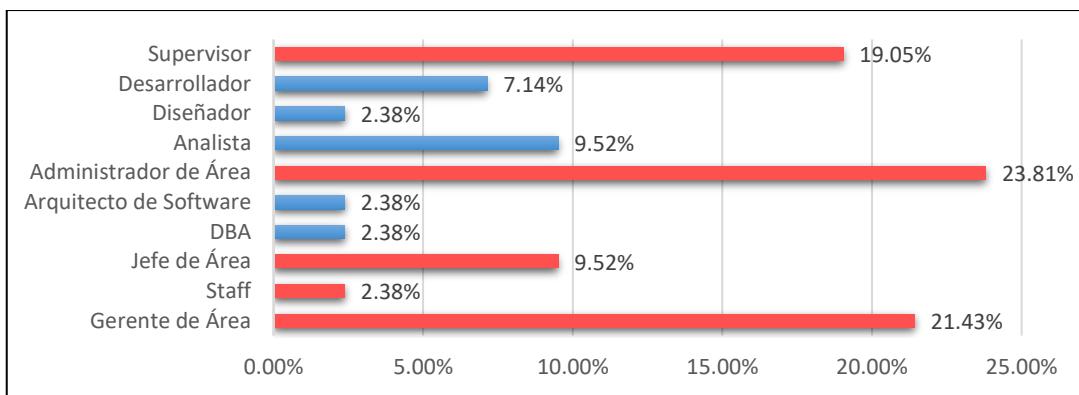
**Cuadro No. 4.** Encuestados por Cargo

Cargo	Total	%
Gerente de Área	9	21.43%
Staff	1	2.38%
Jefe de Área	4	9.52%
DBA	1	2.38%
Arquitecto de Software	1	2.38%
Administrador de Área	10	23.81%
Analista	4	9.52%
Diseñador	1	2.38%
Desarrollador	3	7.14%
Supervisor	8	19.05%
<b>Total</b>	<b>42</b>	<b>100%</b>

Fuente: Elaboración Propia, 2018.

Se aplica la entrevista a los diferentes Gerentes de Línea, Ejecutivos y Funcionarios del área de TI que tienen personal subordinado.

Se puede observar en la **Figura No. 7**, que el 76.19% de los encuestados ocupan cargos críticos y tienen funcionarios a su cargo.

**Figura No. 7.** Muestra por Cargos

Fuente: Elaboración Propia, 2018.

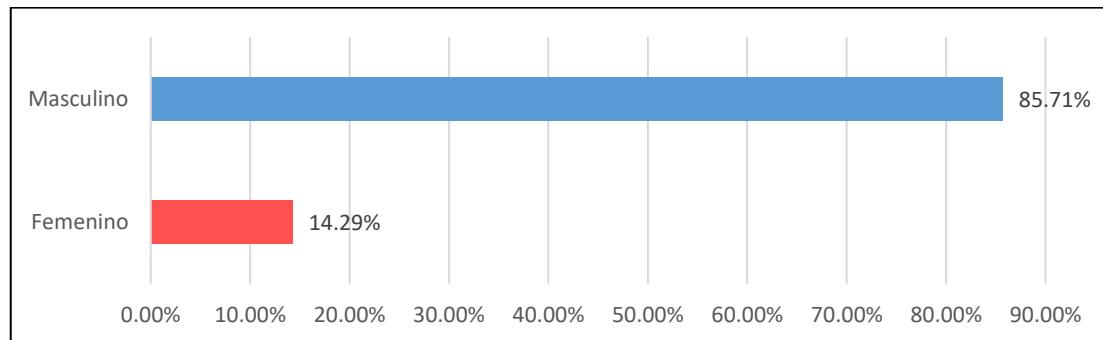
De los encuestados, (36) para el 85.71% son menores de 45 años, distribuidos por edad según el **Cuadro No. 5**.

**Cuadro No. 5.** Encuestados por Edad

Rango de Edad	Total	%
menos de 25 años	0	0.00%
Entre 25 a 34 años	18	42.86%
Entre 35 a 44 años	18	42.86%
Entre 45 a 54 años	6	14.29%
más de 55 años	0	0.00%
<b>Total</b>	<b>42</b>	<b>100%</b>

Fuente: Elaboración Propia, 2018.

Es de destacar que, el 85.71% de los encuestados son de sexo masculino (36) según se observa en la **Figura No. 8**

**Figura No. 8.** Encuestados por Género

Fuente: Elaboración Propia, 2018.

Referido a la experiencia de trabajo en la empresa, el 78.58% de los encuestados tienen entre 1 y 10 años de antigüedad en la empresa (33) según se observa en el **Cuadro No. 6.**

**Cuadro No. 6.** Encuestados por Antigüedad

Antigüedad en la Empresa	Total	%
menos de 1 año	4	9.52%
de 1 a 5 años	17	40.48%
de 6 a 10 años	16	38.10%
de 11 a 15 años	4	9.52%
de 16 a 20 años	1	2.38%
más de 20 años	0	0.00%
<b>Total</b>	<b>42</b>	<b>100%</b>

Fuente: Elaboración Propia, 2018.

Los cargos críticos son ocupados por personas con diferentes grados de escolaridad, siendo la Educación Universitaria completa la de mayor representación (15), lo que representa el 35.71% del total encuestado. El resto de los niveles de estudio se detallan en el

**Cuadro No. 7.**

**Cuadro No. 7.** Encuestados por Nivel de Estudio

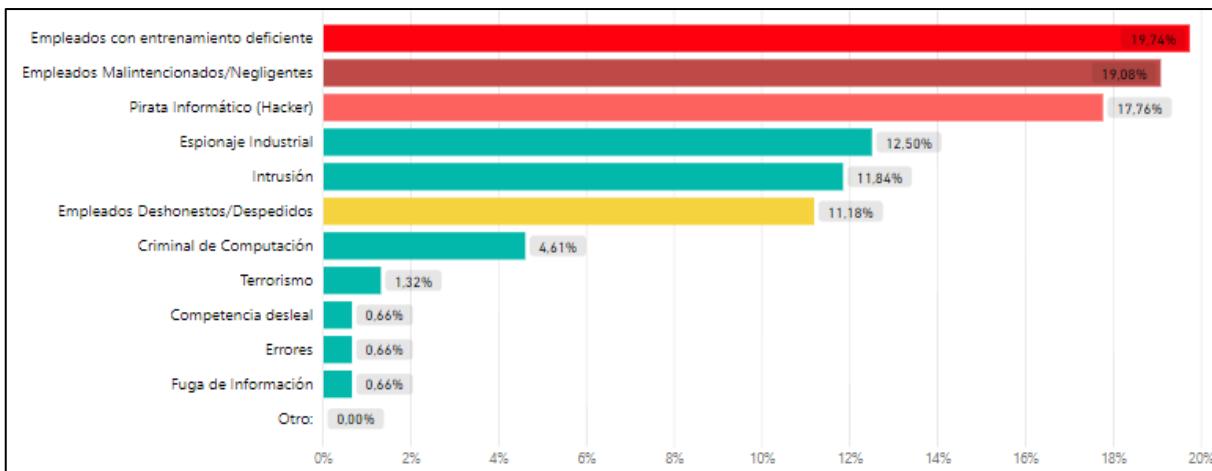
Nivel de Estudio	Total	%
Técnico Superior	3	7.14%
Educación Universitaria incompleta	9	21.43%
Educación Universitaria completa (Licenciatura)	15	35.71%
Postgrado/Diplomado	8	19.05%
Maestría	7	16.67%
<b>Total</b>	<b>42</b>	<b>100%</b>

Fuente: Elaboración Propia, 2018.

## Resultados de la Encuesta

En la pregunta No. 1, sobre las fuentes de riesgos que preocupan a la organización, los encuestados refieren en primer lugar, con 19.74%, Empleados con Entrenamiento deficiente, seguido de Empleados Malintencionados/Negligentes con 19.08% y Pirata Informático (*Hacker*) en tercer lugar, con un 17.76%; el resto de las fuentes de riesgo se observan en la

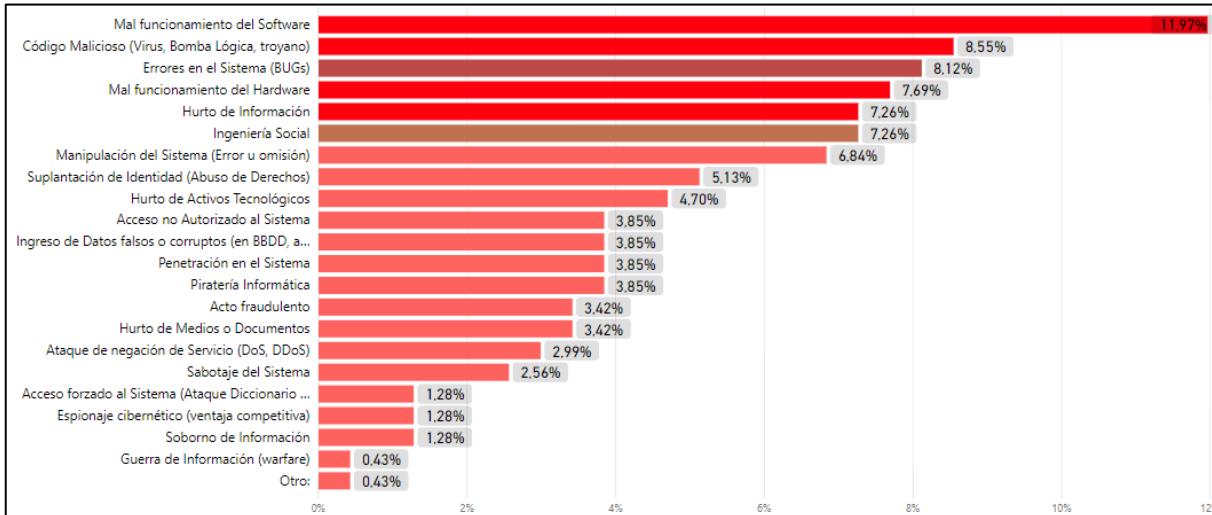
**Figura No. 9.**



**Figura No. 9.** Pregunta 1 – Encuesta

Fuente: Elaboración Propia, 2018.

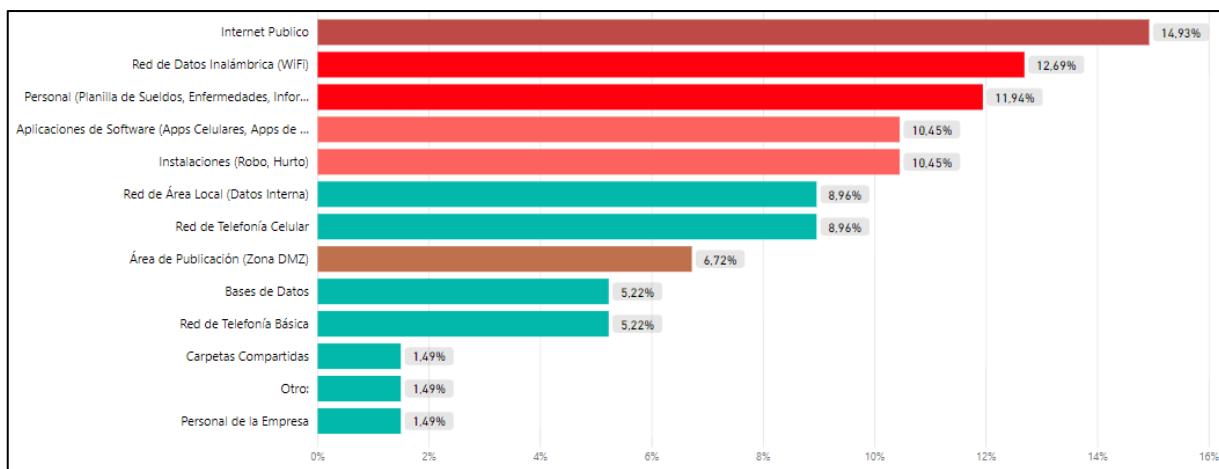
En la pregunta No. 2, referido a las Amenazas de Ciberseguridad que han impactado a la organización en los últimos años, de acuerdo a la **Figura No. 10**, el 82.91% de las amenazas pasa por: Mal funcionamiento de *Software*, Código malicioso (Virus, Bomba Lógica, Troyano), Errores en el Sistema (BUGs) hasta Piratería informática.



**Figura No. 10.** Pregunta 2 – Encuesta

Fuente: Elaboración Propia, 2018.

Al preguntar sobre los posibles vectores de fuga de información en la pregunta No. 3, de acuerdo a la **Figura No. 11**, el 85.07% de los vectores de fuga se consideran desde: Internet Público, Red de Datos Inalámbrica (WIFI) hasta Área de Publicación (Zona DMZ).

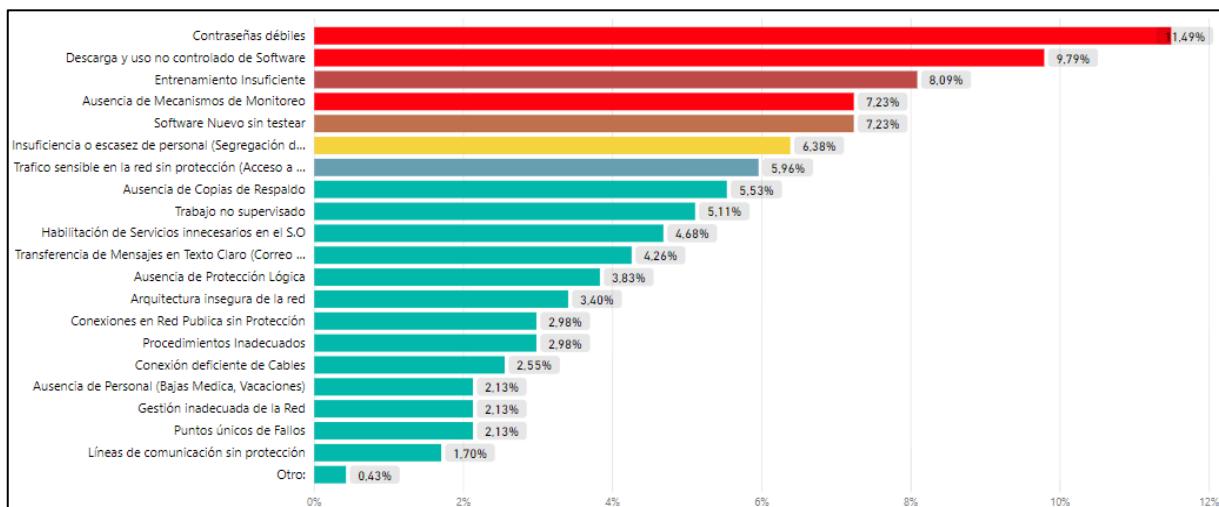


**Figura No. 11.** Pregunta 3 – Encuesta

Fuente: Elaboración Propia, 2018.

En la pregunta No. 4, acerca de los activos de información evaluados en el Análisis de Riesgos, se destacan principalmente los Procesos Críticos como parte de la evaluación.

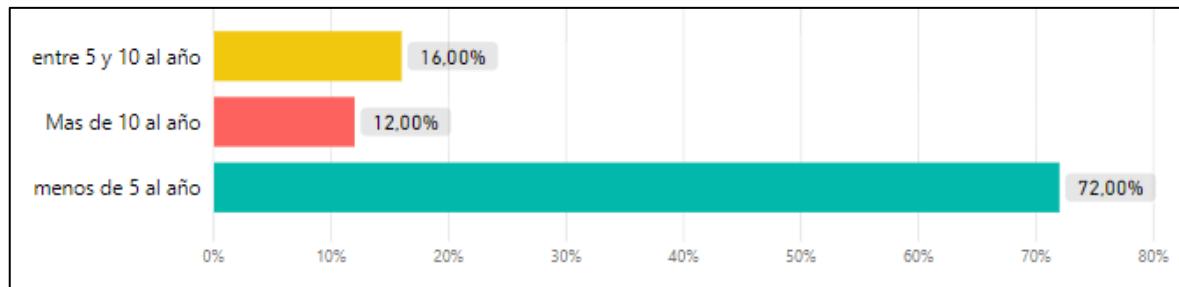
Referido a las Vulnerabilidades detectadas en la Organización, en la Pregunta No. 5, los encuestados destacan: Contraseñas débiles, descarga y uso no controlado de software, entrenamiento insuficiente, hasta ausencia de copias de respaldo, como las vulnerabilidades más críticas que representan un 61.7% del total identificado; el resto de vulnerabilidades se observan en la **Figura No. 12**.



**Figura No. 12.** Pregunta 5 – Encuesta

Fuente: Elaboración Propia, 2018.

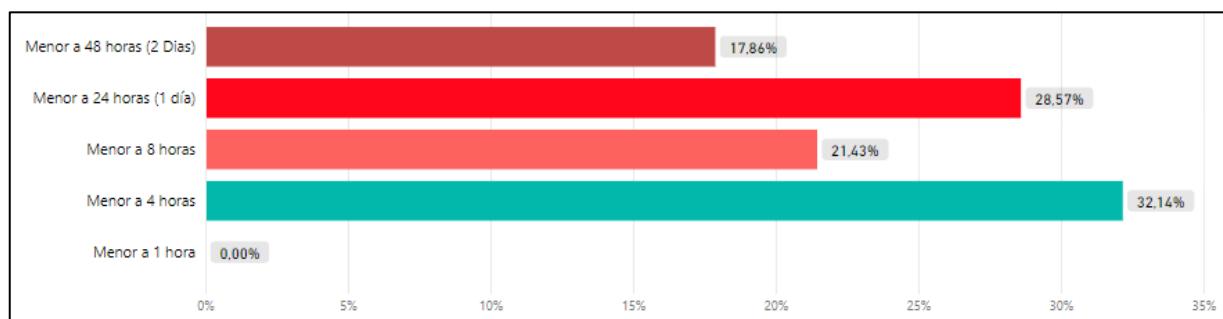
Los encuestados refieren en la pregunta No. 6 que las interrupciones que han impactado los procesos críticos del negocio en los últimos años, tiene una frecuencia menor a 5 incidentes por año, según se observa en la **Figura No. 13**.



**Figura No. 13.** Pregunta 6 – Encuesta

Fuente: Elaboración Propia, 2018.

Un aspecto importante a destacar es el Tiempo Objetivo de Recuperación (RTO) de los últimos incidentes e interrupciones mayores, refrendados en la pregunta No. 7, el 45.24% de los incidentes han sido solucionados entre 8 y 48 horas, aspecto crítico para la organización por la imagen ante sus clientes y accionistas, de acuerdo a la **Figura No. 14**.

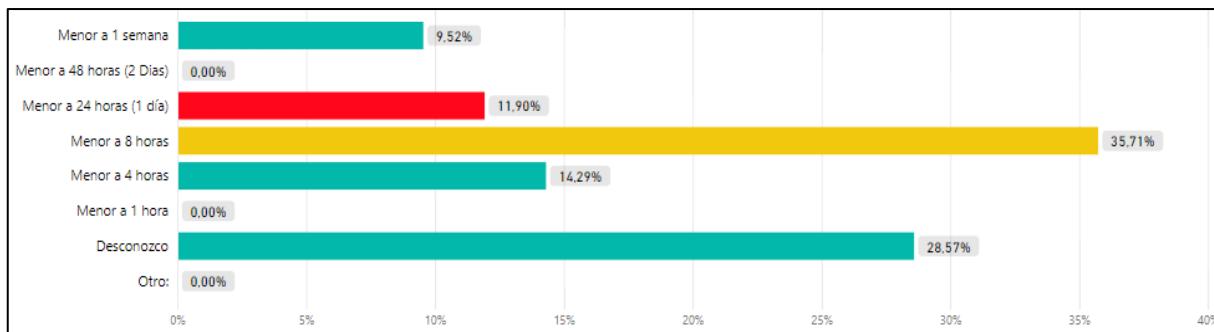


**Figura No. 14.** Pregunta 7 – Encuesta

Fuente: Elaboración Propia, 2018.

Los funcionarios encuestados manifiestan que, en las pruebas de continuidad realizadas, el 71.43% de las ejecuciones han sido entre 4 horas y 1 semana, de acuerdo a la

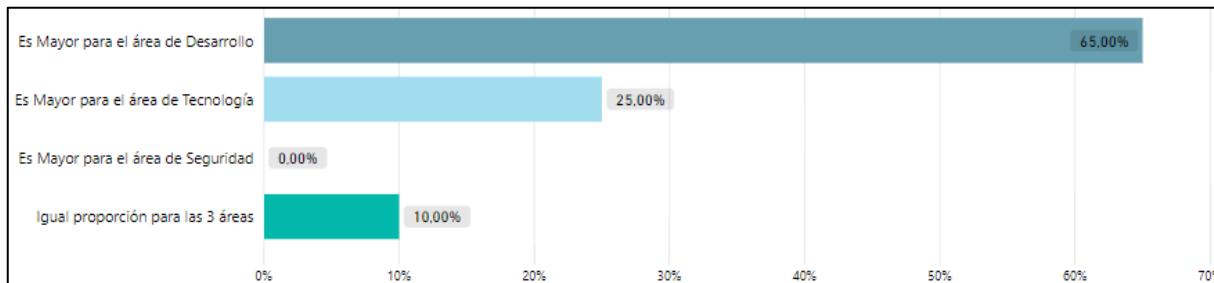
**Figura No. 15.** Aspecto crítico para la organización por el impacto financiero, normativo y regulatorio.



**Figura No. 15.** Pregunta 8 – Encuesta

Fuente: Elaboración Propia, 2018.

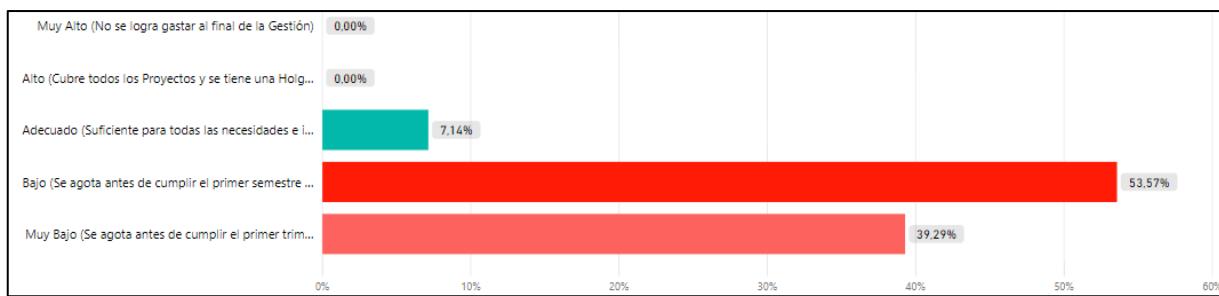
Siendo un aspecto importante la Seguridad de la información y la Continuidad del negocio, pregunta No. 9, los responsables consideran que la mayor cantidad del Presupuesto Anual se destina al desarrollo de *software* (65%), no siendo equitativo para Tecnología y Seguridad, **Figura No. 16**. Los funcionarios consideran que el presupuesto de Tecnología y Seguridad no es equitativo, dado que se utilizan los recursos de Tecnología para cubrir los costos de Seguridad.



**Figura No. 16.** Pregunta 9 – Encuesta

Fuente: Elaboración Propia, 2018.

De acuerdo a la pregunta No. 10, el 92.86% de los encuestados consideran que el presupuesto asignado para Tecnología y Seguridad es bajo o Muy Bajo para garantizar la recuperación en el Tiempo objetivo definido por el Grupo empresarial, **Figura No. 17**.



**Figura No. 17.** Pregunta 10 – Encuesta

Fuente: Elaboración Propia, 2018.

### 2.3.2 Resultados de la aplicación del Cuestionario de Entrevista

A partir de aplicar el cuestionario de entrevista, **Anexo No. 3**, a la Alta Dirección de la Corporación, se tienen los siguientes resultados:

#### A. Perfil de riesgo Inherente de la organización (Riesgos propios del Negocio):

##### Fuga de Información.

- Cobertura de Pólizas de Seguros
- Personas Contratantes
- Registros de Salud de los asegurados
- Siniestros de los asegurados

#### B. Amenazas de Ciberseguridad que generan un Impacto adverso al negocio.

- Espionaje Cibernético/Industrial (Riesgo de exposición de las estrategias de negocio de cada empresa)
- Sabotaje del Sistema (Empleados Deshonestos/Despedidos que han tenido Acceso a los Sistema de información)
- Piratería Informática (Riesgo de Fuga de Información de las Base de Datos de Clientes)

- C. La Continuidad y disponibilidad de los servicios críticos de la empresa NO se consideran una meta Corporativa.**
- Diferenciación por la tecnología
  - Proteger la Información
- D. La arquitectura TI y de seguridad NO consideran los Riesgos y Amenazas de Ciberseguridad que pueden afectar la Misión y Visión Empresarial.**
- Se está trabajando a través de la Gestión Profesional y eficiente de Proyectos (Análisis de Riesgo y Análisis de Impacto) para gestionar los riesgos tecnológicos, la Seguridad y la Continuidad del Negocio.
- E. Interrupciones que han afectado los procesos críticos del negocio en los últimos 5 años.**
- Como toda empresa, no se está libre de eventos e incidentes.
  - En los últimos 5 años ha habido interrupciones críticas que han impactado fuertemente las finanzas, imagen ante clientes e inversionistas.
- F. Como meta Corporativa, considera que el Tiempo Objetivo de Recuperación esperada debe ser medido en Horas.**
- G. No se conocen los resultados de la última prueba realizada al Sistema de Gestión de Continuidad del Negocio.**
- H. La dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estratégicas con los recursos necesarios, delega la responsabilidad a los Gerentes Generales y de Operaciones de cada empresa para disponer y garantizar los recursos.**

- I. El Presupuesto de Tecnología y Seguridad es menor al 1% con respecto a la facturación total del Grupo empresarial.**
- J. Se desconoce el Plan Estratégico de Proyectos de Tecnología y Seguridad, para la Implementación de Controles y Salvaguardas.**

### **2.3.3 Guia de Observación**

De acuerdo al **Anexo No. 6**, se tienen los resultados del Pre-Test realizado a los Riesgos y Amenazas de Ciberseguridad y el Tiempo Objetivo de Recuperación, en el contexto que se investiga.

Se debe destacar como criterios de observación que a veces se observan (AM) y que no se observan (N).

- F. Grado de conocimiento de las vulnerabilidades detectadas
- G. Continuidad y Disponibilidad son metas corporativas
- H. Arquitectura Tecnológica y de Seguridad considera los Riesgos y amenazas de Ciberseguridad
- I. interrupciones o incidentes en los últimos 5 años
- J. Tiempo objetivo de recuperación como meta corporativa
- K. Resultados de las últimas pruebas realizadas
- L. La dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estrategias con los recursos necesarios
- M. % del Presupuesto Operativo Anual de Ti y Seguridad
- N. Grado de conocimiento del Plan estratégico de TI, Seguridad y Continuidad.

## 2.4 Triangulación de los resultados de los instrumentos e identificación de los problemas

Con la aplicación del análisis realizado en el **Anexo No. 7**, a partir de los indicadores de las variables, se obtienen los problemas de acuerdo al diagnóstico realizado al objeto de estudio y campo de acción (Riesgo y Amenazas de Ciberseguridad, Tiempo Objetivo de Recuperación) .

**Indicador 1.1.1 y 1.1.2.** (Dimensión fuentes de riesgo) **P1.** Existe una contradicción entre la visión de la alta dirección y los ejecutivos de la organización en cuanto al grado de conocimiento y dominio de las fuentes de riesgo

**Indicador 1.2.1** (Dimensión Amenazas de Ciberseguridad) **P2.** Las prioridades de las amenazas de ciberseguridad no están alineadas entre la alta dirección y los ejecutivos de la organización.

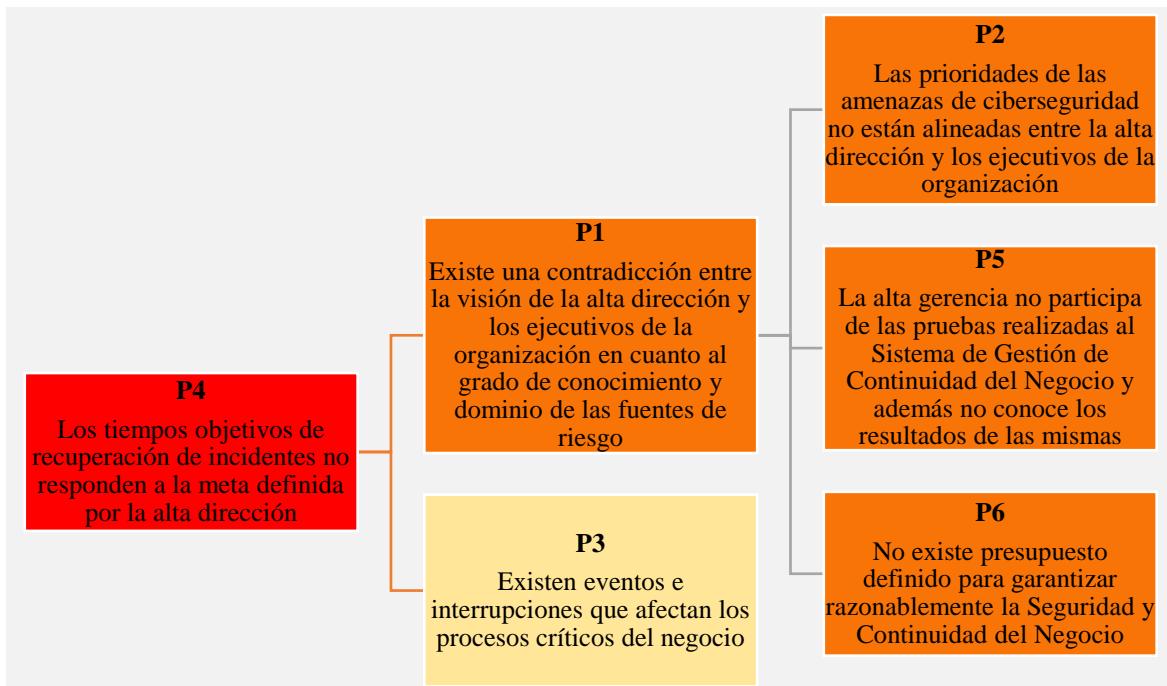
**Indicador 1.5.1** (Dimensión Evaluación) **P3.** Existen eventos e interrupciones que afectan los procesos críticos del negocio.

**Indicador 2.1.1** (Dimensión Política) **P4.** Los tiempos objetivos de recuperación de incidentes no responden a la meta definida por la alta dirección.

**Indicador 2.1.2** (Dimensión Política) **P5.** La alta gerencia no participa de las pruebas realizadas al Sistema de Gestión de Continuidad del Negocio y además no conoce los resultados de las mismas.

**Indicador 2.2.2** (Dimensión Compromiso y Apoyo de la Dirección) **P6.** No existe presupuesto definido para garantizar razonablemente la Seguridad y Continuidad del Negocio.

En la **Figura No. 18**, se muestran la jerarquización de los problemas.



**Figura No. 18.** Jerarquización de los problemas

Fuente: Elaboración Propia, 2019

Como problema crítico se identifica **P4:** Los tiempos objetivos de recuperación de incidentes no responden a la meta definida por la alta dirección, meta principal de la investigación Mejorar el Tiempo Objetivo de Recuperación, con la propuesta de solución alineada a la norma ISO 22301, se da solución a los problemas **P1, P2, P5 y P6.**

Dando solución al problema **P4**, aunque existan incidencias en **P3**, estas tendrán un mínimo impacto en los procesos de la organización.

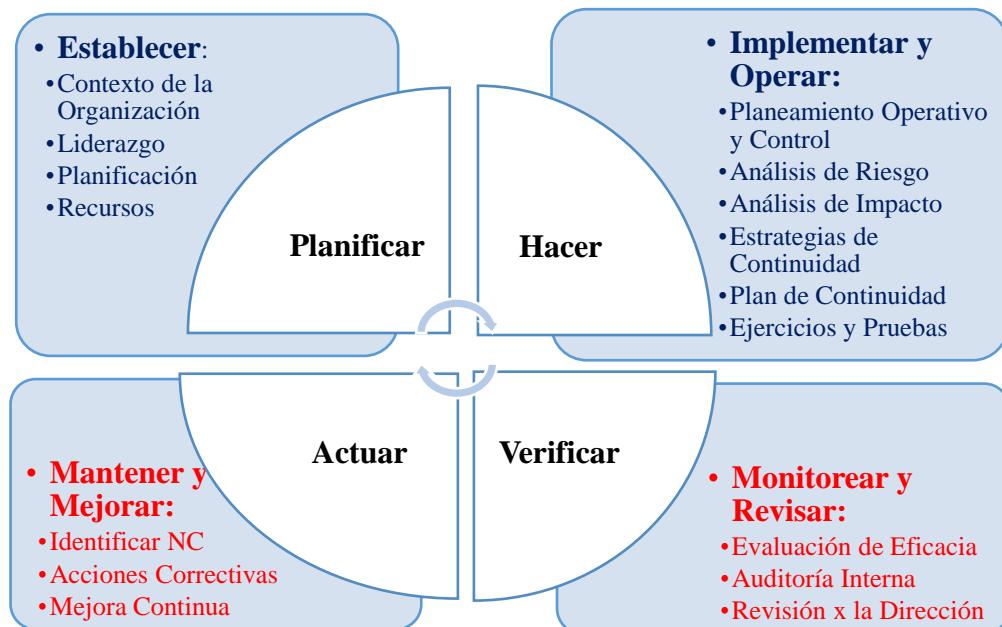
## CAPÍTULO III. PROPUESTA

En el presente capítulo se presenta, con un enfoque de sistemas, la estructura del Modelo de Gestión de Continuidad del Negocio para el contexto que se investiga, se desarrollan a partir de la aplicación de la norma ISO 22301 las diferentes cláusulas y sus objetivos: Contexto de la Organización, Liderazgo, Planificación, Recursos y Operación.

Finalmente se realiza la validación metodológica y estadística de la propuesta con la aplicación de la prueba Chi Cuadrada de Pearson.

### 3.1 Estructura del Modelo de Gestión de Continuidad del Negocio

En la figura **Figura No. 19**, se muestra la estructura del ciclo de mejora continua PHVA aplicado al modelo del Sistema de Gestión de Continuidad del Negocio.



**Figura No. 19.** Grafico del Ciclo de Mejora Continua PHVA aplicado al SGCN

Fuente: Elaboración Propia, 2019

En el

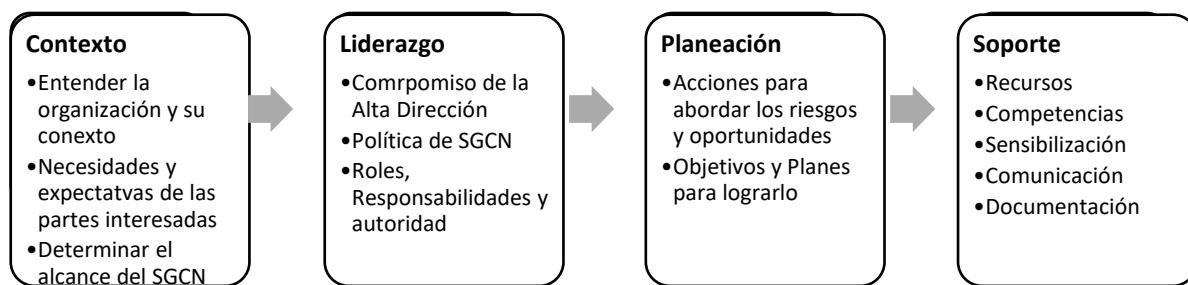
**Cuadro No. 8**, se detallan las actividades del ciclo de mejora continua PHVA aplicado al modelo de Gestión de Continuidad del Negocio.

**Cuadro No. 8.** Explicación del Modelo PHVA

Etapas	Actividades
<b>Planificar</b>	Entender a la organización, establecer la Política de Continuidad, objetivos, metas, responsables, controles, recursos, cronograma de actividades, procesos y procedimientos alineados a las Políticas, objetivos y estrategias de la organización
<b>Hacer</b>	Determinar e Implementar la estrategia de GCN, operar los Controles y PNPs de Respuesta para la Continuidad del Negocio
<b>Verificar</b>	Probar, Monitorear y Revisar el seguimiento y evaluación del desempeño de los controles, procesos y procedimientos contra la Política de Continuidad y de los objetivos del negocio Informar los resultados para su revisión Determinar y autorizar las acciones de remediación y mejora
<b>Actuar</b>	Mantener y mejorar Adopción de medidas correctivas basado en los resultados de la revisión por la dirección Revalorización del Alcance del SGCN, la Política y los Objetivos

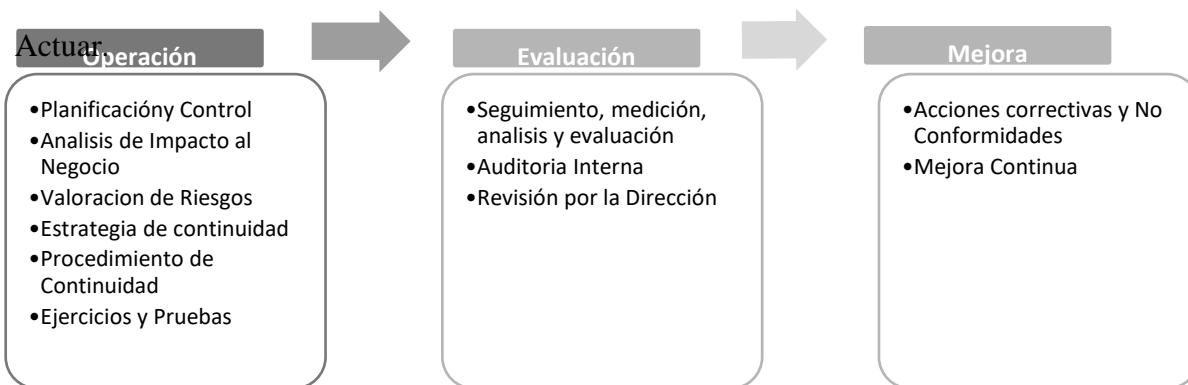
Fuente: Elaboración Propia, 2019

En la **Figura No. 20**, se muestra la estructura de trabajo del ciclo Planificar

**Figura No. 20.** Estructura de Trabajo del ciclo Planificar

Fuente: Elaboración Propia, 2019

En la **Figura No. 21**, se muestra la estructura de trabajo del ciclo Hacer-Verificar-

**Figura No. 21.** Estructura de Trabajo del ciclo Hacer-Verificar-Actuar

Fuente: Elaboración Propia, 2019

### Diferencia entre el Ciclo de vida de Gestión de Continuidad del Negocio (BCM) y el Sistema de Gestión de Continuidad del Negocio (BCMS)

**BCM:** Proceso de gestión holístico que identifica amenazas potenciales a la organización y sus impactos a la operación del negocio que esas amenazas, en caso realizarse, pudieran causar, y provee una estructura para construir resiliencia organizacional con la capacidad para la efectiva respuesta salvaguardando los intereses de las principales partes interesadas, reputación, marca y actividades que crean valor

**BCMS:** La parte del Sistema de Gestión general que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio

La Figura No. 22, detalla las diferencias entre el Ciclo de vida BCM y BCMS baso en el modelo PDCA (*Plan-Do-Check-Act*)

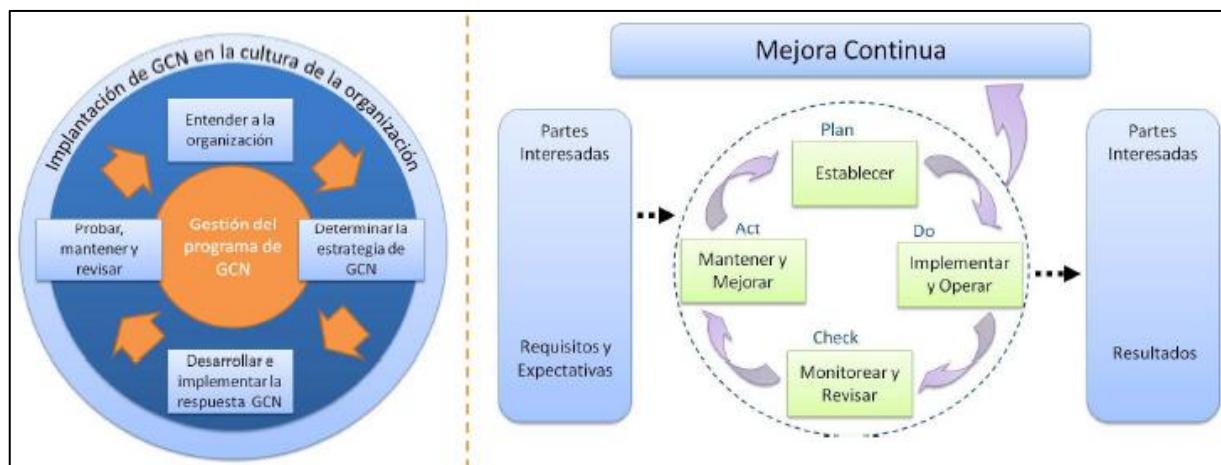


Figura No. 22. Ciclo de vida BCM y BCMS basado en el modelo PDCA

Fuente: Elaboración Propia, 2019

#### 3.1.1 Por qué la ISO 22301

En opinión del autor de la investigación, la norma ISO 22301 permite:

- Entender las necesidades y los objetivos de la empresa para establecer e implementar una Gestión de Continuidad del Negocio (BCM)
- Comprender las amenazas y vulnerabilidades de los servicios de Tecnologías de la información y comunicaciones
- Identificar y tratar los Riesgos y Amenazas de Ciberseguridad más importantes que afectan los procesos críticos de la empresa.
- Minimizar el Impacto al negocio mejorando el Tiempo de Recuperación Objetivo (RTO) tras un incidente mayor
- Implementar los controles y medidas necesarias para gestionar los incidentes y la capacidad de respuesta
- Establecer planes de recuperación y continuidad para asegurar de que la empresa no detenga sus procesos y servicios críticos durante momentos de crisis.
- Fomentar una mejor colaboración entre el personal de TI y los proveedores de servicios (internos y externos)
- Desarrollar y mejorar la competencia del personal mediante la ejecución y demostración de las pruebas del plan de continuidad
- Garantizar los niveles de servicios acordados a la alta dirección proporcionando un apoyo adecuado en el caso de una interrupción
- Ofrecer una confianza en la estrategia de continuidad del negocio a través de la vinculación de inversión en soluciones de TI y a las necesidades del negocio y asegurar que los servicios de TI están protegidos en un nivel apropiado dada su importancia para la organización

- Mejorar la reputación, imagen y eficiencia de la empresa; y obtener una ventaja competitiva a través de la habilidad demostrada para ofrecer continuidad en el negocio

### **3.2 Contexto de la Organización (Cláusula 4)**

#### **3.2.1 Descripción de la Organización**

##### **Estudio de la organización**

El presente trabajo considera los elementos característicos que definen la identidad de las empresas de Seguros del Grupo Empresarial de Inversiones Nacional Vida S.A., con la finalidad de identificar la estructura organizacional y comprender la función y la importancia de cada área para alcanzar los objetivos de la organización.

##### **Misión**

El Grupo Nacional Vida es una corporación empresarial de inversiones que asegura la sinergia entre sus empresas, velando por la rentabilidad y valor agregado de sus accionistas, contribuyendo al desarrollo económico del país.

##### **Visión**

Ser la corporación boliviana con excelencia en gestión empresarial, más confiable, solvente, sólida, rentable, con proyección internacional y responsabilidad social.

El Grupo Empresarial de Inversiones Nacional Vida S.A está conformado por 4 compañías, cada una líder en su rubro.

**Nacional Seguros Vida y Salud:** Compañía líder en seguros de vida, mantiene un 39% de participación de mercado. Una de las claves del éxito para la compañía es la construcción de relaciones de largo plazo con sus clientes buscando crear sinergias en el día a día.

**Nacional Seguros Patrimoniales y Fianzas:** Brinda servicios en seguros generales como ser incendio, automotores, aeronavegación agrícola, transporte, fianza, responsabilidad civil, seguros industriales, petroleros y bancarios entre otros.

**Conecta:** Empresa pionera en el desarrollo de servicios al cliente, dedicada a actividades de *Contact Center*, representaciones y redes de servicios como asistencia al viajero, vehicular y profesional.

**Tecorp:** Ofrece soluciones integrales, innovadoras, cubriendo necesidades inmediatas y brindando tercerización informática y tecnológica.

### **Política de Calidad**

Nacional Seguros, cuenta con un marco de Gestión de Calidad, definido por la misión corporativa y dirección estratégica

A continuación, se describe la política de Calidad, las directrices y el compromiso que asume toda la organización:

- Ser parte de los momentos importantes de la vida de nuestros clientes, individuales y corporativos, asesorándoles y brindándoles soluciones integrales pensando en su comodidad y tranquilidad.
- Mejorar constantemente nuestros productos y servicios, procesos y sistema de gestión de la calidad, en el marco de la normativa legal vigente.

### **Alcance del Sistema de Gestión de Calidad**

El alcance del Sistema de Gestión de Calidad, incluye todos los procesos de negocio:

- Desarrollo, diseño, comercialización, elaboración y servicio posventa de seguros.

### **Estrategia de la organización**

- Diferenciación de servicios

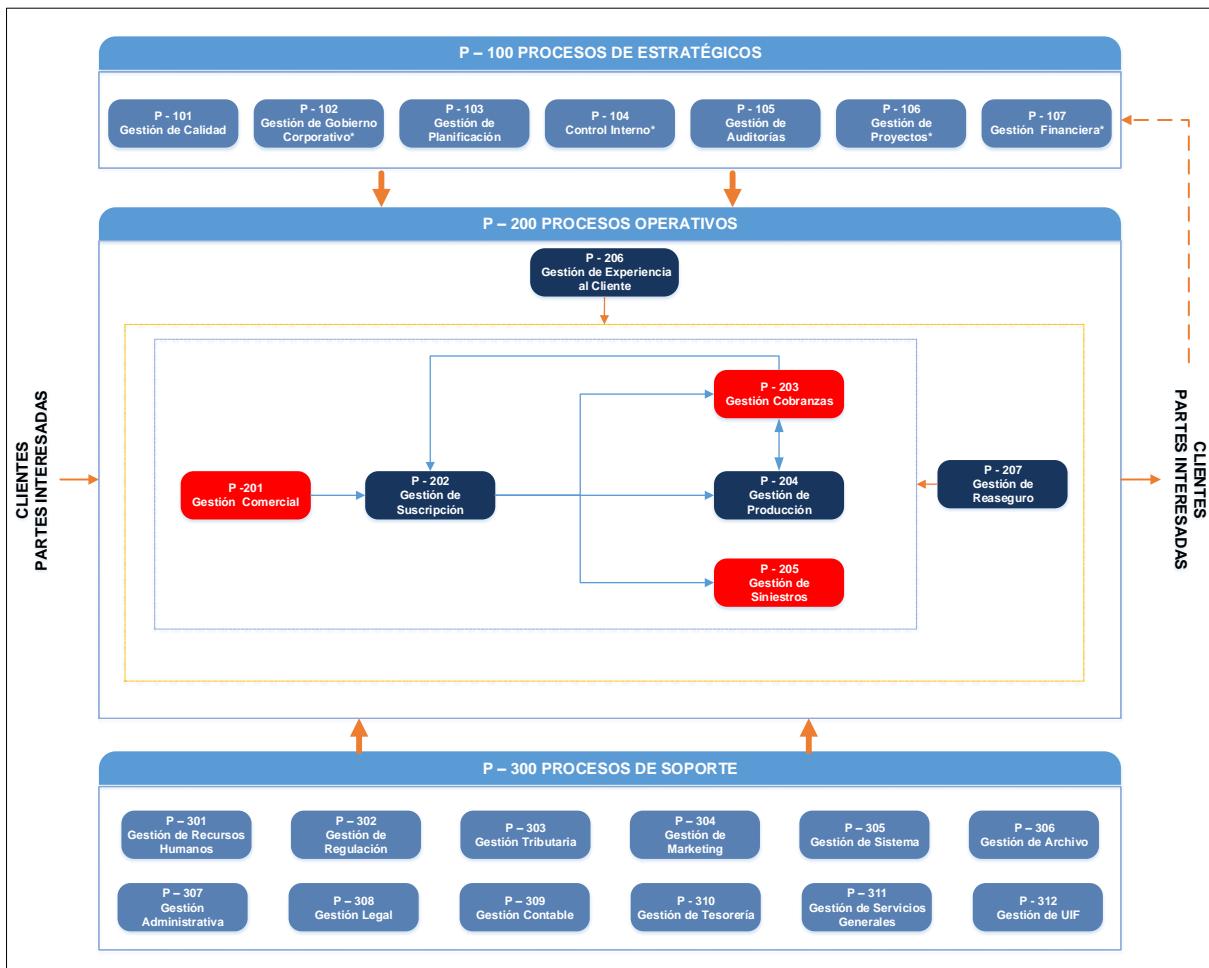
- Disminuir los costos operativos
- Mejorar la calidad de los servicios
- Mejorar las ventas y el margen de utilidad
- Desarrollo o adquisición de Nuevos Sistemas

### **Ámbito del Negocio**

Como marco de análisis se ha tomado el Mapa de Procesos de las empresas de Seguros objeto de estudio, definiendo como dominio el Sistema de Información que cubre los siguientes procesos.

- **Procesos Operativos Críticos**
  - Gestión Comercial
  - Gestión de Cobranzas
  - Gestión de Siniestros
- Procesos Estratégicos
- Procesos Operativos no críticos
- Procesos de Soporte
- Documentos
  - Documento de Uso Público
  - Documento de Uso Interno
  - Documentos Confidenciales
  - Documento Secretos

En la **Figura No. 23**, se observa el mapa de procesos de las empresas de seguros, agrupados por los siguientes macro procesos:



**Figura No. 23.** Mapa de procesos

Fuente: SGC Nacional Seguros, 2018

## Ámbito Tecnológico

- Equipamiento Tecnológico

Todos los aspectos referentes a la infraestructura tecnológica son provistos por la empresa TECorp, que forma parte del Grupo Nacional Vida. Si bien la infraestructura tecnológica implementada por TECorp abarca todas las ciudades donde Nacional Seguros tiene presencia, el programa de gestión de continuidad del negocio abarcará solamente aquellos sistemas e infraestructura que están relacionados con el ámbito de los procesos críticos definidos.

La infraestructura tecnológica que participará del análisis es la siguiente:

- Dominios
  - [B] Capa de Negocio
  - [SI] Servicios Internos
  - [EQ] Equipamiento
  - [SS] Servicios Subcontratados
  - [L] Instalaciones
  - [P] Personal
- Grupos
  - Procesos
  - Documentos
  - [SW] Aplicaciones
  - [HW] Equipos
  - [COM] Comunicaciones
  - [AUX] Auxiliares
- [SW] Aplicaciones

En el **Cuadro No. 9**, se detallan los sistemas informáticos que intervienen en todo el proceso de análisis.

**Cuadro No. 9.** Sistemas Informáticos

Sistema	Descripción del Sistema	NSVS	NSPF	TECorp	Conecta
<b>VidaFlexible</b>	Sistema de Gestión Seguros de Personas a largo plazo.	X			
<b>eLife</b>	Sistema de Gestión de Seguros de Vida a Corto Plazo (Seguro de Desgravamen, Accidentes Personales, Vida en Grupo, Salud Internacional, UIF)	X			
<b>eSalud</b>	Sistema de Gestión de Seguros de Salud con cobertura Nacional.	X			

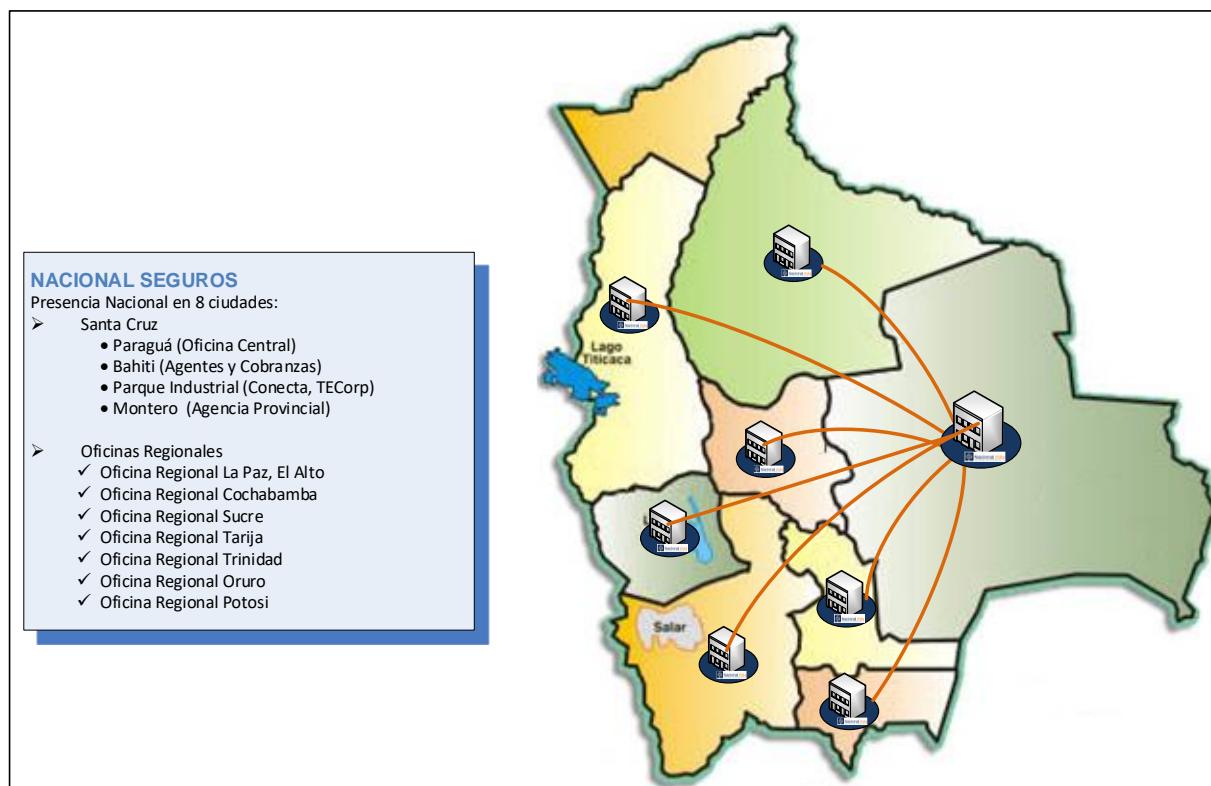
Sistema	Descripción del Sistema	NSVS	NSPF	TECorp	Conecta
<b>eProperty</b>	Sistema de Gestión de Seguros Patrimoniales (Cotización, inspección, Emisión de Pólizas, Mantenimiento, Siniestros)		X		
<b>eDesk</b>	Sistema de Gestión de Mesa de ayuda (Apertura de tickets, Asignación, Priorización)	X	X	X	X
<b>Uponsoft</b>	Sistema de Gestión de Planificación de Recursos Empresariales, que proporciona los módulo de contabilidad, caja, tesorería, bancos, cxc, cxp	X	X	X	X
<b>S! Personal</b>	Sistema de administración de Planillas de Sueldos, Vacaciones de Recursos Humanos.	X	X	X	X

Fuente: Elaboración Propia, 2018

- [L] Instalaciones (Ámbito Geográfico)

Nacional Seguros tiene oficinas distribuidas en varias ciudades de Bolivia, los sistemas informáticos de la compañía se brindan bajo un esquema centralizado, es por ello que este análisis se enfocará en la ciudad de Santa Cruz, principalmente en la oficina central.

En la **Figura No. 24**, se muestra la distribución de las oficinas y agencias regionales en el ámbito nacional.



**Figura No. 24.** Distribución de las oficinas y agencias regionales en Bolivia

Fuente: Elaboración Propia, 2018

En el **Cuadro No. 10**, se detallan los cargos que son parte de las fuentes de información

**Cuadro No. 10.** Fuentes de Información

Código	Descripción del Puesto	Unidad de Dependencia
GG	Gerente General	NSVS/NSPF CONECTA/TECORP
GFC	Gerente Financiero Corporativo	GNI
AI	Auditor Interno	GNI
SGRH	Sub Gerente Corporativo de RRHH	GNI
LEG	Asesor Legal	GNI
SG	Servicios Generales	GNI
GNO	Gerente Nacional de Operaciones	NSVS/NSPF
RM	Gerente de Riesgo	NSPF
GTIS	Gerente de TI y Seguridad	TECORP
GDS	Gerente de Desarrollo de Software	TECORP
JIT	Jefe de IT	TECORP
DBA	Administrador de Bases de Datos	TECORP
ATEL	Administrador de Telecomunicaciones	TECORP

Fuente: Elaboración Propia, 2018

### 3.2.2 Necesidades y expectativas de las partes interesadas

#### Restricciones que afectan a la Organización

Para que la organización pueda cumplir sus objetivos estratégicos en un plazo determinado, y que estos objetivos sean consistentes con la misión y visión de la empresa, se definen las siguientes restricciones:

##### 1) Restricciones de la autoridad de supervisión

Decisiones gubernamentales mandatorias relacionadas con la orientación operativa y estratégica, en el **Anexo No. 8**, se detallan las restricciones de la autoridad de supervisión **ASFI** (Autoridad de Supervisión del Sistema Financiero), en el **Anexo No. 9**, se detallan las restricciones de la autoridad de supervisión **APS** (Autoridad de Fiscalización y Control de Pensiones y Seguros).

##### 2) Restricciones de naturaleza estratégica

Restricciones originadas en los cambios planificados en la estructura de la organización (Planes estratégicos, Planes operativos)

En el **Cuadro No. 11**, se definen las líneas estratégicas de negocios de Nacional Seguros y el lineamiento estratégico genérico para las líneas de negocio.

**Cuadro No. 11.** Lineamiento estratégico

EMPRESA	NSVS	NSPF
<b>Líneas estratégicas</b>	Seguros vida individual	Seguro individuales
	Seguros de salud	Seguros fianzas y cauciones
	Seguros vida corporativa	Seguros corporativos
	Seguros masivos	Seguros masivos
<b>Lineamiento estratégico genérico</b>	Diferenciación	Diferenciación

**Fuente:** Elaboración Propia, 2018

### 3) Restricciones Territoriales

Presencia Nacional en 8 ciudades:

- Santa Cruz
  - Paraguá (Oficina Nacional)
  - Montero (Agencia Provincial)
  - Bahití (Agentes y Cobranzas)
- Oficina Regional La Paz (Oficina Regional)
  - Oficina Regional El Alto (Oficina Regional)
- Oficina Regional Cochabamba (Oficina Regional)
- Oficina Regional Sucre (Oficina Regional)
- Oficina Regional Tarija (Oficina Regional)
- Oficina Regional Trinidad (Oficina Regional)
- Oficina Regional Potosí (Oficina Regional)
- Oficina Regional Oruro (Oficina Regional)

### 4) Restricciones del clima político y económico

El funcionamiento de la organización se ve afectado por los siguientes eventos específicos:

- **Huelgas:** Afecta la paralización de las operaciones normales de cobranzas.
- **Paros cívicos:** Paralizan las operaciones normales de comercialización y cobranza lo que tiene un efecto directo en los ingresos programados de la compañía.
- **Conmoción social:** Afecta los puntos antes mencionados, la estructura física de la empresa, dependiendo de los lugares donde se genere.

- **Crisis Nacional (económica):** Afecta en las proyecciones de venta y cobranza porque reduce la capacidad de pago de los clientes e inversiones.
- **Crisis Internacionales (económica):** Afecta a reaseguradores, que son los principales proveedores operacionales, afecta a las inversiones.

Se establece que los siguientes servicios deberían continuar incluso durante la declaración de una crisis grave:

- Gestión Comercial
- Gestión de Cobranzas
- Gestión de Siniestros

## **5) Restricciones estructurales**

Todos los aspectos referentes a la infraestructura tecnológica son provistos por la empresa TECORP, que forma parte del Grupo Empresarial de Inversiones Nacional Vida.

El Gerente de TI y Seguridad Informática se reporta ante la alta gerencia de la empresa, además participa activamente del comité de Tecnología y Seguridad de Nacional Seguros.

## **6) Restricciones funcionales**

Atención en oficinas de lunes a viernes de 08:30 a 12:30 y 14:30 a 18:30 para personal operativo de atención al cliente interno o externo (Exceptuando paros cívicos y feriados)

Atención por *Call Center* 7x24x365 para atención de siniestros.

Personal ejecutivo sin horario definido.

## **7) Restricciones relacionadas con el personal**

Esta restricción está ligada al nivel de responsabilidad del cargo, tipo de contratación, calificación requerida para el puesto, destrezas, aptitudes, nivel de instrucción,

entrenamiento, toma de conciencia sobre riesgos, seguridad, continuidad, calidad, motivación y disponibilidad del personal, entre otros.

#### **8) Restricciones del calendario de la organización**

Restricción del resultado de una política nacional, que impone fechas determinadas:

- Fecha de cierre fiscal: 31 de diciembre de cada año
- Fecha de envío de información al ente regulador: de acuerdo a la matriz adjunta en los

#### **Anexo No. 8 y Anexo No. 9**

#### **9) Restricciones relacionadas con los métodos**

Restricción de control para los aspectos de seguridad, tales como:

- Adendas de seguridad en contratos (Obligatoriedad de Firma)
- Conformidad de la política de seguridad: FRM Declaración de obligaciones de seguridad
- Especificaciones de productos: Procedimiento de creación de productos
- Desarrollo de *software*: De acuerdo a políticas y procedimientos.

#### **10) Restricciones de presupuesto**

Los controles recomendados para la Seguridad y Continuidad deben estar basados en:

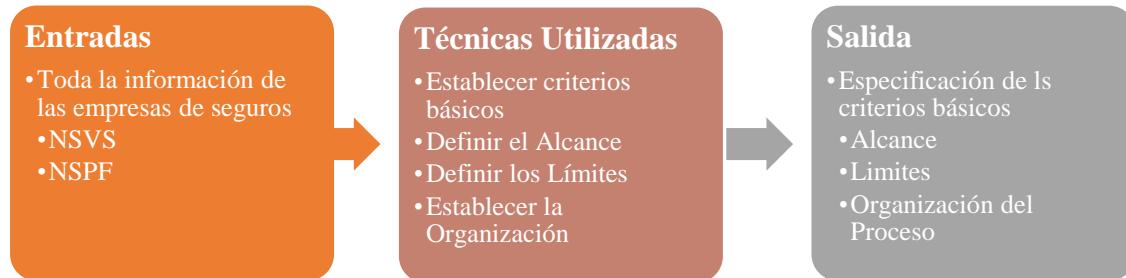
- Plan estratégico quinquenal
- Alineamiento estratégico
- Presupuesto anual
- Casos de Negocio (Análisis costo – beneficio)

## 11) Criterio de Cumplimiento

- La etapa de implementación deberá ser ejecutada entre las gestiones 2018 y 2019 y el proyecto deberá estar completado en la Gestión 2019, cubriendo las etapas de desarrollo, ejecución y adecuación del plan del proyecto.
- El proyecto se dará como completado, una vez que todos los objetivos han sido cumplidos, conjuntamente con el entrenamiento al personal y realizadas las pruebas de simulación de manera satisfactoria, el Plan de continuidad es estandarizado, revisado y aprobado por la alta dirección y mantenido bajo el proceso de mejora continua.

### 3.2.3 Alcance del Modelo de Gestión de Continuidad del Negocio

La **Figura No. 25**, muestra el proceso para definir el alcance y límite del contexto de estudio.



**Figura No. 25.** Proceso para definir el alcance y límite del contexto de estudio.

Fuente: Elaboración Propia, 2019

### Alcance Empresarial

El modelo de Gestión de Continuidad propuesto cubre los procesos críticos de las empresas de Seguros, que dependen de tecnologías de información y comunicaciones.

- **Áreas de la empresa:**

- Gerencia General

- Gerencia Nacional de Operaciones
- Auditoria Interna
- Gerencia de TI y Seguridad Informática
- Gerencia de Desarrollo de *Software*
- Recursos Humanos
- Calidad y Procesos
- **Dominios**

El desarrollo del proyecto de Gestión de Continuidad, en la Fase de Análisis de Riesgo y Análisis de Impacto, se centra en los dominios, definidos en el **Cuadro No. 12.**

**Cuadro No. 12.** Dominios de Trabajo

Código	Nombre del Dominio	Unidad de Dependencia
Base	Dominio Principal (base Común)	NSVS, NSPF, CONECTA, TECorp
SC01	Sitio Central SCZ (Paraguá)	NSVS, NSPF
SC02	Sitio Alterno (P.I)	NSVS, NSPF, CONECTA, TECorp
AL01	Agencias Locales	BAHITI
AR01	Agencias Regionales	NSVS, NSPF

Fuente: Elaboración Propia, 2018

- **Límites**

El proyecto define los siguientes límites alcanzables para satisfacer la factibilidad técnica, operativa y de presupuesto.

- Procesos Operativos (determinados como Críticos para la organización)
  - i. Gestión de Cobranzas
  - ii. Gestión Comercial
  - iii. Gestión de Siniestros

- **Alcance del Modelo de Gestión de Continuidad del Negocio**

El modelo de SGCN (BCMS), en conformidad con los requisitos de la norma considera:

- Planear (Establecer): Entender a la Organización
- Hacer (implementar y Operar): Determinar la Estrategia de GCN
- Verificar (Monitorear y Revisar): Desarrollar e implementar la respuesta GCN
- Actuar (Mantener y Mejorar): Probar, Mantener y revisar

Para efecto de elaboración del Modelo de Gestión de Continuidad del Negocio (BCM) sólo se consideran las siguientes fases:

**Planificar** (Establecer)

- Contexto de la Organización
- Liderazgo
- Planificación
- Recursos

**Hacer** (Implementar y Operar)

- Planeamiento Operativo y Control
- Análisis de Riesgo
- Análisis de Impacto
- Estrategias de Continuidad
- Plan de Continuidad
- Ejercicios y Pruebas

Las siguientes fases no se consideración como parte de la elaboración del Modelo de Gestión de Continuidad del Negocio, ya que son parte de un Sistema de Gestión de Continuidad del Negocio (BCMS)

**Verificar** (Monitorear y Revisar)

- Evaluación de la Eficacia
- Auditoría Interna
- Revisión por la Dirección

**Actuar** (Mantener y Mejorar)

- Identificar No Conformidades
- Acciones Correctivas
- Mejora Continua

### **3.3 Liderazgo (Cláusula 5)**

#### **3.3.1 Responsabilidades y Empoderamiento**

##### **Compromiso de la Alta Dirección**

A través del presente, el [Máxima Autoridad Empresarial] declara que en todos los elementos de la implementación del SGCN se contará con el apoyo de los recursos adecuados para lograr todas las metas y objetivos establecidos en la Política de Gestión de Continuidad del Negocio, como también para cumplir con todos los requisitos identificados.

El [Máxima Autoridad Empresarial] y los Directores de la empresa [nombre de la empresa] nos comprometemos a:

- Disponer de los recursos necesarios en presupuesto para implementar los controles, políticas y procedimientos para mejorar el Sistema de Gestión de continuidad del negocio

- Lograr la satisfacción de nuestros clientes, accionistas y de todas las partes interesadas
- Mejorar de forma continua nuestros procesos organizacionales, estableciendo los objetivos de continuidad con el fin de optimizar el Sistema de Gestión
- Implementar un programa de capacitación y sensibilización orientados a educar, capacitar y comprometer a todos los funcionarios de la empresa [nombre de la empresa] para fortalecer el Sistema de Gestión de Continuidad

Firmado Por : [Máxima Autoridad Empresarial]

Fecha : [xx/xxx/yyyy]

Versión : [1.0]

### **Política para la Gestión de Continuidad del Negocio (BCM)**

El objetivo de la gestión de la continuidad del negocio es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían tener sobre las operaciones de negocios; como también proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

La Gestión de Continuidad de la empresa [nombre de la empresa], debe estar basado en los principios de confidencialidad, integridad y disponibilidad de la información y de los sistemas que soportan los procesos críticos del negocio, así como la necesidad de crear valor como parte del Buen Gobierno Corporativo.

Con la implementación del Modelo de Gestión de Continuidad del Negocio (BCM), [nombre de la empresa] desea cumplir con la misión y visión organizacional, apoyar los objetivos estratégicos y los Procesos operativos determinados como críticos para la organización:

- Gestión Comercial
- Gestión de Cobranzas
- Gestión de Siniestros.

La Gestión de la Continuidad del Negocio (BCM) debe garantizar que los procesos mencionados anteriormente se recuperarán a un nivel predefinido.

Todas las actividades relacionadas con esos productos y servicios están detalladas en la Estrategia de continuidad del negocio definida en el Plan de Dirección del Proyecto de Gestión de Continuidad del Negocio (BCM).

Esta Política se aplica a todo el Modelo de Gestión de la Continuidad del Negocio (BCM), de la empresa [nombre de la empresa].

Los usuarios de este documento son todos los funcionarios de [nombre de la empresa], como también todos los proveedores y socios que cumplen alguna función en la Gestión de Continuidad del Negocio (BCM).

La Gestión de la Continuidad del Negocio se implementa conforme a los requisitos legales, normativos, contractuales, definidos por:

- Autoridad de Supervisión del Sistema Financiero (ASFI)
- Autoridad de Fiscalización y Control de Pensiones y Seguros (APS)
- Bolsa Boliviana de Valores (BBV)

El marco de referencia para la Gestión de Continuidad de riesgos debe estar fundamentado en mejores prácticas internacionales y ser adaptada a su tamaño, naturaleza, complejidad, cultura organizacional, siendo el Tiempo Objetivo de Recuperación (RTO) y el nivel de aceptación o tolerancia al riesgo aprobados por la Alta Dirección.

El marco para la Gestión de Continuidad debe incluir:

- Realizar un análisis sobre los riesgos a los que se expone la empresa
- Realizar un análisis del impacto de los procesos críticos del negocio
- Definir una estrategia de continuidad
- Implementar la estrategia y controles necesarios para garantizar la continuidad del negocio
- Realizar los ejercicios, entrenamientos y pruebas

**Documentos de Referencia:**

- Norma ISO 22301
- Norma BS 25999-2
- Norma ISO/IEC 27001
- PL-404 Plan de dirección del proyecto de Gestión de la Continuidad del Negocio (BCM)

Se debe establecer canales de comunicación orientados a formalizar un vínculo con las partes interesadas

Identificar y dar respuesta a sus necesidades a través de la puesta en marcha del Modelo de Gestión de continuidad del negocio.

Disponer de controles internos integrales que ayuden a la alta dirección y a la administración a controlar y evaluar la idoneidad y eficacia de las políticas, procedimientos del Modelo de Gestión de Continuidad del negocio.

Se deberá identificar y tratar aquellos riesgos que puedan afectar la capacidad de operación o entrega de servicios, considerando las fuentes internas y externas; así como la naturaleza cambiante del entorno.

Se deberá contar con procedimientos prácticos y claros que permitan anticipar, detectar, registrar, analizar, resolver y aprender de los incidentes, evitando su reincidencia.

Las funciones y responsabilidades frente a la continuidad del negocio, deberán estar claramente definidas y ser conocidas dentro de la empresa [nombre de la empresa]

Se deberá establecer mecanismos apropiados a su naturaleza, que permitan monitorear, medir, y reportar el desempeño de la Gestión de continuidad del Negocio (BCM), el RTO de la ejecución de las pruebas, el RTO de las activaciones del sistema por causa de incidentes mayores y el nivel de exposición al riesgo; así como la eficacia de las acciones adoptadas por parte de la Gerencia General para el tratamiento de las mismas.

Las acciones para cumplir estos objetivos serán determinadas en el Plan de tratamiento de riesgos, Plan de preparación para Continuidad del negocio, Procedimiento para medidas correctivas y Revisión por parte de la dirección.

El [Gerente de TI y Seguridad] es el responsable de definir los objetivos para todo el Modelo de Gestión de Continuidad (BCM) y el método para medir el cumplimiento de los mismo

El [Gerente de TI y Seguridad] tiene la responsabilidad de revisar los objetivos al menos una vez por año o cuando ocurran cambios significativos, cualquier modificación o solicitud de excepción a la misma, será analizada y puesta a consideración del Comité de Tecnología, Seguridad y Continuidad de la empresa [nombre de la empresa].

La [alta dirección] debe revisar el Modelo de Gestión de Continuidad del Negocio (BCM) al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión. El objetivo de la revisión por parte de la dirección

es establecer la conveniencia, adecuación y eficacia del Modelo de Gestión de Continuidad del Negocio (BCM).

[nombre de la empresa] medirá lo siguiente:

- Si los objetivos definidos de acuerdo a esta Política son cumplidos: al menos una vez por año, generalmente antes de la Revisión por parte de la dirección.
- Efectividad y adecuación de los planes de continuidad del negocio: según la frecuencia definida en el mismo Plan de continuidad del negocio.
- El [Auditor Interno] elaborará un informe con los resultados de la medición, mientras que el análisis y evaluación de los resultados se realizará en la Revisión por parte de la dirección.

A través del presente, el [Máxima Autoridad Empresarial] declara que en todos los elementos de la implementación del Modelo de Gestión de Continuidad del Negocio (BCM) se contará con el apoyo de los recursos adecuados para lograr todas las metas y objetivos establecidos en esta Política, para cumplir con todos los requisitos de la norma como también con los objetivos propuesto por [nombre de la empresa].

Firmado Por : [Máxima Autoridad Empresarial]

Fecha : [xx/xxx/yyyy]

Versión : [1.0]

### **Roles y responsabilidades del representante de la Dirección**

El Representante de la dirección ante el Modelo de Gestión de Continuidad del Negocio (BCM), tendrá la responsabilidad de:

- Proponer la estrategia, estructura, programas y planes para la Gestión de Continuidad del Negocio (BCM), alineados a la estrategia de la organización
- Proponer la política, normas, procedimientos, metodologías, técnicas y herramientas a ser utilizadas para la gestión efectiva de la Continuidad del Negocio, asegurando su mantenimiento y actualización
- Verificar el cumplimiento de las políticas, procedimientos y metodologías establecidas por la organización para el Modelo de Gestión de Continuidad del Negocio (BCM).
- Monitorear el Modelo de Gestión de Continuidad del Negocio (BCM) y el perfil de riesgo establecido por la organización, con base a indicadores de eficiencia y eficacia aprobadas por la Alta Dirección
- Reportar los cambios en el entorno que puedan afectar al logro de los objetivos estratégicos, informando cualquier desviación y las medidas correctivas tomadas
- Elaborar con destino a los principales interesados, informes periódicos sobre los eventos más relevantes que inciden en el correcto funcionamiento del Sistema y cumplimiento de los planes de acción
- Informar a la Dirección Ejecutiva sobre el desempeño del Sistema de Gestión de Continuidad y de cualquier necesidad de mejora
- Asegurarse de que se establezcan, implementen, mantengan y mejoren los procesos necesarios para el Modelo de Gestión de Continuidad del Negocio (BCM) cumpliendo los requisitos de la norma ISO 22301.
- Elaborar y controlar la documentación del Modelo de Gestión de Continuidad del Negocio (BCM)
- Fortalecer la cultura de la organización para la Gestión de Continuidad del Negocio

- Asegurar el cumplimiento legal, reglamentario y contractual relacionado con la Gestión de continuidad  
Gestionar la comunicación con las partes interesadas (Auditores externos, autoridades y organismos de certificación).

**Autoridad y empoderamiento****COMUNICACIÓN INTERNA**

-GG0001/2019

A : XXXX CARGO: [Gerente de TI y Seguridad]

DE : XXXX CARGO: [Máxima Autoridad Empresarial]

REF: DESIGNACIÓN DE REPRESENTANTE DE LA DIRECCIÓN ANTE EL SGCN

Fecha : xx/xxxx/xxxx

Estimado Señor

Mediante la presente y a tiempo de saludarlo, comunico que Ud. ha sido designado para ser el representante de la dirección y responsable del Modelo de Gestión de Continuidad de la Corporación, basado en la norma ISO 22301.

En este sentido, contamos con su compromiso para el logro de los objetivos en este importante proyecto, le deseamos éxito en su desempeño

Firmado Por : [Máxima Autoridad Empresarial]

Fecha : [xx/xxx/xxxx]

Versión : [1.0]

### 3.4 Planificación (Cláusula 6)

#### 3.4.1 Direccionar Riesgos, Oportunidades

##### Criterios de Seguridad

De acuerdo al **Cuadro No. 13**, la organización establece los siguientes criterios de seguridad, siendo la Disponibilidad, Integridad y Confidencialidad de los datos requeridos por la norma.

**Cuadro No. 13.** Criterios de Seguridad

Código	Nombre de la Dimensión	Estado
[ D ]	Disponibilidad	Requerido
[ I ]	Integridad de los datos	Requerido
[ C ]	Confidencialidad de los Datos	Requerido
[ A ]	Autenticidad de los usuarios e información	No Requerido
[ T ]	Trazabilidad del Servicio y de los Datos	No Requerido

Fuente: Elaboración Propia, 2019

##### Criterios de Impacto

Con el fin de determinar el grado de daño o pérdida para la organización, causados por un evento de seguridad de la información, se definen los siguientes criterios de impacto:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (pérdida de confidencialidad, integridad y disponibilidad).
- Pérdida del negocio (Operativa) y del valor financiero.
- Daños a la imagen y la reputación.
- Incumplimiento con los requisitos legales, reglamentarios y contractuales.

### **3.4.2 Objetivos y planes para Alcanzarlos**

#### **Objetivos del Modelo de Gestión de Continuidad del Negocio**

- Gestionar los Riesgos y Amenazas de Ciberseguridad
- Mejorar el Tiempo Objetivo de Recuperación de los Procesos Críticos del Negocio
- Garantizar los recursos para implementar los controles necesarios
- Reducir los costos de incidentes evitando pérdidas por multas y sanciones legales
- Fortalecer la imagen y reputación de la empresa ante sus accionistas, clientes, funcionarios internos y en especial ante la competencia
- Alinear las iniciativas de Continuidad con la estrategia Organizacional mejorando el Clima Laboral y la Satisfacción de los Clientes.
- Optimizar la productividad de las personas y de los procesos de negocio soportado por una metodología de buenas prácticas de Gestión de Continuidad del Negocio
- Capacitar, sensibilizar y comprometer a todos los funcionarios de la empresa Con la implementación del Modelo de Gestión de Continuidad del Negocio, [nombre de la empresa] desea cumplir con la misión y visión organizacional, apoyar los objetivos estratégicos y los Procesos Operativos determinados como críticos para la organización:

  - Gestión Comercial
  - Gestión de Cobranzas
  - Gestión de Siniestros.

La Gestión de la Continuidad del Negocio debe garantizar que los procesos mencionados anteriormente se recuperarán a un nivel predefinido.

[nombre de la empresa] medirá lo siguiente:

- Si los objetivos definidos son cumplidos: al menos una vez por año, generalmente antes de la Revisión por parte de la dirección.
- Efectividad y adecuación de los planes de continuidad del negocio: según la frecuencia definida en el mismo Plan de continuidad del negocio.
- El [Auditor Interno] elaborará un informe con los resultados de la medición, mientras que el análisis y evaluación de los resultados se realizará en la Revisión por parte de la dirección.

Al evaluar la efectividad y adecuación del Modelo de Gestión y Continuidad del negocio, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y proveedores/socios que no conocen la Política de Gestión de Continuidad del Negocio.
- No-conformidad de Gestión de la Continuidad del Negocio con disposiciones legales, obligaciones contractuales y demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del Modelo de GCN (BCM).
- Responsabilidades ambiguas para la implementación del Modelo de GCN (BCM).

### **3.5 Recursos (Cláusula 7)**

La organización debe determinar y proporcionar los recursos necesarios para establecer, mantener, mejorar el SGCN

La utilización de los recursos incluye al personal, ya que pueden necesitar formación, comunicación. esto se debe apoyar con información documentada.

### **3.5.1 Competencia**

#### **Prácticas Profesionales**

Como parte de los esfuerzos continuos de la empresa [nombre de la empresa], para mantener la relevancia y utilidad del Modelo de gestión de Continuidad del negocio, se definen las habilidades, competencias y las certificaciones profesionales que se requieren para el personal que forma parte del equipo de Continuidad y Respuesta a Incidentes:

#### **Conocimientos y Experiencia**

- Conocimientos avanzados en TIC
- Asimilación de nuevas tecnologías emergentes
- Conceptos de Metodologías para la Gestión de Riesgos
- Amenazas de Ciberseguridad
- Cadena de Suministro empresarial
- Gestión de Proyectos y Programas de Continuidad
- Técnicas de Recuperación de Desastres
- Conocimientos de Estrategias de Continuidad
- Bases de Datos de información
- Redes y comunicaciones
- Seguridad e integridad de la información
- Prácticas empresariales
- Gerencia de proyectos
- Inglés (lectura y redacción)

## **Habilidades**

- Trabajo en equipo, Planeación y organización, Liderazgo, Negociación, Comunicación, Iniciativa, Creatividad e Innovación

## **Certificaciones Internacionales Profesionales**

### **Nivel Inicial:**

- ITIL Foundation (Information Technology Infrastructure Library)
- MTA (Microsoft Technology Associate)
- VCA (VMware Certified Associate)

### **Certificaciones Nivel Intermedio:**

- CCNA (Cisco Certified Network Associate)
- MCSA (Microsoft Certified Solutions Associate)
- CEH (Certified Ethical Hacker)
- OPST (OSSTMM Professional Security Tester)
- VCP (VMware Certified Professional)

### **Certificaciones Nivel Avanzado:**

- CISA (Certified Information Systems Auditor)
- LA ISO 9001 Auditor Líder del Sistema de Gestión de Calidad
- LA ISO 27001 Auditor Líder del Sistema de Gestión de Seguridad de la Información
- LA ISO 22301 Auditor Líder del Sistema de Gestión de Continuidad del Negocio
- LA ISO 31000 Auditor Líder de Gestión de Riesgos
- CCNP (Cisco Certified Network Professional)
- MCSE (Microsoft Certified Solutions Expert)
- PMP (Project Management Professional)

- RHCE (Red Hat Certified Engineer)
- VCAP (VMware Certified Advanced Professional)

#### **Certificaciones Nivel Experto:**

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- RHCA (Red Hat Certified Architect)
- VCDX (VMware Certified Design Expert)
- CCIE (Cisco Certified Internetwork Expert)

#### **3.5.2 Toma de conciencia**

Las personas que realizan trabajos para la organización deben ser consistentes de cumplir con la Política de Seguridad y Continuidad de la empresa:

#### **Declaración del cumplimiento de las Obligaciones de Seguridad y Continuidad**

Todo funcionario debe aceptar y cumplir los requerimientos de la política de seguridad de la empresa en el uso de los recursos de tecnología Informática

- Cumplir con los estándares, procedimientos y políticas de la empresa.
- Mantener la confidencialidad de mis claves de acceso, y no compartirla con nadie
- Comprender los derechos de acceso a los sistemas que me han sido otorgados, y no excederlos intentando ingresar a los sistemas de computación internos de la empresa, o cualquier otro sistema externo.
- No divulgar información confidencial y reservada de la empresa fuera de mi área o fuera de la empresa, sin previa autorización por escrito del Gerente del área.

- No instalar programas informáticos ajenos o de terceros en la computadora que tengo a mi cargo o cualquier otra computadora de la empresa, a menos que la empresa posea las licencias de uso correspondientes, y además me proporcione la autorización para utilizar dicha aplicación.
- No realizar copias ilegales de programas de computación.
- No acceder o descargar de Internet información pornográfica, juegos de azar, o aplicaciones informáticas de sitios inapropiados, por el alto riesgo de contraer virus informáticos, ya que puedo ocasionar pérdidas o daños graves en los Sistemas de Computación o en la red de datos de la empresa.
- No enviar correos electrónicos o mensajes con información difamatoria, pornográfica o contenido inapropiado.
- No dejar en mi escritorio documentos, información confidencial impresa y sellos, debo protegerlos bajo llave.
- No dejar en mi computadora información confidencial de forma desatendida.
- Asegurar mi computadora en áreas y sitios públicos y bloquearla cuando ya no esté cerca de mi escritorio.
- Asegurar que se realizó el respaldo de la información crítica y sensible del negocio y de los datos importantes que almaceno en el disco duro de mi computadora (notebook o desktop).
- Reconozco que soy responsable de la computadora, el software, y los datos que hay almacenados en mi computadora, además entiendo que incumplir con estas obligaciones pueden ocasionarme acciones disciplinarias o despido.

### 3.5.3 Comunicación

Determinar la necesidad de comunicación:

#### Selección del Gerente del proyecto

El responsable del plan de dirección del proyecto de Gestión de Continuidad del Negocio, es el Ing. Alexis García, PM, el cual fue asignado como representante de la Dirección, con la emisión del acta de constitución del Proyecto.

En el **Cuadro No. 14**, se detallan los grupos de interés catalogados por empresa, cargo, clasificación, rol en el proyecto y criterio de éxito, siendo un total de 10 los *stakeholders*.

**Cuadro No. 14.** Identificación de Grupos de interés y partes interesadas

Empresa	Cargo	Clasificación	Rol en el Proyecto	Criterio de Éxito
Nacional Seguros	Presidente	Principal	Patrocinador	Apoyo Organizacional (aporte de recursos)
NSVS	Gerencia General	Financiador	Gerente Organización	Soporte Económico (Apporte de Recursos)
NSPF	Gerencia General	Financiador	Gerente Organización	Soporte Económico (Apporte de Recursos)
TECORP	Gerencia General	Financiador	Gerente Organización	Soporte Económico (Apporte de Recursos)
NSVS	Gerencia de Operaciones	Financiador	Beneficiario	Capacidad Técnica (Objetivos del proyecto)
NSPF	Gerencia de Operaciones	Financiador	Beneficiario	Capacidad Técnica (Objetivos del proyecto)
TECORP	Gerente de TI y Seguridad	Influenciador	Miembro del Equipo	Calidad de Trabajo (Comprometido)
Holding	Asesor Legal	Influenciador	Miembro del Equipo	Capacidad Técnica (Objetivos del proyecto)
NSPF	Gerente de Riesgo	Influenciador	Miembro del Equipo	Capacidad Técnica (Objetivos del proyecto)
TECORP	Gerente de Desarrollo	Influenciador	Miembro del Equipo	Capacidad Técnica (Objetivos del proyecto)

Fuente: Elaboración Propia, 2019

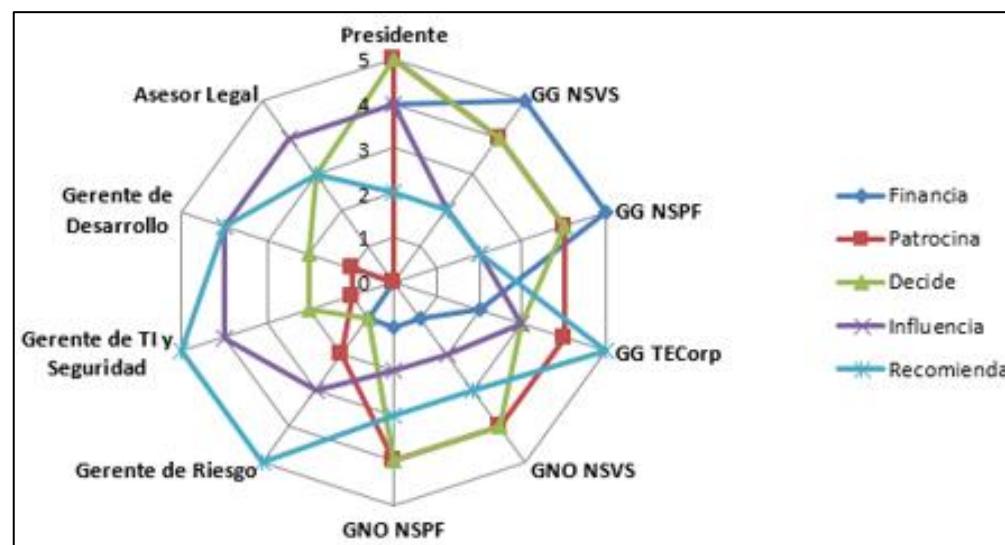
En el **Cuadro No. 15**, se detalla la matriz de poder de los *stakeholders*, categorizados: Financia, Patrocina, Decide, Influencia, Recomienda en el proyecto

**Cuadro No. 15.** Matriz de Poder

Stakeholder	Financia	Patrocina	Decide	Influencia	Recomienda	Poder
<b>Presidente</b>	4	5	5	4	2	20
<b>GG NSVS</b>	5	4	4	2	2	17
<b>GG NSPF</b>	5	4	4	2	2	17
<b>GG TECorp</b>	2	4	3	3	5	17
<b>GNO NSVS</b>	1	4	4	2	3	14
<b>GNO NSPF</b>	1	4	4	2	3	14
<b>Gerente de Riesgo</b>	1	2	1	3	5	12
<b>Gerente de TI y Seguridad</b>	0	1	2	4	5	12
<b>Gerente de Desarrollo</b>	1	1	2	4	4	12
<b>Asesor Legal</b>	0	0	3	4	3	10

Fuente: Elaboración Propia, 2019

En la **Figura No. 26**, se detalla en forma radial el poder de influencia de los *stakeholders*, en el proyecto, categorizados por cargo

**Figura No. 26.** Poder de influencia de los *stakeholders*

Fuente: Elaboración Propia, 2019

### Plan de Gestión de las Comunicaciones

El Plan de Gestión de las Comunicaciones trata de la Planificación de las Comunicaciones, Distribución de la Información, los Reportes de Desempeño y del Cierre Administrativo.

El Plan establece la política de comunicaciones a ser cumplida, y los sistemas y procedimientos para el aseguramiento de una comunicación efectiva, oportuna, adecuada y útil para el éxito del proyecto durante las diversas etapas del ciclo de vida del proyecto, y también durante la fase de operación del producto del proyecto. Sin embargo, es un plan diseñado y dirigido a la administración de las comunicaciones del Proyecto en un entorno multicultural, y busca optimizar el proceso de creación de sinergias. Es por lo tanto un enfoque sistemático, holístico y con una visión integral dirigida a resultados, con una elaboración interactiva y continuada de sus especificaciones y definiciones técnicas, y retroalimentación de lecciones aprendidas en cada etapa, estimulando el trabajo sinérgico y adoptando los más elevados patrones de calidad, responsabilidad y ética profesional.

El intercambio de informaciones es fundamental para el éxito del proyecto debiendo ser altamente estimulado y serán utilizadas las diversas dimensiones de la comunicación para lograr este fin; y con respecto a los estándares y sistemas de información para este proyecto la organización está perfectamente consciente de la necesidad y está adoptando todos los mecanismos y aportando todos los recursos requeridos para la administración exitosa de las comunicaciones del proyecto. El responsable Primario por el control general de la gestión de las Comunicaciones del proyecto es el Gerente de Proyecto (*Project Manager*).

El presente plan fue desarrollado por el Equipo del Proyecto bajo la coordinación del Gerente de Proyecto (*Project Manager*), y su concepción llevó en cuenta la descomposición de la Estructura Detallada del Trabajo (WBS) en las actividades de más bajo nivel que permitieron la identificación detallada de las necesidades específicas para la generación, coleta, organización, distribución, archivo, recuperación efectiva y disposición final de las informaciones del proyecto y de las comunicaciones formales e informales en todas las

direcciones, internas y externas al proyecto. A través de este enfoque, el gerente de proyecto puede entonces garantizar que todo el proyecto será contemplado, para producir un resultado de calidad y atender a las necesidades y expectativas del cliente.

- **Planificación de las comunicaciones**

El proceso de planificación de las comunicaciones del proyecto consistió en la identificación de los estándares de comunicación relevantes para el proyecto y la determinación de cómo atender a estos estándares, con el objetivo de asegurar que el proyecto será concluido dentro de la calidad deseada y de esta manera garantizar la satisfacción del cliente

Este proceso fue utilizado para determinar las necesidades de información, así como los métodos de distribución de esta información, y de comunicación de las partes interesadas, llevando en consideración algunos atributos:

- Tipo/Clase de información
- Objetivo de la información
- Frecuencia de la distribución de la información
- Formato de Presentación de la información
- Formato y Método de transmisión de la información, y
- Responsable por la distribución.

En la medida de lo posible y cuando necesario, serán aplicadas las lecciones aprendida e informaciones históricas de otros proyectos similares, los cuales fueron consideradas en el desarrollo del Proyecto.

## Análisis de los Requerimientos de Comunicación de los interesados

La estructura organizacional del Proyecto y su correspondiente Organigrama Funcional, discutidos en el Plan de Gestión de Recursos Humanos, fueron considerados y ampliamente utilizados en la determinación de los requerimientos de comunicación de las partes interesadas del proyecto.

El análisis del valor de la información y de los requerimientos de comunicación de todos los partes interesados conllevo a una combinación de varios tipos y formatos de comunicación que son relevantes y realmente aportan o contribuyen para el éxito del Proyecto.

Se tiene presente que se debe incrementar y mejorar el nivel y la eficacia actual de las comunicaciones entre las empresas involucradas en el proyecto. Esta información es extremadamente valiosa y se debe prestar extrema atención en este aspecto que puede llevar al fracaso del proyecto.

Si consideramos todas las partes interesadas identificadas, podemos determinar el número de canales potenciales de comunicación para el proyecto a través de la formula a continuación:

$10(10 - 1)/2 = 45$  canales potenciales de comunicación, que deberán ser correctamente gestionados.

El Plan de gestión de las Comunicaciones del Proyecto permite especificar los gestores de cada canal de comunicación y disciplinar el flujo de informaciones, a través de las relaciones de responsabilidad especificadas en las descripciones de funciones individuales de los miembros del equipo del proyecto

Con relación a la logística, la gran mayoría de los interesados se encuentra en el entorno inmediato, de maneras que los recursos disponibles son suficientes para una gestión adecuada y no representa ningún riesgo o restricción al éxito del proyecto.

### **Tecnología de la Información**

Como una de las restricciones al proyecto, se recuerda que: “Deberán ser utilizados solamente los recursos de telecomunicaciones y de tecnología de la información que están disponibles en la Unidad de Negocios”.

La Utilización del correo electrónico, sistema de mensajería colaborativa Lync y el portal de colaboración Intranet, serán los métodos de comunicación formal e informal, Interno y Externo, durante todas las fases del ciclo de vida del Proyecto.

### **Actualización del Plan de Comunicaciones**

El Plan de comunicaciones será contantemente actualizado y seguirá siendo elaborado durante todo el ciclo de vida del proyecto. Todas las informaciones serán organizadas de una manera que facilite su recuperación.

- **Distribución de la Información**

El proceso de Distribución de la Información asegurará que las comunicaciones se darán eficazmente y que la información estará disponible y accesible a todos los interesados cuando lo requieran.

Los métodos de distribución de las informaciones diseñados para el Proyecto son detallados a continuación, y serán exploradas todas las dimensiones de la comunicación, sea escrita y oral, formal o informal, interna o externa, y vertical y horizontal:

- Reuniones de revisión
- Comunicación electrónica

- Base de Datos en el servidor
- Notificaciones y Presentaciones

Las lecciones aprendidas en este proyecto serán debidamente registradas, analizadas, catalogadas y archivadas y serán utilizadas para el desarrollo e implementación de proyectos similares en otras unidades productivas de la Organización.

- **Reporte de Desempeño**

Este proceso involucrará la colección de toda la información de línea base y la distribución de los informes de desempeño a todos los interesados, de acuerdo a la lista de distribución previamente discutida y aprobada.

Los informes de desempeño se diseñan para brindar información sobre el alcance, cronograma, costo, calidad, recursos humanos y riesgos del proyecto; consistiendo de toda la información sobre el desempeño del trabajo, relativa al estado y/o finalización de los entregables. Serán incluidas también informaciones relativas al estado de las solicitudes de cambio aprobadas, como también las acciones correctivas recomendadas a cada caso.

Básicamente los informes de desempeño organizarán la información recopilada y presentarán los resultados y/o comentarios de los análisis comparándolos con la línea base.

Se proveerá información sobre el avance el estado del proyecto, así como los pronósticos actualizados del valor ganado (EV: *Earn value*), basados en el desempeño actual. Los informes serán emitidos para determinados niveles de detalle de acuerdo a las necesidades específicas de las partes interesadas.

El formato estándar del informe de desempeño del proyecto, incluirá Diagramas Gantt, histogramas de utilización de recursos, tablas y gráficas en general.

### 3.6 Operación (Cláusula 8) *Disaster Recovery Institute (DRI)*

Le empresa debe determinar, planificar y controlar las acciones necesarias para cumplir con la política y los objetivos de continuidad del negocio y satisfacer las necesidades y requisitos aplicables.

La metodología utilizada para desarrollar y operar el Modelo de Gestión de Continuidad del Negocio se basa en la cláusula 8 de la norma ISO 22301 y de las prácticas profesionales del Instituto de Recuperación de Desastres (DRI).

Se considera dentro del alcance:

- P01 – Planificación y Control Operacional
- P02 - Evaluación de Riesgos
- P03 - Análisis de Impacto al Negocio (BIA)
- P04 - Estrategias de Continuidad del Negocio
- P06 - Desarrollo e Implementación del Plan de Continuidad del Negocio (BCP)

Fuera del alcance:

- P05 - Respuesta a Incidentes
- P07 - Programa de Concientización y Entrenamiento
- P08 - Ejercicio, Evaluación y Mantenimiento del Plan
- P09 – Advertencia y Comunicación de Crisis
- P10 – Coordinación con dependencias externas

### **3.6.1 P01 Planificación y Control Operacional**

#### **Inicio y Administración del Programa**

##### **Problemática actual**

El crecimiento sostenido de las empresas del Grupo Nacional Seguros, en términos de negocio y organización, han determinado de la misma manera el crecimiento de la prestación de servicios informáticos para cubrir los requerimientos.

La expansión de las empresas en términos de presencia comercial con oficinas regionales distribuidas en diferentes ciudades de Bolivia, conlleva una infraestructura amplia que sostiene los servicios informáticos que llegan a todas las oficinas. La utilización de sistemas de información centralizados y consolidados ha llevado a la implementación de un sistema de comunicación integrado que utiliza diversos servicios de comunicación, así como, la implementación de centros de cómputo que cubren los servicios y demandas bajo esquemas de trabajo dedicados a los procesos y servicios básicos integrados.

Las unidades de negocio de Nacional Seguros, no disponen de un adecuado Plan de Continuidad del negocio, de esta manera no se han identificado los activos y procesos críticos del negocio, de modo de poder asegurar de que se pueda proveer garantía en el caso de una interrupción. Actualmente, no se puede asegurar que los procesos críticos serán reiniciados y gestionados de manera correcta.

En cumplimiento con los entes reguladores ASFI y APS, las empresas del Grupo Nacional Seguros, llevaron a cabo una auditoría financiera la cual además evaluó entre otros, los sistemas, la postura de la seguridad, tecnologías, infraestructura tecnológica, procesos, procedimientos como también los planes de contingencia y continuidad del negocio.

## Meta

Responder con un Tiempo Objetivo de Recuperación (RTO) razonable, a los incidentes y amenazas de ciberseguridad que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado.

## Contexto

La seguridad hoy en día se ha convertido en parte muy importante para el tema de la inversión en tecnología, por lo cual en toda inversión tecnológica se deben considerar aspectos relacionados con la gestión de seguridad y continuidad.

Con el fin de que esta inversión esté alineada plenamente a los objetivos estratégicos del negocio y que garantice de manera efectiva y eficiente su continuidad.

El Gerente de TI y Seguridad junto con las Gerencias Nacionales de Operaciones, y un equipo multidisciplinario de profesionales y siguiendo las buenas prácticas de la industria, deben elaborar e implementar una metodología de gestión de continuidad del negocio, que incluya un análisis de riesgo, análisis de impacto al negocio, y una estrategia probada de continuidad, que permita iniciar una revisión periódica del esquema de continuidad y seguridad, las pruebas y simulaciones necesarias a fin de asegurar el correcto mantenimiento del plan

En el **Anexo No. 10**, se declara el Acta de Constitución del Proyecto (*Project Charter*), definido por la alta dirección.

## Gestión del Alcance

El Plan de Gestión de Continuidad es aplicable a las empresas del Grupo Nacional Seguros, incluyendo las siguientes etapas:

### **Primera Etapa**

- Iniciación del Proyecto (*Project Charter*)
- Informe de Evaluación y Tratamiento de Riesgos (RA)
- Informe de Análisis de Impacto al Negocio (BIA)
- Informe de Estrategias de Continuidad

### **Segunda Etapa**

- Informe de Evaluación de propuestas
- Pliego de especificaciones técnicas particulares para la provisión de bienes y Servicios
  - Pliegos técnicos
  - Lista de Invitación (empresas y marcas)
  - Proceso de licitación y adjudicación
- Documentos de Visión, Alcance y Cronograma de implementación del BCM
- Acta de Entrega de Equipos
- Documentos de arquitectura, configuración y administración de las soluciones, políticas, normas, procesos, procedimientos y formularios

### **Tercera Etapa**

- Implementar el Plan de Continuidad
  - Sitio Alterno Operativo
  - Documentos de Gestión de Continuidad del Negocio (BCM)
  - Capacitación y Entrenamiento
  - Acta de las Pruebas y Simulaciones del Plan
  - Protocolos de aceptación de pruebas (ATP)

## Principales Entregables-Hitos

En el **Cuadro No. 16**, se detallan los principales entregables que serán elaborados por el proyecto los cuales están referenciados en su respectivo hito.

**Cuadro No. 16.** Principales entregables del proyecto

Etapa	Hito	Descripción de los entregables y/o servicios
Etapa 1	<b>H01</b>	<b>Propuesta de proyecto aprobado por personal ejecutivo</b> La descripción del proyecto ( <i>Project Charter</i> ) aprobado por el directorio y la alta dirección de las empresas del Grupo NAVI.
	<b>H02</b>	<b>Informe de Análisis y Tratamiento de Riesgos aprobado por el comité de tecnología y seguridad.</b> El informe de Análisis y Tratamiento de Riesgos del grupo, incluyendo: La metodología de análisis de riesgos, activos identificados, Amenazas y Vulnerabilidades aplicables, controles existentes evaluados, con los riesgos priorizados, valorados, tratados y aceptados.
	<b>H03</b>	<b>Informe de Análisis de Impacto al Negocio aprobado por el comité de tecnología y seguridad.</b> El informe BIA incluyendo: La metodología de análisis de impacto del grupo, Procesos, Sistemas, Personas y Recursos críticos identificados, Nivel de tolerancia de los recursos críticos, SLA acordados, elementos de configuración identificados, parámetros de recuperación y Niveles de impacto establecidos.
	<b>H04</b>	<b>Informe de las Estrategias de Continuidad aprobado por el comité de tecnología y seguridad y la estrategia de Continuidad seleccionada por la Alta dirección</b> El informe de Estrategias de Continuidad del Grupo, incluyendo el estudio de las alternativas: Sitio frio ( <i>Cold Site</i> ), Sitio Templado ( <i>Warm Site</i> ), Sitio Caliente ( <i>Hot Site</i> ), Sitio espejado ( <i>Mirror Site</i> ).
Etapa 2	<b>H05</b>	<b>Informe de Evaluación de propuestas comunicado y aprobado por el comité de tecnología y seguridad.</b> Informe de evaluación de los sobres A (Documentación Legal y Financiera) y B (Propuesta técnica y Económica) incluyendo: La metodología utilizada para la evaluación, los criterios de aceptación y el contrato borrador
	<b>H06</b>	<b>Pliego de especificaciones técnicas particulares para la provisión de bienes y Servicios, revisado y aprobado por el comité de tecnología y seguridad.</b> Los pliegos de especificaciones han sido elaborados, con el alcance y criterios de evaluación de las ofertas y calidad de los productos, conjuntamente con la lista de las empresas y marcas invitadas para la provisión de bienes y servicios, actas de entrega de la invitación directa
	<b>H07</b>	<b>Documentos de Visión, alcance y cronograma de implementación del BCM son revisados por la Gerencia de Desarrollo de Software, Gerencia de TI y Seguridad y aprobados por el comité de Tecnología y Seguridad.</b> Los documentos de Visión y Alcance han sido elaborados, revisados y aprobados, se ha establecido el cronograma de implementación de las soluciones.

<b>Etapa</b>	<b>Hito</b>	<b>Descripción de los entregables y/o servicios</b>
	<b>H08</b>	<b>Acta de entrega de equipos</b> Los documentos de Visión y Alcance han sido elaborados, revisados y aprobados, incluyendo: El acta de entrega de equipos en almacenes y el establecimiento del cronograma de inicio para implementación de las soluciones.
	<b>H09</b>	<b>Documentos de arquitectura, configuración y administración de las soluciones, políticas, normas, procesos, procedimientos y formularios.</b> Los documentos han sido elaborados, revisados y aprobados por la Alta dirección, actas de entregas de las copias controladas de documentos, actas de capacitación para el personal clave.
<b>Etapa 3</b>	<b>H11</b>	<b>Sitio alterno operativo</b> El acceso al sitio alterno es controlado, los sistemas están configurados y probados exitosamente y se encuentran listos para operar en caso de una declaración de incidente.
	<b>H12</b>	<b>Acta de las pruebas y simulaciones del BCM</b> El acta de las pruebas de simulación del BCM incluyendo la fecha establecida anticipada, la lista de las actividades de recuperación con los responsables claves, los resultados exitosos y fallidos de las pruebas.

**Fuente:** Elaboración Propia, 2019

### **Gestión del Cronograma**

El objetivo del Plan de Gestión del Cronograma es considerar la correcta aplicación de todos los procesos necesarios para la ejecución del Modelo de Gestión de Continuidad del Negocio (proyecto BCM), de acuerdo al tiempo previsto en la línea base.

La principal técnica utilizada durante el desarrollo del proyecto es: Juicio de Expertos; Utiliza la experiencia del gerente de área y de los ingenieros con experiencia en Proyectos Similares.

### **Línea base del cronograma**

La línea base del cronograma está establecida por el Cronograma Preliminar del Proyecto y las **Necesidades y expectativas de las partes interesadas** conforme a la sección **3.2.2**

## **Lista de actividades**

A partir del desglose de la Estructura Detallada de Trabajo (WBS), del **Anexo No. 11**, se desarrolla la lista de Actividades del Proyecto, teniendo un total de 108 actividades.

## **Estimación de tiempos**

Para la estimación de tiempos se ha aplicado la técnica de Juicio experto, dando a cada actividad, valores de tiempo de acuerdo a la experiencia del experto, además se incluye el riesgo en el cálculo a través del método PERT (*Project Evaluation and Review Techniques*), dado por tres escenarios estimados: Optimista, Pesimista y el Más Probable (Busio, 2018).

Se determinó el cálculo ponderado de la estimación de tiempos utilizando el método PERT. En el **Cuadro No. 17**, se resume la estimación de tiempos por Etapas y Fases, siendo 348 el Optimista, 518 el Más Probable, 716 el Pesimista, y de **537.17** días el tiempo calculado a través del método **PERT**.

**Cuadro No. 17.** Estimación Resumida de Tiempos

ÍTEM	EDT	TAREA	Optimista (Días)	Más Probable (Días)	Pesimista (Días)	PERT (Días)
1	1	Programa de Gestión de Continuidad del Negocio (BCM)	348.00	518.00	716.00	537.17
2	1.1	Etapa I - Plan de Gestión de Continuidad (BCM)	62.00	94.00	146.00	102.33
3	1.1.1	Fase 1 - Gestión del Proyecto (PM)	11.00	18.00	36.00	19.83
10	1.1.2	Fase 2 - Evaluación de Riesgos (RA)	14.00	22.00	33.00	22.50
18	1.1.3	Fase 3 - Análisis de Impacto	16.00	24.00	36.00	24.67
25	1.1.4	Fase 4 - Estrategia de Continuidad	21.00	30.00	41.00	35.33

35	1.2	Etapa II - Plan de Implementación del BCP	286.00	424.00	570.00	434.83
36	1.2.1	Fase 5 - Implementar el BCP	129.00	201.00	279.00	202.00
76	1.2.2	Fase 6 - Entrenamiento y Pruebas	10.00	18.00	26.00	18.00
90	1.2.3	Fase 7 - Estrategia de Ciberseguridad	147.00	205.00	265.00	205.33
105	1.2.4	Fase 8 - Revisión y Cierre del Proyecto	6.00	9.00	15.00	9.50

Fuente: Elaboración Propia, 2019

En el **Anexo No. 12**, se presenta los resultados de la estimación de tiempo, aplicados a todas las actividades de la lista

Si se adiciona una desviación estándar (diferencia del valor Pessimista y el Optimista / 6) al tiempo calculado con PERT, la duración del proyecto se estimaría entre el PERT +/- la desviación estándar del tiempo la actividad.

Si se consideran:

- una desviación estándar, el nivel de confianza será de 68.26%.
- dos desviaciones estándar, el nivel de confianza será de 95.46%.
- tres desviaciones estándar, el nivel de confianza será de 99.73%

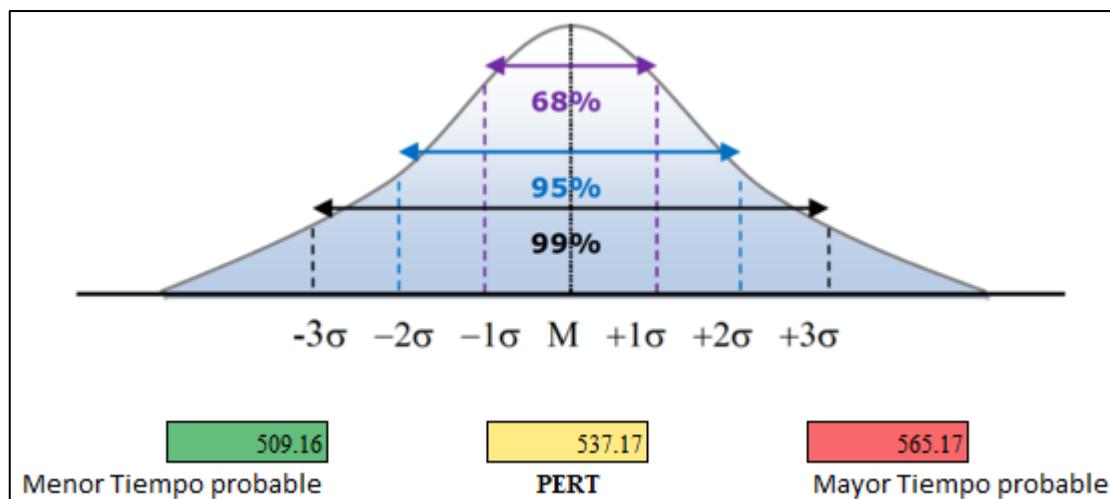
Según el **Cuadro No. 18**, al aplicar un nivel sigma 3 (tres desviaciones estándar), se estima una duración entre el menor tiempo probable de 509.16 y el Mayor Tiempo Probable 565.17 días. (para un nivel de confianza del 99.73%)

**Cuadro No. 18.** Nivel Sigma aplicado a la Estimación de Tiempo

Nivel Sigma	Probabilidad	Desv Estándar	Media Min	Media Max
1	68.2600%	9.33	527.83	546.50
2	95.4600%	18.67	518.50	555.84
3	99.7300%	28.00	509.16	565.17

Fuente: Elaboración Propia, 2019

En la **Figura No. 27**, se explica la estimación de tiempo con un nivel sigma de tres sobre la curva de distribución normal

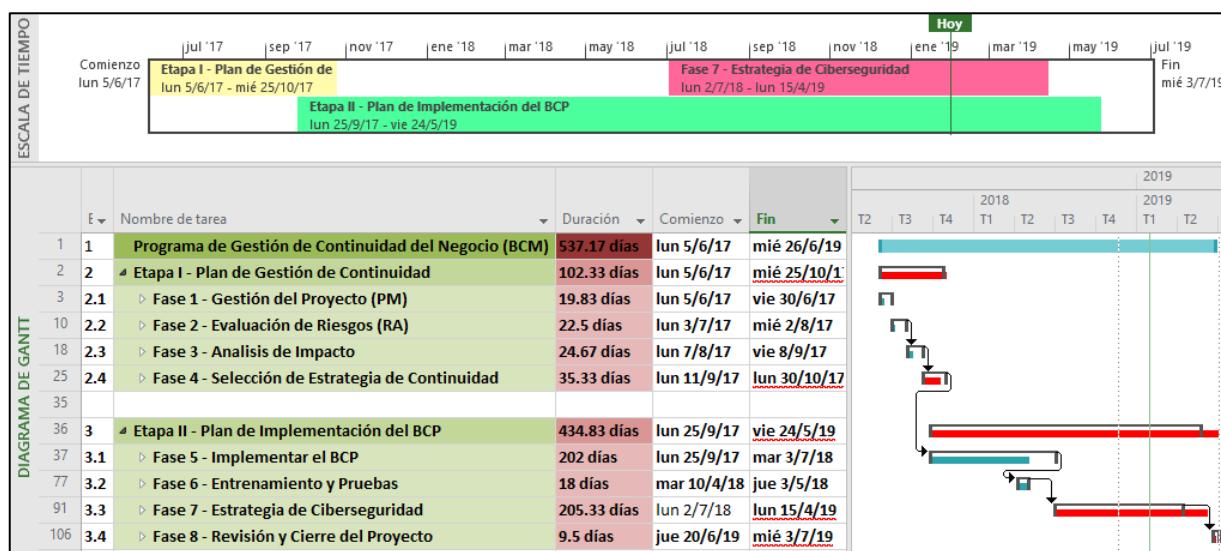


**Figura No. 27.** Estimación de Tiempo aplicado a la curva de Distribución Normal

Fuente: Elaboración Propia, 2019

## Cronograma

A continuación, se describe en la **Figura No. 28**, el resumen de los elementos claves del cronograma de trabajo



**Figura No. 28.** Cronograma de Trabajo

Fuente: Elaboración Propia, 2019

## Gestión de Costos

### Línea base del costo

La línea base del costo establecida en el Proyecto y determinada por PERT como el costo máximo, el cual asciende a \$us 863,013.11

En el **Cuadro No. 19**, se resume la estimación de costos del proyecto en etapas y fases

**Cuadro No. 19.** Estimación Resumida de Costos

ÍTEM	EDT	TAREA	Optimista (USD)	Más Probable (USD)	Pesimista (USD)	PERT (USD)
1	1	Programa de Gestión de Continuidad del Negocio (BCM)	797,308.59	862,662.73	922,928.77	863,013.11
2	1.1	Etapa I - Plan de Gestión de Continuidad (BCM)	18,354.92	27,928.72	43,682.27	28,958.68
3	1.1.1	Fase 1 - Gestión del Proyecto (PM)	3,530.67	5,777.46	11,554.91	6,365.90
10	1.1.2	Fase 2 - Evaluación de Riesgos (RA)	4,311.41	6,788.08	10,136.58	6,933.39
18	1.1.3	Fase 3 - Análisis de Impacto	5,195.16	7,798.71	11,709.99	8,016.66
25	1.1.4	Fase 4 - Estrategia de Continuidad	5,317.69	7,564.48	10,280.79	7,642.73
35	1.2	Etapa II - Plan de Implementación del BCP	778,953.67	834,734.01	879,246.50	834,054.43
36	1.2.1	Fase 5 - Implementar el BCP	524,668.40	559,158.75	598,118.44	559,903.64
76	1.2.2	Fase 6 - Entrenamiento y Pruebas	1,700.28	3,170.68	4,641.07	3,170.68
90	1.2.3	Fase 7 - Estrategia de Ciberseguridad	252,584.99	272,404.58	276,486.99	269,781.72
105	1.2.4	Fase 8 - Revisión y Cierre del Proyecto	756.88	1,135.32	1,892.21	1,198.40

Fuente: Elaboración Propia, 2019

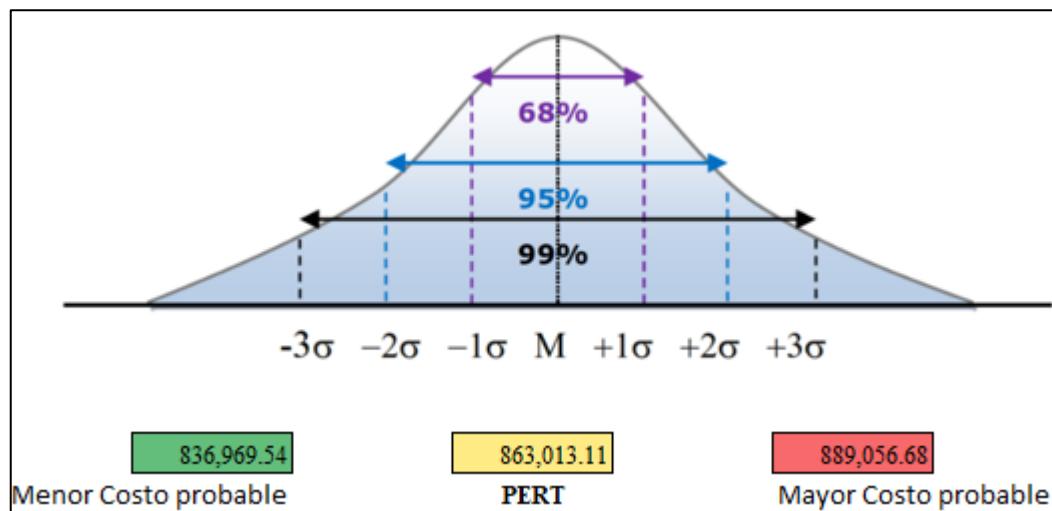
Según el **Cuadro No. 20**, al aplicar un nivel sigma 3 (tres desviaciones estándar), para un nivel de confianza del 99.73%), se estima que el proyecto podría suponer un costo mínimo probable de \$us 836,969.54 y un costo mayor probable de \$us 889,056.68. (para un nivel de confianza del 99.73%)

**Cuadro No. 20.** Nivel Sigma aplicado a la Estimación de Costos

Nivel Sigma	Probabilidad	Desv Standard	Media Min	Media Max
1	68.2689%	8,681.19	854,331.92	871,694.30
2	95.4499%	17,362.38	845,650.73	880,375.49
3	99.7300%	26,043.57	836,969.54	889,056.68

Fuente: Elaboración Propia, 2019

En la **Figura No. 29**, se explica la estimación de costos con un nivel sigma de tres sobre la curva de distribución normal.



**Figura No. 29.** Estimación de Costos aplicado a la curva de Distribución Normal

Fuente: Elaboración Propia, 2019

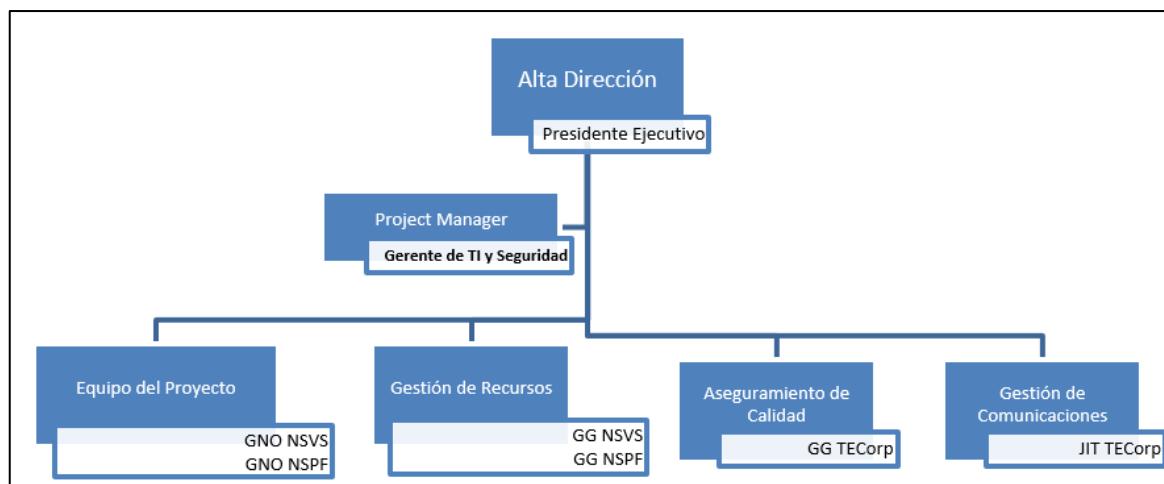
El desglose de la estimación del costo del proyecto se detalla en el **Anexo No. 13**.

### Estimación de Costos

### Gestión de RRHH

### Organigrama del Proyecto

El organigrama de la organización básica del proyecto BCM se presenta en la **Figura No. 30**.



**Figura No. 30.** Organigrama funcional del Proyecto BCM

Fuente: Elaboración Propia, 2019

### Matriz de Responsabilidades

La matriz de asignación de responsabilidades (RACI), es utilizada para relacionar las actividades con recursos. Para lograr asegurar que cada uno de los componentes o actividades esté asignado a un individuo o equipo.

- **Responsable (*Responsible*):** Este rol realiza el trabajo y es responsable por su realización.
- **Aprobador (*Accountable*):** Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él.
- **Consultado (*Consulted*):** Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
- **Informado (*Informed*):** Este rol debe ser informado sobre el progreso y los resultados del trabajo.

En el **Cuadro No. 21**, se detallan las responsabilidades del proyecto BCM aplicados en la matriz RACI.

**Cuadro No. 21.** Matriz de asignación de responsabilidades del proyecto BCM.

Componentes o Actividad	Alta Dirección	Gerente de Proyecto (Project Manager)	Equipo del Proyecto	Gestión de Recursos	Aseguramiento de Calidad	Gestión de Comunicaciones
<b>Apoyo Organizacional</b>	Responsable	Consultado	Informado	Informado	Informado	Informado
<b>Soporte Económico</b>	Aprobador	Consultado	Responsable	Informado	Informado	Informado
<b>Administración de Capacidad Técnica</b>	Aprobador	Consultado	Responsable	Informado	Informado	Informado
<b>Administración de Calidad del Trabajo</b>	Consultado	Aprobador	Informado	Informado	Responsable	Informado
<b>Administración de Costos</b>	Aprobador	Responsable	Consultado	Informado	Informado	Informado
<b>Administración de RRHH</b>	Informado	Aprobador	Consultado	Responsable	Informado	Informado
<b>Administración de Comunicaciones</b>	Informado	Aprobador	Consultado	Informado	Informado	Responsable
<b>Administración de Riesgos</b>	Aprobador	Responsable	Consultado	Informado	Informado	Informado

Fuente: Elaboración Propia, 2019

## Responsabilidades de Equipos

En el **Cuadro No. 22**, se detallan las acciones y responsables de la participación de los equipos, sobre el cual depende el nivel de interrupción del servicio y de los tipos de activos perdidos o dañados.

**Cuadro No. 22.** Responsabilidades de Equipos en el proyecto BCM

Equipo	Acciones	Responsable
<b>Equipo de respuesta a incidentes</b>	Recibir la información sobre todo el incidente que pueda ser considerado como una amenaza a los activos/procesos	<ul style="list-style-type: none"> <li>▪ Gerente de TI y Seguridad</li> <li>▪ Jefe de IT</li> </ul>
<b>Equipo de Acción de Emergencia</b>	Es el primer equipo de respuesta, cuya función es ocuparse de la respuesta a emergencia: Seguridad Física, Bomberos, UDEM Policía	<ul style="list-style-type: none"> <li>▪ Servicios Generales</li> </ul>
<b>Equipo de Seguridad de la Información</b>	Implementar las medidas de seguridad necesarias en el entorno del procedimiento alternativo, necesarios para mantener un nivel de información y seguridad	<ul style="list-style-type: none"> <li>▪ Gerente de TI y Seguridad</li> <li>▪ Jefe de IT</li> </ul>

Equipo	Acciones	Responsable
	de los recursos de TI similares al que se encontraba en el sitio principal	
<b>Equipo de Valoración de Daños</b>	Valora el grado de los daños una vez ocurrido el desastre y estima el tiempo que se requiere para las operaciones de recuperación en el lugar afectado	<ul style="list-style-type: none"> <li>▪ Servicios Generales</li> <li>▪ Jefe de IT</li> </ul>
<b>Equipo de Gestión de Emergencia</b>	Responsable de coordinar las actividades de todos los otros equipos (Recuperación, Continuidad, Respuesta) y está a cargo de la toma de decisiones clave. Además determinan la activación del BCP	<ul style="list-style-type: none"> <li>▪ Gerente General TECorp</li> </ul>
<b>Equipo de almacenamiento en sitio alterno</b>	Responsable de obtener, empacar y enviar los medios y los registros a las instalaciones de recuperación	<ul style="list-style-type: none"> <li>▪ Supervisor de Soporte Técnico</li> </ul>
<b>Equipo del Software</b>	Responsable de restaurar el software del sistema operativo y sus actualizaciones, probar el software y resolver los problemas a nivel de sistemas	<ul style="list-style-type: none"> <li>▪ Administrador de Servidores</li> </ul>
<b>Equipo de las Aplicaciones</b>	Restaurar los paquetes y los programas de aplicaciones del usuario en el sistema de respaldo	<ul style="list-style-type: none"> <li>▪ Supervisor de Soporte Técnico</li> </ul>
<b>Equipo de Operaciones de emergencia</b>	Residirán en el lugar de recuperación de los sistemas y gestionaran las operaciones del sistema durante la totalidad del desastre	<ul style="list-style-type: none"> <li>▪ Equipo de Primeros Auxilios</li> <li>▪ Equipo de Control de Incendio</li> <li>▪ Equipo de Evacuación</li> </ul>
<b>Equipo de recuperación de la red</b>	Responsable de dirigir el tráfico Voz y datos de la red WAN, restablecer el control y el acceso de la red al lugar de recuperación. Proveer soporte continuo para las comunicaciones de datos y supervisar las comunicaciones	<ul style="list-style-type: none"> <li>▪ Administrador de Redes</li> </ul>
<b>Equipo de Comunicaciones</b>	Trabaja conjuntamente con el equipo de recuperación de red. Responsable de conseguir e instalar el hardware de comunicaciones en el lugar de recuperación y coordinar con los proveedores locales.	<ul style="list-style-type: none"> <li>▪ Administrador de Telecomunicaciones</li> </ul>
<b>Equipo de transporte</b>	Equipo de apoyo para ubicar un lugar de recuperación. Responsable de coordinar el transporte de los empleados de la compañía al sitio de recuperación, también ayuda a contactar a los empleados para informarles de los nuevos lugares de trabajo	<ul style="list-style-type: none"> <li>▪ Servicios Generales</li> <li>▪ Gerente Nacional de Operaciones</li> </ul>
<b>Equipo de Hardware de usuario</b>	Ubica y coordina la entrega e instalación de computadoras personales, impresoras, fotocopiadoras, teléfonos y otros equipos necesarios	<ul style="list-style-type: none"> <li>▪ Supervisor de Soporte Técnico</li> <li>▪ Servicios Generales</li> <li>▪ </li> </ul>
<b>Equipo de preparación de Datos y Registros</b>	Actualiza los parámetros iniciales de los sistemas y de las bases de datos.	<ul style="list-style-type: none"> <li>▪ Subgerente de Soporte de Aplicaciones</li> </ul>

Equipo	Acciones	Responsable
	Supervisa al personal contratado para el ingreso de los datos y asiste en los esfuerzos de salvar los registros	
<b>Equipo de soporte administrativo</b>	Provee soporte al personal de oficina, a los otros equipos y sirve como centro de mensajes para el lugar de recuperación del usuario. Controla las funciones de contabilidad y de nomina	<ul style="list-style-type: none"> <li>▪ Subgerente de Contabilidad</li> <li>▪ Subgerente Administrativo Contable</li> </ul>
<b>Equipo de suministros</b>	Da apoyo al equipo de hardware de usuarios contactando a los vendedores y coordinando la logística para un suministro continuo de los elementos necesarios de oficina y de computo	<ul style="list-style-type: none"> <li>▪ Servicios Generales</li> <li>▪ Recursos Humanos</li> </ul>
<b>Equipo de salvamento</b>	Gestiona el proyecto de reubicación, además de la valoración de los daños para determinar si la planeación debería estar dirigida a la reconstrucción o reubicación. Coordina el salvamento inmediato de los registros y provee información necesaria para presentar reclamos de seguros	<ul style="list-style-type: none"> <li>▪ Equipo de Primeros Auxilios</li> <li>▪ Equipo de Control de Incendio</li> <li>▪ Equipo de Evacuación</li> </ul>
<b>Equipo de reubicación</b>	Coordina el traslado de la sala de servidores al sitio alterno o nueva ubicación. Reubicación de las operaciones de procesamiento de los sistemas de información, tráfico de comunicaciones y operaciones de usuario, Monitoreo del nivel de servicio	<ul style="list-style-type: none"> <li>▪ Jefe de IT</li> <li>▪ Administrador de Telecomunicaciones</li> </ul>
<b>Equipo de Coordinación</b>	Responsable de coordinar los esfuerzos de recuperación en las diversas oficinas ubicadas en lugares geográficos diferentes	<ul style="list-style-type: none"> <li>▪ Recursos Humanos</li> </ul>
<b>Equipo de Asuntos legales</b>	Responsable de manejar los problemas legales que surjan por diversas razones debido a cualquier incidente, incluye daños a terceros.	<ul style="list-style-type: none"> <li>▪ Corporación Jurídica</li> <li>▪ Asesor Legal Corporativo</li> </ul>
<b>Equipo de Prueba de recuperación</b>	Responsable de probar los diversos planes desarrollados y de analizar el resultado	<ul style="list-style-type: none"> <li>▪ Gerente de TI y Seguridad</li> <li>▪ Gerente de Desarrollo de Software</li> <li>▪ Jefe de IT</li> <li>▪ Auditor Interno</li> </ul>
<b>Equipo de capacitación</b>	Proveerá capacitación a los usuarios para las disposiciones de los procedimientos de continuidad del negocio y recuperación de desastres	<ul style="list-style-type: none"> <li>▪ Responsable de Gestión y DO</li> <li>▪ Subgerente Corporativo de Calidad</li> </ul>
<b>Equipo de relaciones públicas</b>	Ayudar a contener el daño a la imagen y asegurar que la crisis no empeore	<ul style="list-style-type: none"> <li>▪ Corporación Jurídica</li> <li>▪ Asesor Legal Corporativo</li> </ul>

Fuente: Elaboración Propia, 2019

### **3.6.2 P02 Evaluación de Riesgos**

#### **Objetivos**

Realizar el análisis de los procesos críticos, de las tecnologías de información y comunicaciones, sobre la cual depende la organización a manera de poder reducir los riesgos de las amenazas de ciberseguridad del negocio, hasta un nivel aceptable dentro de su entorno de operación.

#### **Objetivos Específicos**

- Identificar las amenazas y vulnerabilidades de la entidad para evaluar los controles existentes y el impacto acumulado sobre los activos.
- Evaluar los riesgos detectados para sugerir las medidas preventivas y correctivas necesarias a través de un Plan de Tratamiento de Riesgos
- Elaborar un Plan de respuesta a Incidentes para mejorar la continuidad operacional de la compañía considerando los principales riesgos y amenazas de ciberseguridad

#### **Metas**

Entender los diferentes aspectos que conforman las amenazas, identificando las vulnerabilidades y los factores de riesgo, tanto en el aspecto tecnológico, como en los procesos críticos del negocio, los cuales son soportados por las aplicaciones y la infraestructura tecnológica.

#### **Propósito**

El propósito para el desarrollo del presente programa de Análisis de Riesgos Informáticos, se establece por:

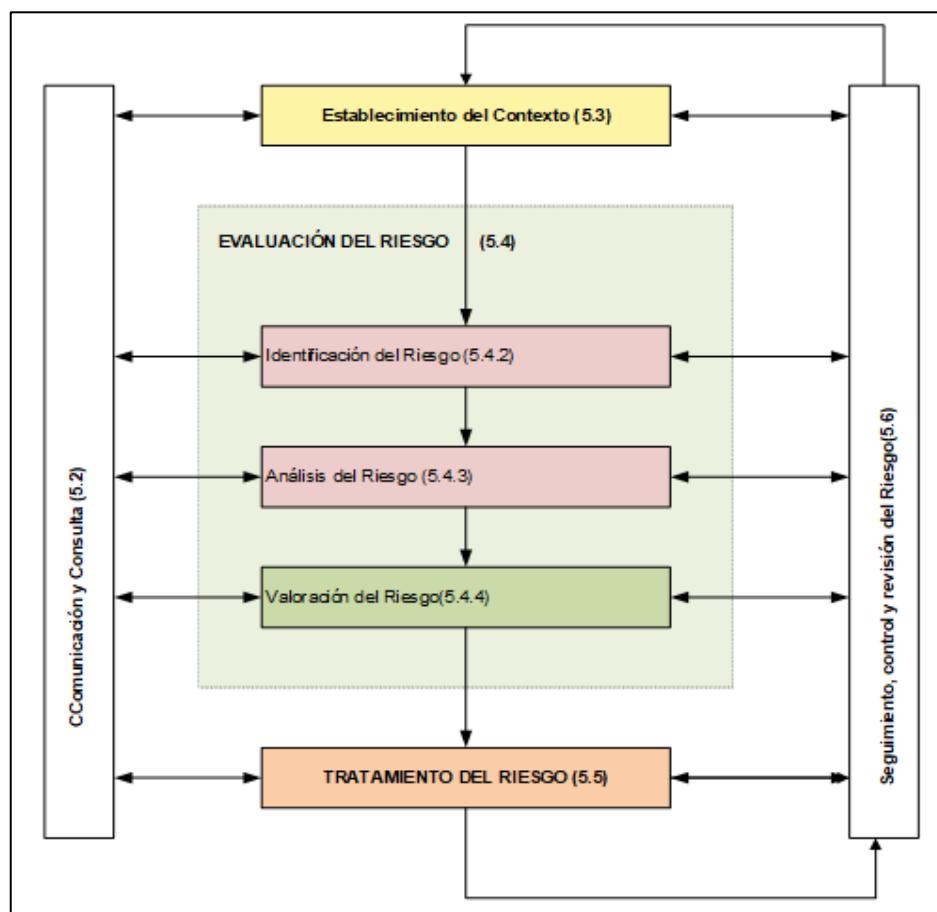
- Apoyar al Sistema de Gestión de Seguridad de la Información

- Dar soporte al Modelo Gestión de Continuidad del Negocio (BCM)
- Garantizar el cumplimiento de la organización con requisitos legales y regulatorios
- Demostrar la entrega de evidencia de la rendición de cuentas y debida diligencia

## Metodología

Para el proceso de Gestión de Riesgos de Seguridad de la Información del Grupo Empresarial de Inversiones Nacional Vida S.A. y para dar soporte particular a los requisitos del Modelo de Gestión de Continuidad del Negocio (BCM), se ha utilizado como directriz la norma **NB/ISO/IEC 31000:2009** “Gestión del Riesgo-Principios y Directrices”.

En Proceso de Gestión del Riesgo se muestra en la **Figura No. 31**



**Figura No. 31.** Proceso de Gestión del Riesgo

Fuente: (ISO 31000, 2014, pág. 17)

Para la elaboración del Programa de Análisis de Riesgos de las Tecnologías de Información, se utiliza como referencia **ISO 27005:2010** “Gestión del Riesgo en la Seguridad de la Información”

Para la valoración y estimación del programa de Análisis de Riesgo se utiliza como referencia la metodología **MAGERIT** versión 2 “Metodología de Análisis y Gestión de Riesgos de los Sistemas Información”.

### **Alineamiento Normativo**

- NB/ISO/IEC 27001:2007 Requisitos del Sistema de Gestión de Seguridad de la información.
- NB/ISO 27005:2010 Gestión del Riesgo en la Información
- NB/ISO 22301:2012 Requisitos del Sistema de Gestión de Continuidad del Negocio.

### **Determinación de los criterios básicos de riesgo**

Los criterios de riesgos, incluyen además los siguientes factores:

- La naturaleza y los tipos de causas
- Consecuencias que pueden ocurrir y cómo se van a medir
- La evolución temporal de probabilidad y de las consecuencias

### **Métodos**

El análisis de riesgo se evalúa por los métodos cualitativos y semicuantitativos

### **Criterios de Evaluación del riesgo**

Con el fin de determinar el riesgo en la seguridad de la información de la organización, se definen los siguientes aspectos:

- La importancia de la Confidencialidad, integridad y disponibilidad para las operaciones y el negocio y la relación de las dimensiones Disponibilidad, Integridad y Confidencialidad

- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso a la información cuando lo requieran y a sus activos asociados.

Si una amenaza afectará la disponibilidad las consecuencias serían graves.

- **Integridad:** Garantía de la exactitud y completitud de la información y los métodos de su procesamiento

Si los datos se alteran de manera no voluntaria o intencionada, causaría graves daños a la organización.

- **Confidencialidad:** Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso

La revelación de datos críticos y sensibles causaría graves daños a la organización.

### **Excepciones:**

Cuando un activo no está disponible durante largos períodos de tiempo, este carece de valor, por lo que no supone mayor daño.

Cuando los datos están clasificados como uso público o de uso interno, estos carecen de valor apreciable, por lo cual su conocimiento o alteración no supone preocupación alguna

Para definir los criterios de evaluación de riesgos, se define una escala de diez valores, dejando en valor 0 como despreciable y el valor 10 como muy alto a efectos de riesgo

El **Cuadro No. 23**, muestra los criterios de valoración de riesgo cualitativo considerados en el Análisis de Riesgo.

**Cuadro No. 23.** Criterios de valoración de riesgo cualitativo

Valor	Descripción	Criterio
<b>10</b>	Muy Alto	Daño muy grave a la organización
<b>De 7 a 9</b>	Alto	Daño grave a la organización
<b>De 4 a 6</b>	Medio	Daño importante a la organización
<b>De 1 a 3</b>	Bajo	Daño menor a la organización
<b>0</b>	Despreciable	Irrelevante

Fuente: Elaboración Propia, 2019

### Apetito de riesgo

- Disminuir las pérdidas por el orden del 10%, ocasionadas en los procesos críticos
- Los riesgos materializados no deben exponer más del 5% del Patrimonio
- La empresa tiene que hacer negocios de manera segura, por lo que el riesgo no deberá pasar los niveles de aceptación

### Niveles de Aceptación de Riesgos

- El primer umbral de riesgo, corresponde al riesgo objetivo o deseado por la organización
- El segundo umbral de riesgo, debe ser acompañado de un plan de tratamiento de riesgos  
Para ser aceptado, debe aprobarse el plan con las acciones correctivas para reducirlo a un nivel aceptable dentro de un tiempo definido.

### Criterios de Aceptación del riesgo

Con el fin de definir el beneficio y el riesgo estimado para el negocio, se establece que los riesgos mayores (que se encuentren por encima de los umbrales definidos), serán considerados como nivel de riesgo aceptable.

El riesgo en la seguridad de la información de la organización, se define en las siguientes escalas:

- Para los riesgos que originan brechas de seguridad que afectan la Disponibilidad, Integridad y Confidencialidad de la información.
- Si el promedio del riesgo de Seguridad (D+I+C) /3, es mayor de 8 sobre 10, será necesario aceptar el riesgo con excepción.

### **Excepciones para aceptar el riesgo**

La alta gerencia acepta los riesgos por encima del umbral definido, cuando:

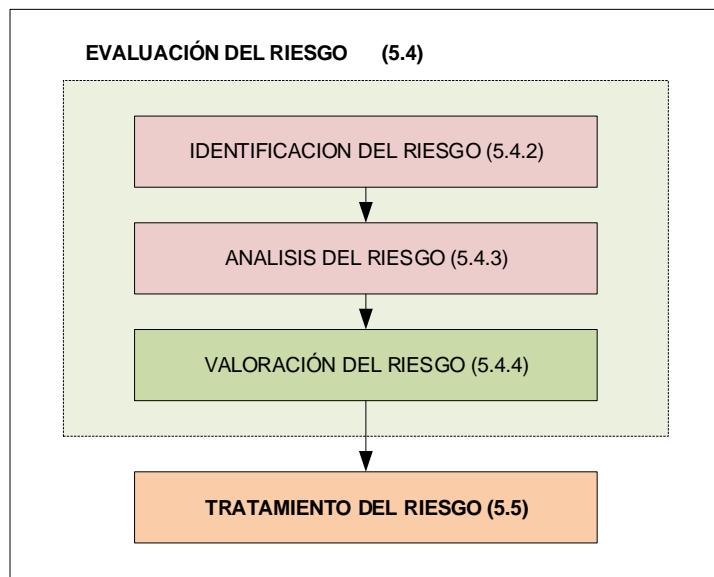
- Estos no resultan en incumplimiento con leyes o reglamentos del ente regulador.
- En el caso que las operaciones, tecnologías y finanzas no sean afectadas.
- En el caso que la actividad que origina el riesgo sea temporal o de corto plazo.
- Exista aprobación y compromiso para ejecutar acciones de tratamiento adicional que reduzcan dicho riesgo a un nivel aceptable en un periodo definido de tiempo (inmediato, a corto plazo, a mediano plazo, a largo plazo).
- A criterio del negocio se puede permitir la aceptación de riesgos altos e identificar el nivel aceptable del riesgo.

#### **1) Establecimiento del Contexto (Cláusula 5.3)**

Todo lo relacionado con el establecimiento del **Contexto en la organización**, se definió en el epígrafe **3.2**

#### **2) Evaluación del Riesgo (Cláusula 5.4)**

De acuerdo a la **Figura No. 32**, la evaluación del riesgo es el proceso general de identificación, análisis y valoración del Riesgo.



**Figura No. 32.** Proceso de Evaluación del Riesgo

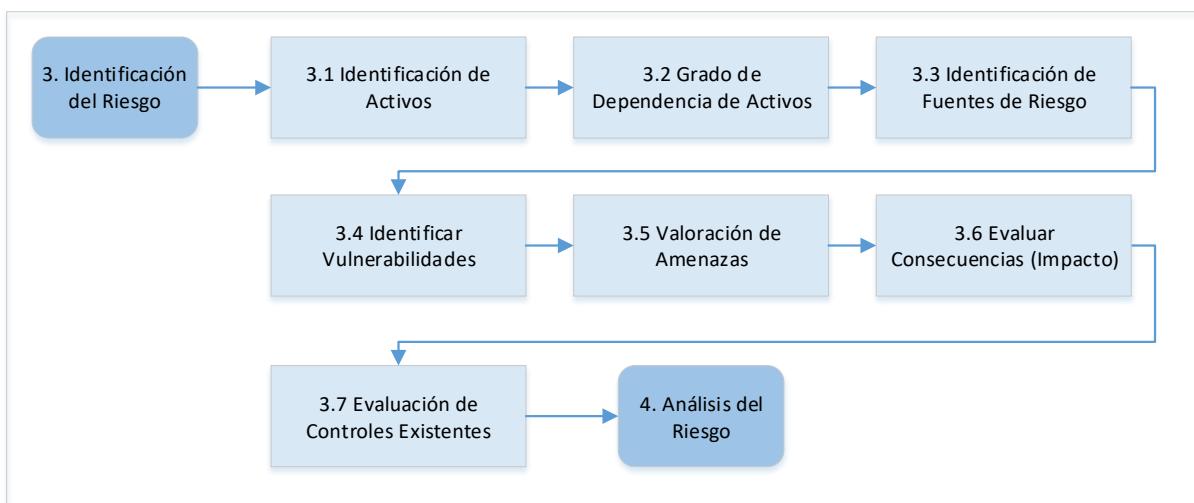
**Fuente:** Elaboración Propia, 2019

El objetivo del Proceso de evaluación del Riesgo, es determinar el valor de los activos de información, identificar amenazas y vulnerabilidades aplicables que existen, identificar los controles existentes y sus efectos en el riesgo identificado, determinar las consecuencias potenciales y priorizar los riesgos derivados frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

## **Identificación del Riesgo (5.4.2)**

Determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

En la **Figura No. 33**, se muestra la Secuencia de tareas en la etapa de Identificación de Riesgos.



**Figura No. 33.** Secuencia de tareas en la etapa de Identificación de Riesgos

Fuente: Elaboración Propia, 2019

### Identificación de Activos

Como punto de partida se realiza en esta fase la identificación de los activos de información que pueden ser afectados en lo que se refiere a su confidencialidad, integridad y disponibilidad.

Se considera un **activo** a todo lo que tiene valor para la empresa (ISO IEC 27000, 2018).

Fueron identificados (48) activos críticos y elementos de configuración, la lista de activos críticos y elementos de configuración, que serán utilizados en la evaluación de Riesgos, se detallan en el **Anexo No. 14**

A partir de la lista de dominios, grupos de activos y elementos de configuración, se realiza la identificación de las fuentes de riesgos, amenazas y consecuencias, para luego registrar los riesgos y establecer un plan de tratamiento de riesgo en conformidad con la política y alineado con las expectativas del negocio:

En el **Cuadro No. 24**, se muestran la agrupación de los activos de información catalogados por 6 Dominios, 6 Grupos de Activos y 48 Elementos de Configuración.

**Cuadro No. 24.** Activos de información catalogados

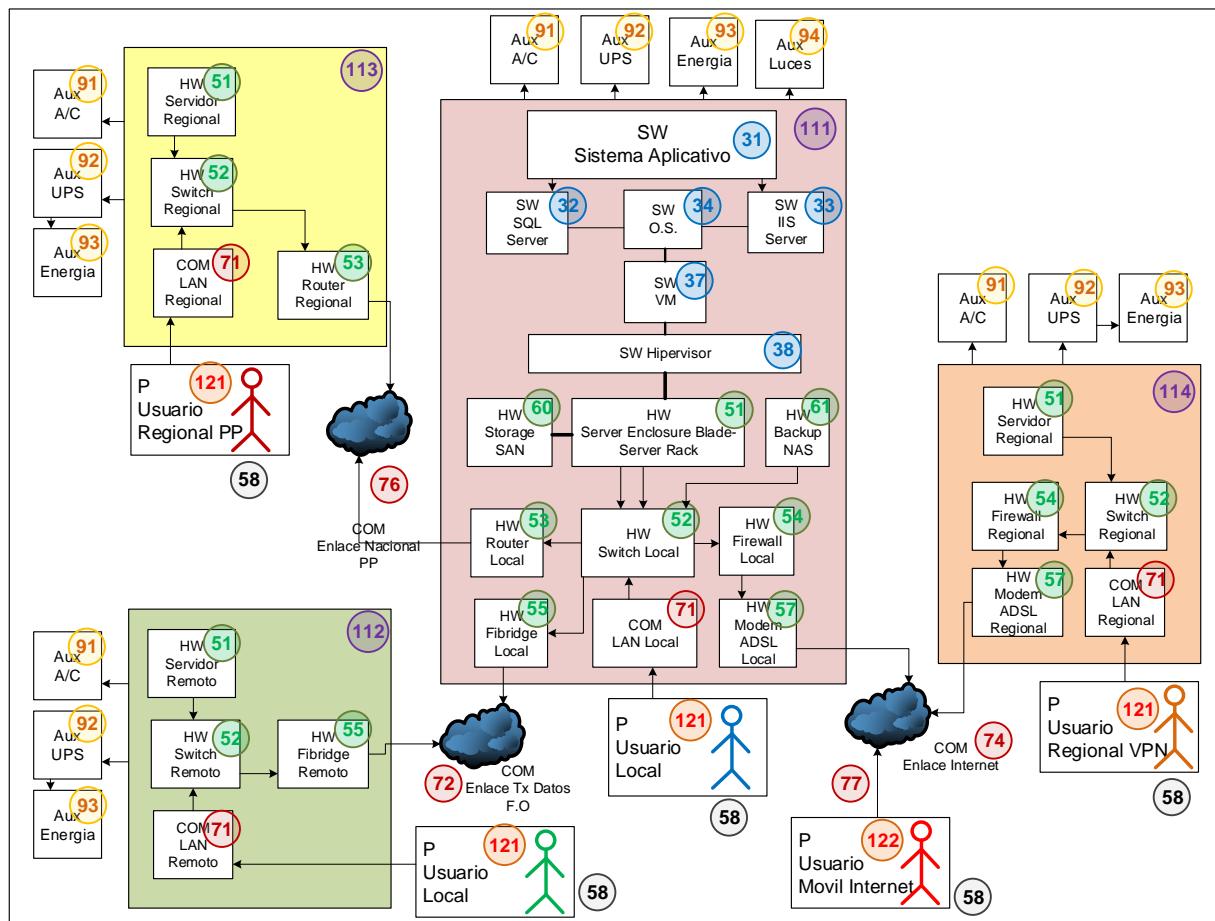
Dominio	Descripción	Total	Grupo	ID	Elemento
[B]	Capa de Negocio	7			
			<b>Procesos</b>		
					<b>P1</b> Proceso Crítico 1 - Gestión Comercial
					<b>P2</b> Proceso Crítico 2 - Gestión de Cobranzas
					<b>P3</b> Proceso Crítico 3 - Gestión de Siniestros
			<b>Documentos</b>		
					<b>D11</b> Documento Uso Público
					<b>D12</b> Documento Uso Interno
					<b>D13</b> Documento Confidencial
					<b>D14</b> Documento Secreto
[SI]	Servicios Internos	1			
				<b>SI21</b>	Infraestructura de Colaboración
[EQ]	Equipamiento	26			
			<b>[SW] Aplicaciones</b>		
					<b>SW31</b> Sistema de Aplicación (ERP)
					<b>SW32</b> Motor de base de Datos ( <i>SQL Server</i> )
					<b>SW33</b> Servicio de Publicación (IIS)
					<b>SW34</b> Sistemas Operativos de Red
					<b>SW35</b> Suite Ofimática del Usuario
					<b>SW36</b> Utilitarios
					<b>SW37</b> Máquina Virtual
					<b>SW38</b> <i>Hipervisor</i>
			<b>[HW] Equipos</b>		
					<b>HW51</b> Servidor Físico/Virtual
					<b>HW52</b> <i>Switch</i> (comutador)
					<b>HW53</b> <i>Router</i> (Enrutador)
					<b>HW54</b> <i>Firewall</i> (Pared de Fuego)
					<b>HW55</b> <i>Fibridge/Transceiver</i> (Conversor OE)
					<b>HW56</b> PBX (Central Telefónica)
					<b>HW57</b> Modem ADSL (Equipo de Modulación)
					<b>HW58</b> Equipo Computador (PC Escritorio/Portátil)
					<b>HW59</b> Equipos Utilitarios ( <i>Data Show</i> , Impresora, Escáner)
					<b>HW60</b> <i>Storage SAN</i>
					<b>HW61</b> <i>Backup NAS</i>
			<b>[COM] Comunicaciones</b>		

Dominio	Descripción	Total	Grupo	ID	Elemento
				<b>COM71</b>	Red Lan (Local/Wireless)
				<b>COM72</b>	Enlace F.O (Tx Voz/Datos)
				<b>COM73</b>	Enlace E1 (Tx Voz)
				<b>COM74</b>	Enlace Internet (ADSL/ <i>OnLine</i> )
				<b>COM75</b>	Acelerador de Ancho de banda
				<b>COM76</b>	<i>Link</i> Nacional (Punto a Punto/FR)
				<b>COM77</b>	Red Privada Virtual ( VPN <i>Site2Site</i> , <i>Client2Site</i> )
	<b>[AUX] Auxiliares</b>				
				<b>AUX91</b>	Aire Acondicionado
				<b>AUX92</b>	UPS (Sistema Ininterrumpido de Energía)
				<b>AUX93</b>	Energía No Regulada
				<b>AUX94</b>	Sistemas Esenciales (Iluminación, Alarmas)
[SS]	<b>Servicios Subcontratados</b>	<b>3</b>			
				<b>SS101</b>	Servicios Generales (Seguridad Física, Limpieza, Mantenimiento)
				<b>SS102</b>	<i>Holding</i> (RRHH, Legal, Auditoria)
				<b>SS103</b>	Proveedores de Telecomunicaciones
[L]	<b>Instalaciones</b>	<b>3</b>			
				<b>L111</b>	Sitio Central
				<b>L112</b>	Sitio Alterno
				<b>L113</b>	Agencias Locales/Regionales
[P]	<b>Personal</b>	<b>4</b>			
				<b>P121</b>	Usuario Interno (Local/Remoto/Regional)
				<b>P122</b>	Usuario Externo ( <i>Internet/Móvil</i> )
				<b>P123</b>	Soporte L1 ( <i>Help Desk</i> Técnico de Soporte)
				<b>P124</b>	Soporte L2 (Administradores Infraestructura Tecnológica)

Fuente: Elaboración Propia, 2019

### Grado de dependencia de los Activos

Los procesos críticos dependen de los datos, aplicaciones, tecnologías, infraestructura y de los recursos humanos. En la **Figura No. 34**, se muestra un diagrama de dependencia de colaboración y visibilidad, el cual se considera en la materialización de riesgos múltiples



**Figura No. 34.** Diagrama de Colaboración y visibilidad con dependencias

Fuente: Elaboración Propia, 2019

Como parte del trabajo se realiza el análisis de dependencia de los activos, considerando la valoración en el **Cuadro No. 25**, para la valoración de los activos críticos de información catalogados

**Cuadro No. 25.** Valoración de dependencia de activos

Grado	Categoría	Valoración
0%	N/A	No depende
1%	Baja	Prácticamente despreciable
10%	Media	Significativo
50%	Alta	Cierto grado de dependencia
90%	Muy Alta	Altamente dependiente
100%	Total	Totalmente dependiente

Fuente: Elaboración Propia, 2019

En el **Anexo No. 15**, se detalla el grado de dependencia evaluado en todos los activos

### **Identificación de Fuentes de Riesgo (Amenazas 5.4.2)**

La norma ISO 31000 en la cláusula 2.16 define una Fuente de Riesgo como, “Elemento que solo o en combinado posee potencial intrínseco para originar el riesgo” (ISO 31000, 2014, p. 7).

La norma ISO 27000 en la cláusula 3.74 define una Amenaza (*threat*) como, “Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización” (ISO IEC 27000, 2018, pág. 10).

La ISO 31000 no proporciona ejemplos de fuentes de riesgos y/o amenazas, por lo cual, la identificación se realiza con la orientación de MAGERIT (metodología de análisis y gestión de riesgos de los Sistemas de Información).

En el **Anexo No. 19**, se muestra un subconjunto de amenazas definidas por la metodología MAGERIT, que se utilizan en el presente trabajo

En el **Cuadro No. 26**, se presenta la identificación de (129) Amenazas posibles sobre los grupos de activos de información, se consideran las reacciones en cadena y los efectos acumulativos en cascada.

Para cada amenaza se genera una lista de los posibles riesgos sobre la base de aquellos eventos que pueden originar, incrementar o retrasar el logro de los objetivos.

**Cuadro No. 26.** Listado de amenazas sobre los activos de información

Dominio	Grupo	ID	Amenazas
<b>Capa de Negocio</b>			
	<b>Procesos</b>		
		A.07	Uso no previsto
<b>Documentos</b>			
		E.01	Errores y fallos de los usuarios
		E.02	Errores del Administrador del Sistema

Dominio	Grupo	ID	Amenazas
		E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )
		E.18	Destrucción de la Información
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )
		A.06	Abuso de privilegios de acceso
		A.11	Acceso no autorizado
		A.15	Modificación de la Información
		A.18	Destrucción de la Información
		A.19	Revelación de la Información ( <i>Dataleaks</i> )
<b>Servicios Internos</b>			
<b>Infraestructura de Colaboración</b>			
		I.05	Avería de origen físico o lógico
		E.01	Errores y fallos de los usuarios
		E.02	Errores del Administrador del Sistema
		E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, <i>Spyware</i> )
		E.09	Errores de re-encaminamiento
		E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )
		E.18	Destrucción de la Información
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		E.20	Vulnerabilidad de los Programas
		E.21	Errores de Mantenimiento / Actualización ( <i>software</i> )
		A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )
		A.06	Abuso de privilegios de acceso
		A.07	Uso no previsto
		A.08	Difusión de Software Dañino
		A.09	Re-encaminamiento de mensajes
		A.11	Acceso no autorizado
		A.15	Modificación de la Información ( <i>Defacement</i> )
		A.18	Destrucción de la Información
		A.19	Revelación de la Información ( <i>Dataleaks</i> )
		A.22	Manipulación del software
<b>Equipamiento</b>			
<b>[SW] Aplicaciones</b>			
		I.05	Avería de origen físico o lógico
		E.01	Errores y fallos de los usuarios
		E.02	Errores del Administrador del Sistema
		E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, <i>Spyware</i> )
		E.09	Errores de re-encaminamiento
		E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )
		E.18	Destrucción de la Información

Dominio	Grupo	ID	Amenazas
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		E.20	Vulnerabilidad de los Programas
		E.21	Errores de Mantenimiento / Actualización ( <i>software</i> )
		A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )
		A.06	Abuso de privilegios de acceso
		A.07	Uso no previsto
		A.08	Difusión de <i>Software</i> Dañino
		A.09	Re-encaminamiento de mensajes
		A.11	Acceso no autorizado
		A.15	Modificación de la Información ( <i>Defacement</i> )
		A.18	Destrucción de la Información
		A.19	Revelación de la Información ( <i>Dataleaks</i> )
		A.22	Manipulación del <i>software</i>
<b>[HW] Equipos</b>			
		N.01	Fuego
		N.02	Daños por Agua
		N.*	Desastres Naturales
		I.01	Fuego
		I.02	Daños por agua
		I.*	Desastres Industriales
		I.05	Avería de origen físico o lógico
		I.06	Corte del Suministro Eléctrico
		I.07	condiciones inadecuadas de temperatura/humedad
		E.02	Errores del Administrador del Sistema
		E.23	Errores de Mantenimiento / Actualización ( <i>hardware</i> )
		E.24	Caída del Sistema por agotamiento de Recursos ( <b>Disponibilidad</b> )
		E.25	Perdida de Equipos
		A.06	Abuso de privilegios de acceso
		A.07	Uso no previsto
		A.11	Acceso no autorizado
		A.23	Manipulación del <i>Hardware</i>
		A.24	Denegación de Servicio (DoS)
		A.25	Robo de Equipos
		A.26	Ataque destructivo (Vandalismo/terrorismo)
<b>[COM] Comunicaciones</b>			
		I.08	Fallo en servicios de comunicaciones (Interrupción Accidental o Deliberada)
		E.02	Errores del Administrador del Sistema
		E.09	Errores de re-encaminamiento
		E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )

<b>Dominio</b>	<b>Grupo</b>	<b>ID</b>	<b>Amenazas</b>
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		E.24	Caída del Sistema por agotamiento e Recursos ( <b>Disponibilidad</b> )
		A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )
		A.06	Abuso de privilegios de acceso
		A.07	Uso no previsto
		A.09	Re-encaminamiento de mensajes
		A.10	Alteración e Secuencia
		A.11	Acceso no autorizado
		A.12	Análisis de Trafico
		A.14	Interceptación de la Información ( <i>Sniffers</i> )
		A.15	Modificación de la Información ( <i>Defacement</i> )
		A.19	Revelación de la Información ( <i>Dataleaks</i> )
		A.24	Denegación de Servicio (DoS)
		A.26	Ataque destructivo (Vandalismo/terrorismo)
<b>[AUX] Elementos Auxiliares</b>			
		N.01	Fuego
		N.02	Daños por Agua
		N.*	Desastres Naturales
		I.01	Fuego
		I.02	Daños por agua
		I.*	Desastres Industriales
		I.05	Avería de origen físico o lógico
		I.06	Corte del Suministro Eléctrico
		I.07	condiciones inadecuadas de temperatura/humedad
		I.09	Interrupción de otros servicios o suministros esenciales
		E.23	Errores de Mantenimiento / Actualización ( <i>hardware</i> )
		A.07	Uso no previsto
		A.23	Manipulación del Hardware
		A.25	Robo de Equipos
		A.26	Ataque destructivo (Vandalismo/terrorismo)
<b>Servicios Subcontratados</b>			
		E.28	Indisponibilidad del Personal (Enfermedad, Huelga)
		A.19	Revelación de la Información
		A.25	Robo de Equipos
		A.29	Extorsión
		A.30	Ingeniería Social
<b>Instalaciones</b>			
		N.01	Fuego
		N.02	Daños por Agua
		N.*	Desastres Naturales

Dominio	Grupo	ID	Amenazas
		I.01	Fuego
		I.02	Daños por agua
		I.*	Desastres Industriales
		E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )
		E.18	Destrucción de la Información
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		A.07	Uso no previsto
		A.11	Acceso no autorizado
		A.26	Ataque destructivo (Vandalismo/terrorismo)
<b>Personal</b>			
	<b>Usuarios de Sistemas</b>		
		E.19	Fuga de Información ( <b>Confidencialidad</b> )
		E.28	Indisponibilidad del Personal (Enfermedad, Huelga)
		A.19	Revelación de la Información
		A.25	Robo de Equipos
		A.29	Extorsión
		A.30	Ingeniería Social

Fuente: Elaboración Propia, 2019

### Identificación de Vulnerabilidades (Cláusula 5.4.2)

En el **Anexo No. 17**, se presenta la identificación de (94) Vulnerabilidades detectadas sobre los Dominios y grupos de activos de información sobre la plataforma tecnológica.

Para cada Vulnerabilidad se genera una lista de los posibles riesgos sobre la base de aquellos eventos que pueden originar, incrementar o retrasar el logro de los objetivos.

En el **Cuadro No. 27**, se identifica la motivación y beneficios del atacante para explotar una vulnerabilidad sobre la plataforma tecnológica.

**Cuadro No. 27.** Identificación, Motivación y Beneficio del Atacante

ID del Dominio	Nombre del Dominio	Grupo	Vulnerabilidad	Valoración
[SC01]	Sitio Central SCZ			
	[101]	<b>Identificación del Atacante</b>		
		<b>101.b</b>	Competidor Comercial	Bajo
		<b>101.c</b>	Proveedor de servicios	Medio
		<b>101.d</b>	Grupos de presión política/activista/extremista	Bajo

ID del Dominio	Nombre del Dominio	Grupo	Vulnerabilidad	Valoración
		<b>101.e</b>	Periodistas	Bajo
		<b>101.g</b>	Personal interno	Medio
		<b>101.h</b>	Bandas criminales	Alto
		<b>101.i</b>	Grupos terroristas	Alto
	[102]	<b>Motivación del Atacante</b>		
		<b>102.a</b>	Beneficio económico	Medio
		<b>102.b</b>	Beneficios Comerciales	Medio
		<b>102.c</b>	Personal propio con problemas de conciencia	Bajo
		<b>102.f</b>	Con ánimo destructivo	Alto
		<b>102.g</b>	Con ánimo de causar daño	Medio
	[103]	<b>Beneficio del Atacante</b>		
		<b>103.a</b>	Moderadamente interesado	Bajo
	[104]	<b>Motivación del Personal Interno</b>		
		<b>104.b</b>	Baja calificación profesional / escasa formación	Alto
		<b>104.c</b>	Sobrecargado de trabajo	Medio
		<b>104.d</b>	Con problemas de conciencia	Bajo
	[105]	<b>Permisos de los usuarios (derechos)</b>		
		<b>105.a</b>	Se permite el acceso a Internet	Medio
		<b>105.b</b>	Se permite la ejecución de programas sin autorización	Bajo
		<b>105.c</b>	Se permite la instalación de programas sin autorización	Bajo
		<b>105.d</b>	Se permite la conexión de dispositivos removibles	Alto
	[111]	<b>Conectividad del Sistema de Información</b>		
		<b>111.c</b>	Conectado a un conjunto amplio de redes conocidas	Medio
	[112]	<b>Ubicación del Sistema de Información</b>		
		<b>112.a</b>	Dentro de una zona segura	Bajo

Fuente: Elaboración Propia, 2019

## Valoración de Amenazas

Para realizar la valoración de las amenazas sobre la plataforma tecnológica, se considera la frecuencia y el criterio de seguridad afectado utilizando la herramienta Pilar.

En el **Cuadro No. 28**, se describen los **Dominios de Amenazas** utilizados en la etapa de valoración.

**Cuadro No. 28.** Dominios de Amenazas

Dominio	Descripción de la Amenaza	Categorías
[N]	Desastres Naturales	2
[I]	Origen Industrial	11
[E]	Errores y fallos no intencionados	28
[A]	Ataques deliberados	30

Fuente: Elaboración Propia, 2019

Se puede observar en el **Cuadro No. 29**. Valoración por Dominio de Amenaza, que el 48.00% de las amenazas detectadas (60), corresponden al dominio «[A] - Ataques Deliberados», es decir, están directamente asociadas a riesgos de Ciberseguridad, mientras que el 29.60% de las amenazas detectadas (37), corresponden al dominio «[E] - Errores y Fallos no intencionados», es decir, están relacionadas con fallos no intencionales causados por las personas.

**Cuadro No. 29.** Valoración por Dominio de Amenaza

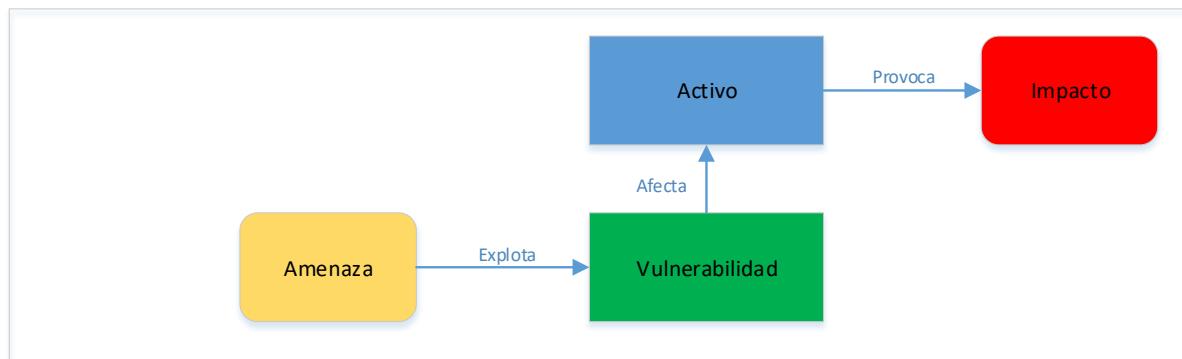
Dominio	Descripción de la Amenaza	Cantidad	Porcentaje
[N]	Desastres Naturales	9	7.20%
[I]	Origen Industrial	19	15.20%
[E]	Errores y Fallos no intencionados	37	29.60%
[A]	Ataques Deliberados	60	48.00%
	<b>Total</b>	<b>125</b>	<b>100.00%</b>

Fuente: Elaboración Propia, 2019

En el **Anexo No. 16**, se detalla el proceso de valoración de las amenazas agrupados por Dominio y Categoría sobre los distintos activos de información, como resultado obtenemos el grado de afectación de las amenazas y el valor acumulado.

## Evaluar Consecuencias (Impactos)

En la **Figura No. 35**, se observa la materialización de una **amenaza** sobre un **activo** aprovechando una **vulnerabilidad**



**Figura No. 35.** Relación Amenaza, Vulnerabilidad, Activo e Impacto

Fuente: Elaboración Propia, 2019

La norma (ISO IEC 27000, 2018) considera una **amenaza** a la causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización, y una **vulnerabilidad** a la debilidad de un activo o control que puede ser explotado por una o más amenazas.

En el **Cuadro No. 30**, se describe la tabla de valoración de impactos, utilizado para calcular las consecuencias.

**Cuadro No. 30.** Tabla de valoración de impactos

Tipo	Identificador	Impacto	Descripción
Directo	[F]	Financiero	Costo de Reposición del Activo
Directo	[O]	Operativo	Costo de las operaciones Interrumpidas, incluye adquisición, instalación, configuración y recuperación de Información ( <i>Backups</i> )
Indirecto	[I]	Imagen	Afectación de la Imagen y Reputación de Mercado
Indirecto	[N]	Normativo	Incumplimiento de las Regulaciones
Indirecto	[L]	Legal	Incumplimiento de obligaciones Contractuales
Indirecto	[P]	Personal	Incumplimiento de Código de ética o conducta

Fuente: Elaboración Propia, 2019

Se realiza la primera valoración de impacto sin considerar ningún tipo de control, a través de una combinación de valores entre 1 a 10, siendo 1 un impacto insignificante y 10 muy alto impacto.

Se procede a evaluar los activos de información en términos de costos de reemplazo o de reconstrucción.

En el **Cuadro No. 31**, se muestra la Evaluación de impactos acumulados, según el análisis, los dominios: Procesos, Documentos, Infraestructura, Aplicaciones, Comunicaciones y Servicios subcontratados, serán los más impactados por las vulnerabilidades y amenazas identificadas.

**Cuadro No. 31.** Evaluación de impactos acumulados

Domini o	Grupo	ID	Vulnerabili d	Amenaza	[F]	[O]	[I]	[N]	[L]	[P] ]	[T]
Capa de Negocio											
	Procesos	14	9	7 5 5 5 7 5 34							
	Documentos	5	4	5 5 4 7 7 5 33							
Servicios Internos											
	Infraestructura de Colaboración	14	8	7 5 6 7 5 5 35							
Equipamiento											
	[SW] Aplicaciones	16	7	5 5 6 5 5 5 31							
	[HW] Equipos	8	8	3 5 5 5 5 5 28							
	[COM] Comunicaciones	10	7	9 5 7 5 7 7 40							
	[AUX] Elementos Auxiliares	6	6	3 3 5 5 5 5 26							
Servicios Subcontratados		9	7	5 3 5 7 5 5 30							
Instalaciones		4	4	5 5 5 5 5 3 28							
Personal		9	7	3 5 3 5 5 5 26							
<b>Total</b>			<b>95</b>	<b>67</b>							

Fuente: Elaboración Propia, 2019

En el **Anexo No. 18**, se muestra en detalle el resultado del proceso de **Valoración de las consecuencias (Impactos) de vulnerabilidades y amenazas** sobre los activos de

información, se observan las vulnerabilidades y amenazas de alto impacto que requieren un tratamiento o la aplicación de un Control.

### Evaluación de Controles Existentes

Con el objetivo de evaluar la eficacia y eficiencia de los controles de seguridad implementados en los activos de información, se realiza una identificación del nivel de madurez actual.

En el **Cuadro No. 32**, se reflejan los distintos **Niveles de Madurez** utilizados

**Cuadro No. 32.** Niveles de Madurez

Nivel	Descripción
<b>N0 - Inexistente</b>	Ausencia total de controles identificables
<b>N1 - Inicial</b>	Es evidente que la empresa es consciente de la existencia del problema y la necesidad de estudiarlo. Sin embargo, no hay un proceso estandarizado
<b>N2 - Repetible</b>	Los controles se han implementado hasta una fase en que diferentes personas utilizan los mismos procedimientos
<b>N3 - Definido</b>	Los controles han sido estandarizados, cuenta con su procedimiento documentado y comunicado
<b>N4 - Gestionado</b>	Es posible controlar y medir el cumplimiento de los controles y tomar medidas donde parecen no funcionar correctamente
<b>N5 - Optimizado</b>	El proceso de control ha alcanzado el nivel de las mejores prácticas

Fuente: Elaboración Propia, 2019

Los controles implementados en los dominios: **Procesos, Documentos, Comunicaciones, Elementos Auxiliares y Personal**, se encuentran en un nivel **N1 – Inicial**  
En términos generales, considerando todos los dominios evaluados, los controles se encuentran en un nivel **N2 – Repetible**.

En el **Cuadro No. 33**, se muestra un **Resumen de evaluación de Controles existentes** considerando las mejores prácticas.

**Cuadro No. 33.** Resumen de evaluación de Controles existentes

Dominio	Grupo	Nivel de Madurez
Capa de Negocio		
	Procesos	N1 - Inicial
	Documentos	N1 - Inicial

Dominio	Grupo	Nivel de Madurez
<b>Servicios Internos</b>		
	Infraestructura de Colaboración	N2 - Repetible
<b>Equipamiento</b>		
	[SW] Aplicaciones	N2 - Repetible
	[HW] Equipos	N1 - Inicial
	[COM] Comunicaciones	N1 - Inicial
	[AUX] Elementos Auxiliares	N2 - Repetible
<b>Servicios Subcontratados</b>		N2 - Repetible
<b>Instalaciones</b>		N2 - Repetible
<b>Personal</b>		N1 - Inicial
<b>Nivel de Madurez General</b>		N2 - Repetible

Fuente: Elaboración Propia, 2019

Se evaluó el cumplimiento de 83 controles, diseñados para proteger los activos de información de 125 amenazas detectadas, en el **Anexo No. 20**, Se muestra el detalle de la **evaluación de controles existentes**.

### Análisis del Riesgo Cualitativo (5.4.3)

Desarrollar una compresión del riesgo considerando las Causas, Amenazas (Fuentes de riesgo) y las Consecuencias (Impactos), para analizar la probabilidad y determinar el Nivel de Riesgo, proporcionando finalmente una entrada para la valoración del Riesgo.

En la **Figura No. 36**, se muestra la Secuencia del proceso de **Análisis de Riesgos**.



**Figura No. 36.** Secuencia de la etapa de Análisis de Riesgos

Fuente: Elaboración Propia, 2019

### Registro de Riesgos

Para elaborar el formulario de registro de los riesgos, se utiliza el enfoque de la metodología MAGERIT.

De un total de 48 registros de riesgos, se adjunta un ejemplo en el **Anexo No. 22, formulario de registro de riesgos.**

### Evaluación de la Probabilidad

De acuerdo a (ISACA, 2016, pág. 106), la evaluación de Riesgo se expresa en la ecuación:

$$\text{Amenazas} \times \text{Vulnerabilidades} \times \text{Consecuencias} = \text{Riesgo}$$

Cuando se identifica el riesgo, la **probabilidad** se utiliza para calcular el nivel de riesgo en base a la cantidad de eventos combinado con las **Consecuencias** (Impacto) de que pudieran ocurrir en un determinado periodo de tiempo.

La **probabilidad**, es una medida de la frecuencia en que puede ocurrir un evento, deriva de la oportunidad de que una amenaza explote una vulnerabilidad.

Si no hay **Consecuencias** (Impacto), el Riesgo no es importante y se considera inexistente.

En el

**Cuadro No. 34,** se muestra el **Mapa de Calor** utilizado para el Análisis de Riesgo Cualitativo.

**Cuadro No. 34.** Mapa de Calor

			Consecuencias					
			Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5	
Probabilidad	A Casi certeza	Muy Alta	5 M	10 H	15 E	20 E	25 E	
	B Probable	Alta	4 M	8 H	12 H	16 E	20 E	
	C Posible	Media	3 L	6 M	9 H	12 H	15 E	
	D Improbable	Baja	2 L	4 M	6 M	8 H	10 H	
	E Raro	Muy Baja	1 L	2 L	3 L	4 M	5 M	
<b>Leyenda</b>								
		Riesgo Extremo	Requiere acción inmediata					
		Riesgo Alto	Necesita atención de la alta gerencia					
		Riesgo Moderado	Debe especificarse responsabilidad gerencial					
		Riesgo Bajo	Administrar mediante procedimientos de rutina					

Fuente: Elaboración Propia, 2019

Se procede a evaluar las Consecuencias de la amenaza en una escala predefinida de 1 hasta 5 (siendo 1: insignificante, 2: Menor, 3: Moderado, 4: Mayor, 5: Catastrófico), de cada uno de los activos de información, luego se procede a evaluar la probabilidad de ocurrencia de la amenaza en una escala predefinida de A hasta E (siendo A: Casi certeza, B: Probable, C: Posible, D: Improbable, E: Raro).

Se determina el Nivel del Riesgo multiplicando Consecuencias x Probabilidad.

En el

**Anexo No. 21**, se adjunta el desarrollo de la **Matriz de Determinación de Riesgos**

**Cualitativos**, utilizando como guia el Mapa de Calor.

#### **Valoración del Riesgo (5.4.4)**

Con los resultados del **Análisis del Riesgo Cualitativo**, se evalúa el nivel de riesgo asociado y su prioridad y se determina la necesidad de tratamiento, proporcionando una entrada para el Tratamiento de Riesgos.

En la **Figura No. 37**, se muestra la Secuencia de la etapa de **Valoración de Riesgos**.



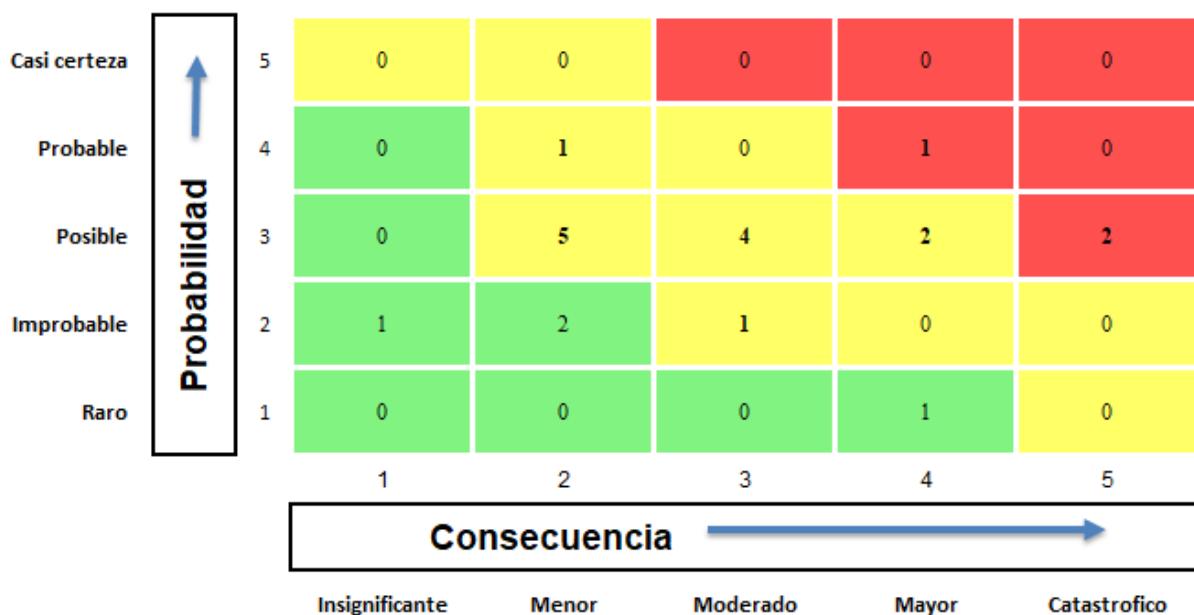
**Figura No. 37.** Secuencia de la etapa de Valoración de Riesgos

Fuente: Elaboración Propria, 2019

#### **Evaluación del Nivel de Riesgo**

Se asignan nuevos valores a la Probabilidad y se procede a contabilizar los riesgos por niveles de todos los activos de información, relacionando los nuevos valores de Consecuencias evaluadas y la Probabilidad de ocurrencia de la amenaza para desarrollar un mejor criterio de riesgo.

En la **Figura No. 38**, se observa la **Matriz de Riesgos totales** agrupados por Nivel de riesgos.



**Figura No. 38.** Matriz de Riesgos totales  
**Fuente:** Elaboración Propia, 2019

**Cuadro No. 35.** Resumen de riesgos Totales

Riesgos	Cantidad	%
Altos	3	15%
Medios	7	35%
Bajos	10	50%
Total	20	100%

**Fuente:** Elaboración Propria, 2019

En el **Cuadro No. 36**, Se muestra el **Nivel de Tolerancia al Riesgo** definido por la empresa.

Se observa que los riesgos **altos** son definidos como nivel de riesgo Intolerable, lo que requiere una acción inmediata de la alta gerencia (Nivel Estratégico).

Los riesgos **medios** son definidos como Significativos, por lo que se debe especificar un control para el tratamiento del riesgo en términos de costo-beneficio y comunicar al propietario del riesgo designado en el Formulario de Registro de Riesgos del **Anexo No. 22**.

Sin embargo, los riesgos **bajos**, son definidos como Tolerables, es decir, Insignificantes, por lo que no precisan ser tratados.

**Cuadro No. 36.** Nivel de Tolerancia al Riesgo (**figura**)

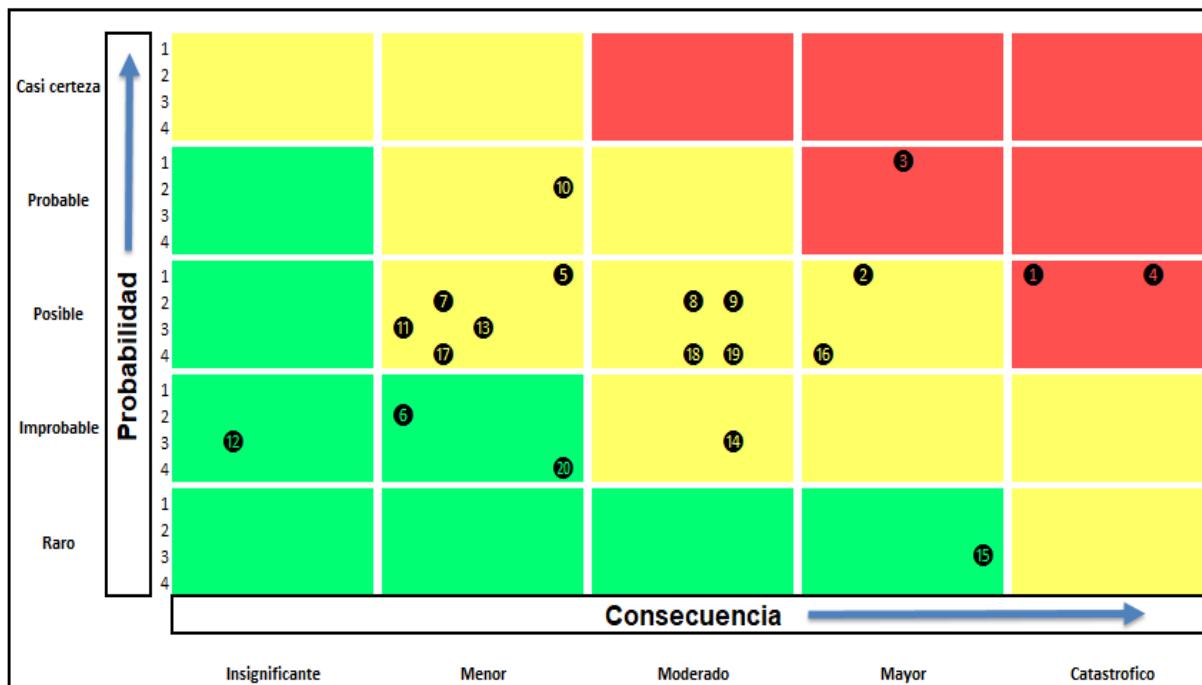
Nivel	Tolerancia al Riesgo	Acción
25 20 16 15	<b>Intolerable</b>	Nivel de Riesgo Intolerable Requiere acción inmediata de la alta gerencia (Estratégico)
12 10 9 8 6 5	<b>Significativo</b>	Debe especificarse responsabilidad del propietario del riesgo Considerar el Análisis Costo-beneficio al aplicar los controles (Táctico)
4 3 2 1	<b>Tolerable</b>	Nivel de Riesgo Insignificante Administrar mediante procedimientos de rutina (Operativo)

Fuente: Elaboración Propia, 2019

### Priorización de riesgos

Con los resultados del **Análisis del Riesgo Cualitativo**, se determina el Nivel de Riesgo a partir del Impacto (Consecuencia) y la Probabilidad, en el **Anexo No. 23**, se desarrolla la medición de la **Matriz de Riesgos con prioridad**.

Conocido los niveles de Tolerancia y la Matriz de Riesgos totales por nivel de riesgo, se define, la **Matriz de Nivel de Riesgos**, para apreciar el panorama de los riesgos identificados en cada nivel, de acuerdo a la **Figura No. 39**.



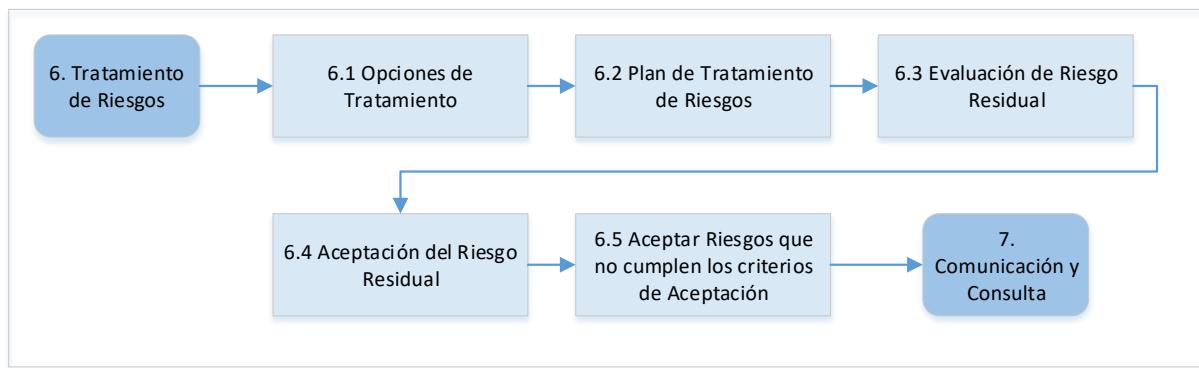
**Figura No. 39.** Matriz de Nivel de Riesgos

**Fuente:** Elaboración Propia, 2019

Se identifican los riesgos en la Matriz de nivel de Riesgos para observar sus niveles de Riesgos en el mapa de calor. Se agrupan múltiples riesgos bajos (verdes) y medios (amarillos), para determinar si la acumulación del riesgo podría dar como resultado un riesgo más alto para poder ser evaluado según corresponda.

### **3) Tratamiento del Riesgo (Cláusula 5.5)**

El tratamiento del riesgo implica la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. En la **Figura No. 40**, se muestra la **Secuencia de la etapa de Tratamiento de Riesgos**.



**Figura No. 40.** Secuencia de la etapa de Tratamiento de Riesgos

Fuente: Elaboración Propia, 2019

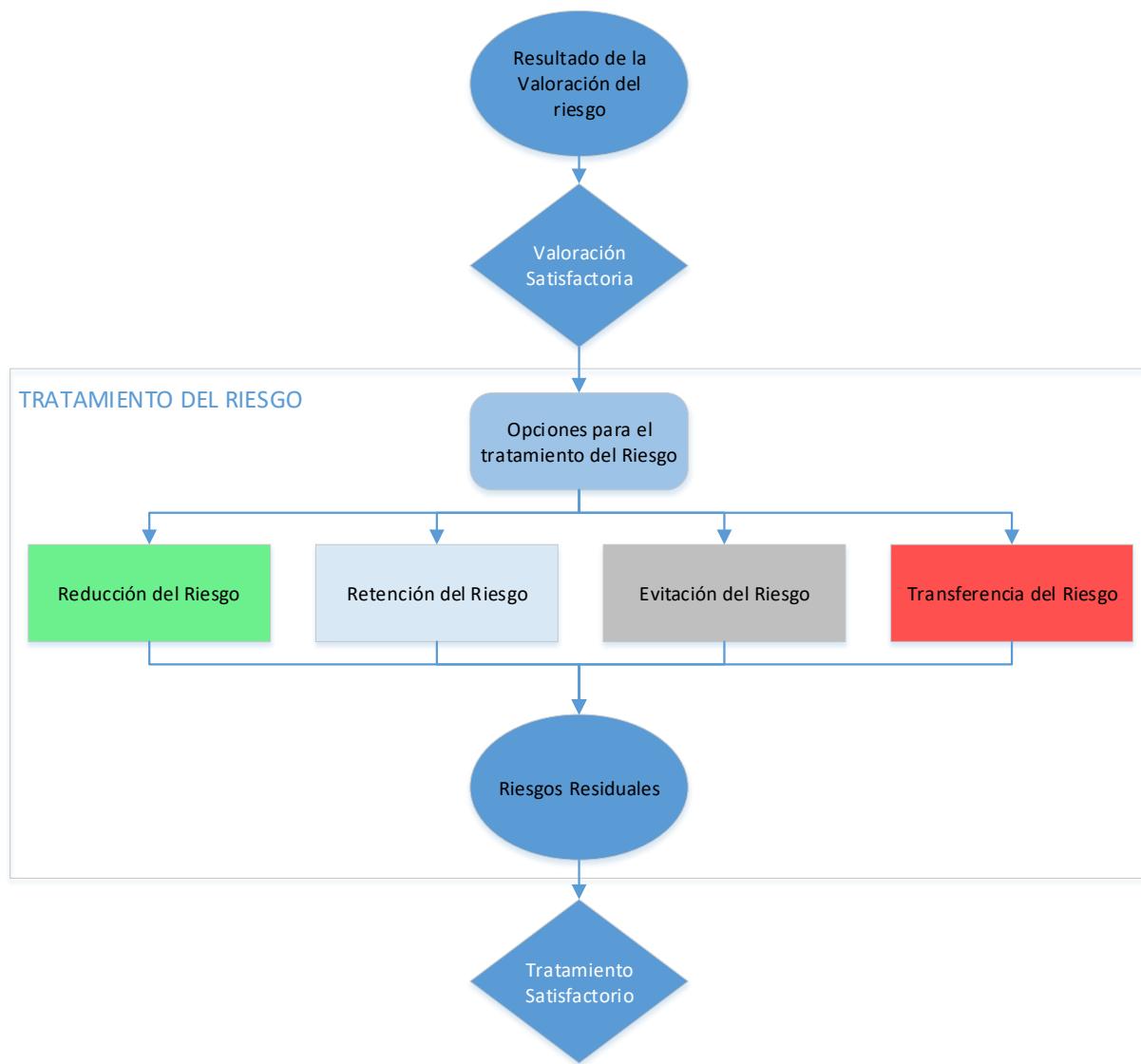
### Opciones de Tratamiento

Las opciones de tratamiento de riesgos se seleccionan con base en el resultado de la Valoración del riesgo que no se excluyen mutuamente, es decir, la combinación de las opciones podría beneficiar significativamente a la empresa en la reducción de la Probabilidad de los riesgos o de sus consecuencias.

De acuerdo a la norma (ISO 31000, 2014, pág. 22), las opciones de tratamiento del riesgo son las siguientes:

- Evitar riesgos (No comenzar o no continuar con la actividad)
- Aceptar el riesgo o Aumentarlo (Persiguiendo una oportunidad)
- Eliminar la fuente de riesgo (Cancelar las actividades)
- Modificar la Probabilidad o las Consecuencias del riesgo (Reducir)
- Compartir el Riesgo con otra parte (Transferir)
- Retener el Riesgo (Cumple con los criterios de aceptación)

En la **Figura No. 41**, se muestra la **Secuencia de Actividades para las opciones de Tratamiento del Riesgo**.



**Figura No. 41.** Secuencia de Actividades para el Tratamiento del Riesgo

Fuente: (ISO 27005, 2010)

### Plan de Tratamiento de Riesgos

En el **Anexo No. 24**, se desarrolla el **Plan de Tratamiento del Riesgo priorizado por Nivel de riesgo**, utilizando Métodos de Control (Controles Administrativos, técnicos y físicos) y Categorías de Control (disuasivos, preventivos, detectivos, correctivos y compensatorios).

## Evaluación del riesgo Residual

El riesgo residual es el riesgo que permanece después de que el riesgo ha sido tratado, es decir, después de la aplicación de los controles.

$$\text{Riesgo Residual} = \text{Riesgo inherente} - \text{Riesgo tratado (Controles)}$$

En el **Cuadro No. 37**, a partir del nivel de riesgo individual, se muestra el cálculo del riesgo individual y el riesgo tratado,

**Cuadro No. 37.** Calculo del riesgo Individual y del Riesgo tratado

ID Riesgo	Valor Impacto	Valor Probabilidad	Evaluación	Riesgo Medido	%Riesgo Individual	Riesgo tratado
1	4	4	16	Alto	9.8%	69.5%
2	5	3	15	Alto	9.1%	
3	5	3	15	Alto	9.1%	
4	4	3	12	Medio	7.3%	
5	4	3	12	Medio	7.3%	
6	3	3	9	Medio	5.5%	
7	3	3	9	Medio	5.5%	
8	3	3	9	Medio	5.5%	
9	3	3	9	Medio	5.5%	
10	2	4	8	Medio	4.9%	
11	2	3	6	Bajo	3.7%	30.5%
12	2	3	6	Bajo	3.7%	
13	2	3	6	Bajo	3.7%	
14	2	3	6	Bajo	3.7%	
15	3	2	6	Bajo	3.7%	
16	2	3	6	Bajo	3.7%	
17	2	2	4	Bajo	2.4%	
18	4	1	4	Bajo	2.4%	
19	2	2	4	Bajo	2.4%	
20	1	2	2	Bajo	1.2%	
<b>Total Riesgo</b>		<b>164</b>		<b>100.00%</b>	<b>100.00%</b>	

Fuente: Elaboración Propia, 2019

Se define la siguiente estimación para calcular el riesgo residual:

1. Se estima el Riesgo tratado o máximo

$$\text{Riesgo tratado [máximo]} = [\text{Riesgo inherente} - \text{Riesgo no tratado}]$$

$$\text{Riesgo tratado [máximo]} = [100\% - 30.5\%] = 69.5\%$$

2. Se estima el Riesgo no tratado o mínimo

$$\text{Riesgo no tratado [mínimo]} = [\text{Riesgo inherente} - \text{Riesgo tratado (Controles)}]$$

$$\text{Riesgo no tratado [mínimo]} = [100\% - 69.5\%] = 30.5\%$$

Para considerar los riesgos no identificados, calculamos la toleración a través de una desviación estándar (diferencia del valor máximo y mínimo) / 6, la estimación estaría entre +/- la desviación estándar.

$$\text{Desv. Estándar} = \left[ \frac{\{\text{Riesgo tratado [máximo]} - \text{Riesgo no tratado [mínimo]}\}}{6} \right]$$

$$\text{Desv. Estándar} = \left[ \frac{69.5\% - 30.5\%}{6} \right] = 6.5\%$$

Se estima el riesgo residual, considerando además una holgura para los riesgos no identificados (desviación estándar).

$$\text{Riesgo Residual [estimado]}$$

$$= \text{Riesgo inherente} - \text{Riesgo tratado (Controles)} \pm \text{Desv. std}$$

$$\text{Riesgo Residual [estimado]} = [100\% - 69.5\%] \pm 6.5\%$$

$$\text{Riesgo Residual [estimado]} = [30.5\%] \pm 6.5\%$$

Al aplicar un nivel sigma 1 (una desviación estándar=6.5%), se estima el menor riesgo residual probable de 24% y el mayor riesgo residual probable 37%. (para un nivel de confianza del 68.26%).

### Aceptación del riesgo Residual

- La dirección es consciente de la estimación del riesgo residual

- El riesgo residual estimado es equivalente a los criterios de la organización para el riesgo aceptable y la tolerancia
- El nivel de tolerancia del riesgo residual es aceptable y permitido por la Dirección (desviación <=10%).
- Los controles sugeridos para los activos de información evaluados reducen los impactos a niveles aceptables

La dirección acepta la responsabilidad sobre los controles necesarios identificados en el

**Anexo No. 24**, Plan de Tratamiento del Riesgo priorizado por Nivel de riesgo.

#### **Aceptar los riesgos que no cumplen los criterios de aceptación**

Es necesario aceptar el riesgo cuando cumple los siguientes requisitos:

- Los beneficios que acompañan a los riesgos son muy atractivos
- El costo del control sobre el riesgo es demasiado alto

El presente estudio no arroja riesgos fuera de los criterios de aceptación, por lo cual no se requiere tratamiento adicional

### **3.6.3 P03 Análisis de Impacto al Negocio (BIA)**

#### **Objetivo**

Identificar las funciones y procesos de la entidad con el fin de determinar qué procesos son esenciales para la continuidad de las operaciones y su posible impacto en caso de que no estén disponibles.

#### **Objetivos Específicos**

- Caracterizar los procesos críticos que soportan el servicio para determinar la prioridad y los tiempos estimados de recuperación (RTO).
- Determinar los tiempos máximos tolerables de interrupción (MTD) para determinar las estrategias adecuadas de recuperación
- Evaluar los recursos requeridos para apoyar el proceso de análisis de impacto al negocio.
- Analizar los resultados para determinar las brechas entre los requerimientos de la entidad y su capacidad para ofrecer esos requerimientos.

#### **Metas**

Proveer garantía de que, en el caso de una interrupción, los procesos de continuidad del negocio asegurarán el reinicio a su debido tiempo de los servicios de TI mientras que se minimiza el impacto sobre el negocio.

Entender los diferentes procesos del negocio, identificando el nivel de impacto de parada de una actividad de negocio que afecta las operaciones, cumplimiento legal contractual, Ingresos financieros, reputación, marca y el trabajo de los recursos y talentos humanos.

## Propósito

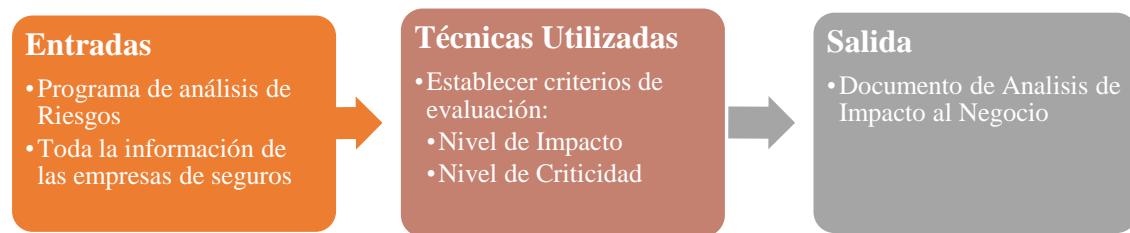
El BIA es un paso crítico para desarrollar el BCM. Esta etapa implica identificar los diversos eventos que pueden tener un impacto sobre la continuidad de las operaciones y su impacto financiero, humano, legal y de reputación sobre la organización.

El propósito para el desarrollo del presente programa de Análisis de Impacto del Negocio, se establece por:

- Dar soporte al Modelo Gestión de Continuidad del Negocio (BCM)
- Lograr un entendimiento de la organización, de los procesos claves del negocio y de los recursos de Seguridad Informática utilizados para soportarlos.
- Establecer la criticidad de los recursos de información (Datos, Aplicaciones, Tecnologías, Instalaciones, Recursos Humanos) que dan soporte a los procesos críticos del negocio.
- Garantizar el cumplimiento de la organización con requisitos legales y regulatorios
- Ayudar a la preparación del plan para la continuidad del Negocio

## Alcance de la técnica de Análisis de Impacto al Negocio

La **Figura No. 42**, muestra el **proceso para definir el alcance de la técnica de Análisis de Impacto al Negocio**.



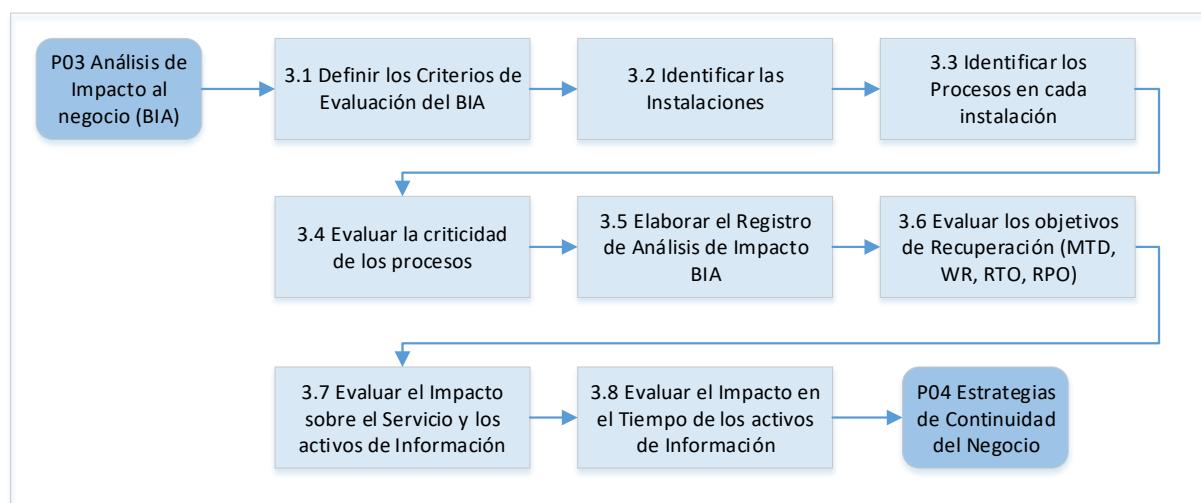
**Figura No. 42.** Alcance de la técnica de Análisis de Impacto al Negocio  
**Fuente:** Elaboración Propia, 2019

## Metodología

El BIA implica determinar las labores y los recursos esenciales para respaldar la continuidad del negocio, su criticidad, su impacto para el negocio.

Para desarrollar el Análisis de Impacto al negocio (BIA) del Grupo Empresarial de Inversiones Nacional Vida S.A. y para dar soporte particular a los requisitos del Modelo de Gestión de Continuidad del Negocio (BCM), se utiliza como directriz la metodología del BCI (*Business Continuity Institute*).

**La Secuencia de tareas de la etapa de Análisis de Impacto al negocio (BIA), se muestra en la Figura No. 43.**



**Figura No. 43.** Secuencia de tareas de Análisis de Impacto al negocio (BIA).

Fuente: Elaboración Propia, 2019

## Proceso de Análisis de Impacto al Negocio (BIA)

### 1) Definir los Criterios de Evaluación del Análisis de Impacto del Negocio

#### Criterios de Evaluación del Impacto

Con el fin de determinar el nivel de impacto en el negocio, se definen los siguientes aspectos:

### **Resumen x Periodo de Impacto:**

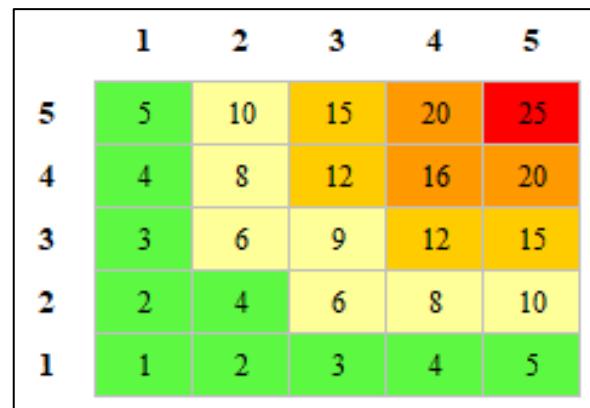
Si la suma de la fila TOTAL en el **FRM de Análisis de Elementos de Servicios Críticos para el Análisis de Impacto al negocio (BIA)**, es mayor de 15 afectará el Periodo de Impacto.

En el **Cuadro No. 38**, se detallan el **valor por periodo de impacto**, y en la **Figura No. 44**, se muestra la Matriz de calor por periodo de impacto.

**Cuadro No. 38.** Valor por periodo de impacto

Valor	Color	Periodo de Impacto
21 a 25	Rojo	Muy Grave
16 a 20	Naranja	Grave
12 a 15	Amarillo	Medio
6 a 10	Límon	Bajo
0 a 5	Verde	Muy Bajo

Fuente: Elaboración Propia, 2019



**Figura No. 44.** Matriz de calor por periodo de impacto  
Fuente: Elaboración Propia, 2019

### **Resumen x Tipo de Actividad de Negocio:**

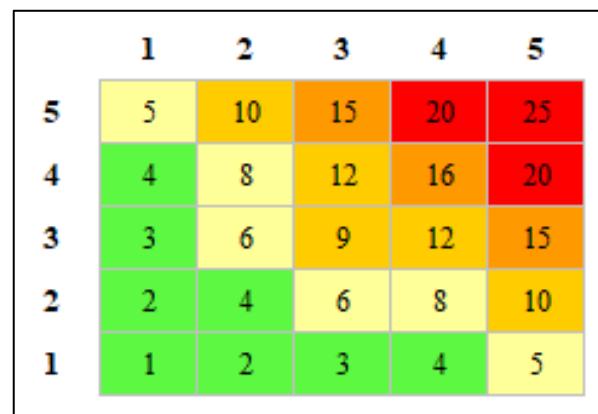
Si la suma de la columna TOTAL es mayor de 12 afectará el Tipo de Actividad de Negocio. Se debe validar que los valores estén por debajo del RTO, caso contrario se recomienda un estudio de Análisis de Riesgo más exhaustivo.

En el **Cuadro No. 39**, se detallan el **valor por tipo de actividad**, y en la **Figura No. 45**, se muestra la Matriz de calor por tipo de Actividad.

**Cuadro No. 39.** Valor por tipo de Actividad

Valor	Color	Actividad de Impacto
20 a 25	Rojo	Muy Grave
13 a 16	Naranja	Grave
9 a 12	Amarillo	Medio
5 a 8	Límon	Bajo
1 a 4	Verde	Muy Bajo

Fuente: Elaboración Propia, 2019



**Figura No. 45.** Matriz de calor por tipo de Actividad

Fuente: Elaboración Propia, 2019

## Criterios de Criticidad

Con el fin de determinar el grado de daño o pérdida para la organización, causados por un evento de seguridad de la información, se definen los siguientes criterios de impacto.

En el **Cuadro No. 40**, se describe el Nivel de criticidad por tipo de Impacto.

**Cuadro No. 40.** Nivel del Criticidad por Tipo de Impacto

VALOR	NIVEL	FINANCIERO	OPERATIVO	IMAGEN	NORMATIVO	HUMANO
Muy Bajo	1	Sin impacto	Sin impacto	Sin impacto	Sin impacto	Sin impacto
Bajo	2	Pérdidas mensuales por	Dificulta la realización de los procesos internos.	Repercusión interna, no afecta a las	Apercibimiento legal.	Afecta levemente a algunos empleados.

VALOR	NIVEL	FINANCIERO	OPERATIVO	IMAGEN	NORMATIVO	HUMANO
		valor inferior a 10,000 \$us		unidades de negocio		
Medio	3	Pérdidas mensuales por valor de 10,000 \$us hasta 100,000 \$us	Interrupción de servicios internos; el cliente no se ve afectado.	Repercusión interna, afecta a áreas de Negocio	Apertura de expediente disciplinario o procedimiento sancionador	Afecta a varios empleados de un sector / área de la Compañía.
Alto	4	Pérdidas mensuales por valor de 100,000 \$us hasta 1,000,000 \$us	Interrupción de servicios internos y externos; el cliente se ve afectado.	Repercusión en los clientes	Apertura de expediente o procedimiento con repercusión económica	Afecta gravemente a empleados de la Compañía
Muy Alto	5	Pérdidas mensuales por valor mayor de 1,000.000 \$us	Interrupción continua del servicio; afecta a la continuidad de Negocio	Trascendencia al exterior, precisa de notificación a los medios de comunicación.	Resolución que obliga a rescindir, eliminar o rehacer actividades del Negocio	Provoca movilizaciones, protestas y consecuencias organizativas

Fuente: Elaboración Propia, 2019

## Categoría de Procesos

En el **Cuadro No. 41**, se muestran las **categorías de procesos** con su respectiva descripción.

**Cuadro No. 41.** Categorías de procesos

Categoría	Descripción
CRÍTICOS	Funciones que pueden realizarse sólo si las capacidades se remplazan por otras similares o idénticas. No pueden remplazarse por métodos manuales. Muy baja tolerancia a interrupciones.
VITALES	Pueden realizarse manualmente por un periodo breve. Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 o menos días, por ejemplo).
SENSITIVOS	Funciones que pueden realizarse manualmente por un periodo prolongado a un costo tolerable. El proceso manual puede ser complicado y requeriría de personal adicional.
NO CRÍTICOS	Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

Fuente: Elaboración Propia, 2019

## 2) Identificar Instalaciones

### [L] Instalaciones (Ámbito Geográfico)

Se validan las instalaciones físicas donde opera la empresa a nivel nacional.

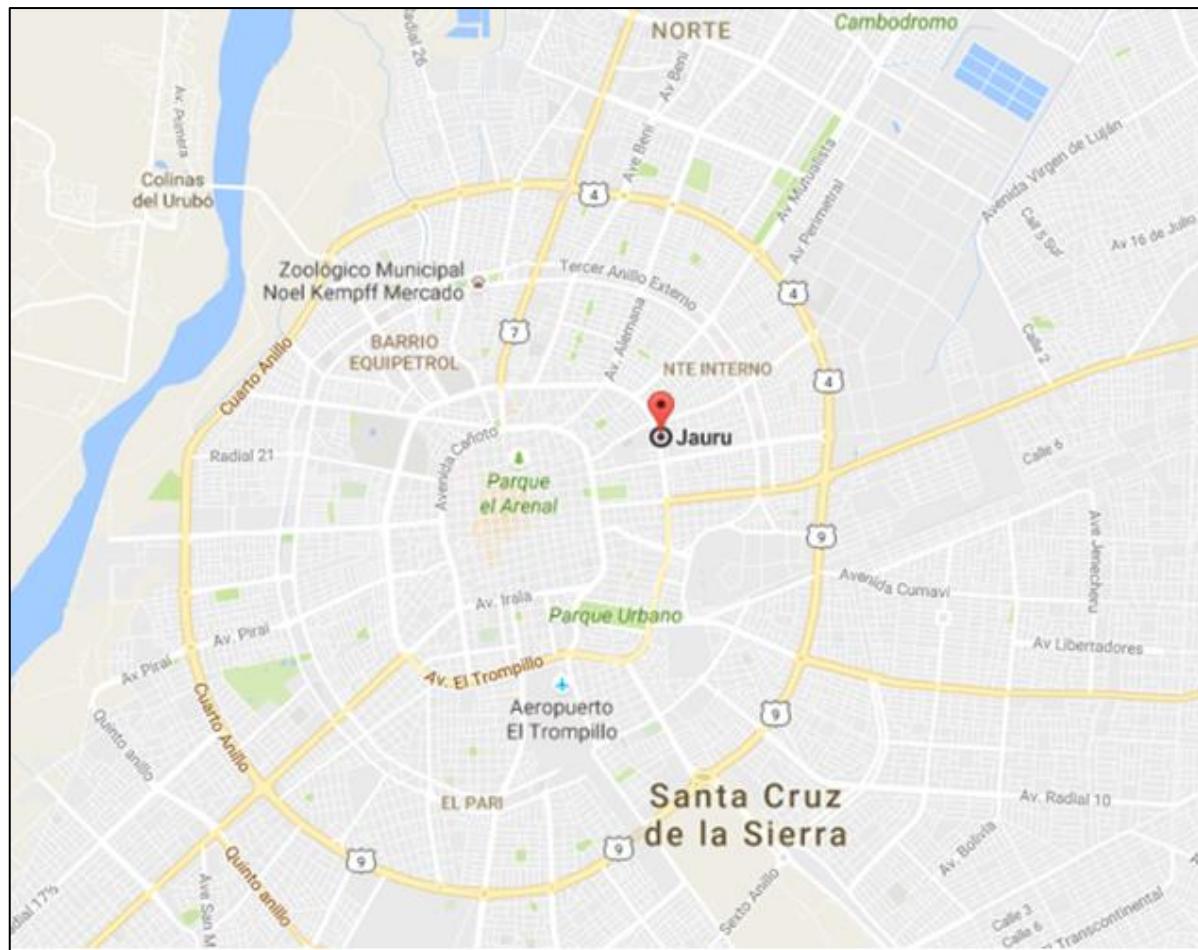
Los aspectos referidos a las [L] Instalaciones (ámbito geográfico) de la empresa, fueron definidos en la sección 3.2.1 **Ámbito Tecnológico**

#### Ubicación del sitio principal

##### Dirección: Oficina Central Santa Cruz

Av. Santa Cruz 2do anillo, Esq. Jaurú N. 333, entre Av. Paraguá y Av. Canal Cotoca

En la **Figura No. 46**, se muestra el **Mapa de ubicación del Sitio Principal**



**Figura No. 46.** Mapa de ubicación del Sitio Principal

Fuente: Google Maps, 2019

**3) Identificar los procesos Críticos del sitio Principal**

- **Gestión Comercial:** Contacto con clientes, comercialización de productos, mantener la operación del negocio
- **Gestión de Cobranzas:** Realizar la cobranza, emitir facturas y recibos, mantener el flujo de caja
- **Gestión de Siniestros:** Recibir las denuncias, evaluar documentación, realizar el pago de siniestros, evitar problemas legales, sanciones y multas

**4) Evaluar la criticidad de los procesos**

Se evalúa la criticidad de cada uno de los procesos identificados relacionados con la empresa.

**Proceso Crítico: Gestión Comercial**

En el

**Cuadro No. 42,** se detalla el Análisis del Proceso crítico de gestión de **Comercial**, se evalúan las funciones críticas, personas, dependencias con recursos de tecnologías, amenazas, vulnerabilidades y los tiempos de recuperación.

**Cuadro No. 42.** Análisis del proceso crítico de gestión Comercial

<b>Unidad de Negocio</b>	<b>NACIONAL SEGUROS VIDA Y SALUD S.A</b>	<b>Objetivo Punto de Recuperación (RPO)</b> : [ 24 hr ] <b>Ventana de Recuperación (WR)</b> : [ 08 hr ] <b>Caída Maxima Tolerable (MTO)</b> : [ 40 hr ] <b>Objetivo Tiempo de Recuperación (RTO)</b> : [ 48 hr ]
<b>Proceso Crítico</b>	<b>Gestión Comercial</b>	
<b>Descripción del Proceso:</b>	Contacto con clientes, comercialización del producto <b>Mantener la operación del negocio</b>	
<b>Funciones Críticas</b>	1. Comercializar productos individuales	1. Comercializar productos corporativos
<b>Personas</b>	1. Agente	1. Brokers
<b>Dependencia con Recursos de Tecnología</b>	SW : eLife, eSalud, VidaFlexible, HW : Serv DB, Serv App, PBX COM: Red Local Tx de Datos (Regional)	SW : Cotizador Web, eMail HW : PC Local, impresora COM: Acceso a Internet
<b>Amenazas</b>	Desastre Natural Incendio Conmoción Social/Paro cívico Proveedor Tx Datos Ingeniería Social	Desastre Natural Conmoción Social/Paro cívico Hacking/Phishing Internet Ingeniería Social Proveedor Internet
<b>Vulnerabilidad</b>	104 Motivación del Personal Interno 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Info.	101 Identificación del Atacante 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Información

**Fuente:** Elaboración Propia, 2019

### Proceso Crítico: Gestión de Cobranzas

En el **Cuadro No. 43**, se detalla el Análisis del Proceso crítico de gestión de **cobranzas**, se evalúan las funciones críticas, personas, dependencias con recursos de tecnologías, amenazas, vulnerabilidades y los tiempos de recuperación.

**Cuadro No. 43.** Análisis del proceso crítico de gestión de Cobranzas

<b>Unidad de Negocio</b>	<b>NACIONAL SEGUROS VIDA Y SALUD S.A</b>		<b>Objetivo Punto de Recuperación (RPO) : [ 24 hr ]</b>
<b>Proceso Crítico</b>	<b>Cobranzas</b>		<b>Ventana de Recuperación (WR) : [ 08 hr ]</b>
<b>Descripción del Proceso</b>	<b>Realizar la cobranza, emitir las facturas y recibos</b>		<b>Caída Maxima Tolerable (MTO) : [ 40 hr ]</b>
	<b>Mantener el Flujo de Caja</b>		<b>Objetivo Tiempo de Recuperación (RTO) : [ 48 hr ]</b>
<b>Funciones Críticas</b>	1. Contacto de Cobranza 2. Agendamiento de cobranza 3. Cobranzas previstas diarias	1. Cobranza	1. Hoja de Ruta
<b>Personas</b>	1. Agente Call Center 2. Supervisor de Cobranza 3. Jefe de Operaciones	1. Cajero (Sistema) 2. Cobrador	1. Cobrador
<b>Dependencia con Recursos de Tecnología</b>	SW : SSP, eLife, eSalud, VidaFlexible, Uponsoft HW : Serv DB, Serv App, PBX COM: Red Local Tx de Datos (Regional)	SW : SSP, eLife, eSalud, VidaFlexible Cobranza Movil, UponSoft HW : Serv DB, Serv App, PC Local, POS COM: Red Local, GSM	SW : Cobranza Movil HW : Celular, impresora, POS COM: Red GSM
<b>Amenazas</b>	Desastre Natural Incendio Conmoción Social/Paro cívico Proveedor Tx Datos Ingeniería Social	Desastre Natural Robo Conmoción Social/Paro cívico Sobrecarga del Sistema (GSM)	Desastre Natural, Incendio Conmoción Social/Paro cívico Virus Sobrecarga del Sistema (Tx Datos GPRS)
<b>Vulnerabilidad</b>	101 Identificación del Atacante 104 Motivación del Personal Interno 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Info.	101 Identificación del Atacante 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Información	101 Identificación del Atacante 105 Permisos de Usuarios 111 Conectividad del Sistema Info.

Fuente: Elaboración Propia, 2019

## Proceso Crítico: Gestión de Siniestros

En el **Cuadro No. 44**, se detalla el **Análisis del Proceso crítico de Gestión de Siniestros**, se evalúan las funciones críticas, personas, dependencias con recursos de tecnologías, Amenazas, vulnerabilidades y los tiempos de recuperación.

**Cuadro No. 44.** Análisis del proceso crítico de Gestión de Siniestros

<b>Unidad de Negocio</b> : NACIONAL SEGUROS VIDA Y SALUD S.A <b>Proceso Crítico</b> : Gestión de Siniestros <b>Descripción del Proceso</b> : Recibir las denuncias, evaluar doc., pago de siniestros <b>Evitar problemas legales, sanciones y multas</b>		Objetivo Punto de Recuperación (RPO) : [ 24 hr ] Ventana de Recuperación (WR) : [ 08 hr ] Caída Máxima Tolerable (MTO) : [ 40 hr ] Objetivo Tiempo de Recuperación (RTO) : [ 48 hr ]	
Funciones Críticas	1. Recepción de Denuncias 2. 3.	1. Relevar Documentacion 2. Evaluar 3.	1. Indemnizar 2. 3.
Personas	1. Plataforma de atención ATC 2. Agente Call Center	1. Supervisor de siniestros 2. Auditores médicos	1. Ejecutivos de siniestros 2. Departamento contable
Dependencia con Recursos de Tecnología	SW : eLife, eSalud, VidaFlexible, UponSoft HW : Serv DB, Serv App, PBX COM: Red Local Tx de Datos (Regional)	SW : eLife, eSalud, VidaFlexible, HW : Serv DB, Serv App, PBX COM: Red Local Tx de Datos (Regional)	SW : UponSoft HW : Serv DB, Serv App, PBX COM: Red Local Tx de Datos (Regional)
Amenazas	Desastre Natural, Incendio Conmoción Social/Paro cívico Proveedor Tx Datos Ingeniería Social	Desastre Natural, Incendio Conmoción Social/Paro cívico Proveedor Tx Datos	Desastre Natural, Incendio Robo Conmoción Social/Paro cívico
Vulnerabilidad	101 Identificación del Atacante 104 Motivación del Personal Interno 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Info.	101 Identificación del Atacante 104 Motivación del Personal Interno 105 Permisos de Usuarios (derechos) 111 Conectividad del Sistema Información	101 Identificación del Atacante 105 Permisos de Usuarios 111 Conectividad del Sistema Info.

**Fuente:** Elaboración Propia, 2019

## 5) Elaborar el Registro de Análisis de Impacto (BIA)

Para el registro del Análisis de Impacto (BIA), se desarrolló el formulario de Análisis de Elementos de Servicios Críticos que Impactan al Negocio.

De un total de 48 registros del análisis de Impacto BIA, se adjunta un ejemplo en el **Anexo No. 25, FRM de Análisis de Elementos de Servicios Críticos para el Análisis de Impacto al negocio (BIA)**.

## Diccionario de Datos del Formulario BIA

El Cuadro No. 45, describe la denominación general del Activo de Información.

**Cuadro No. 45. BIA- Denominación general del Activo de Información**

Item.	Campo	Descripción
1.1	Denominación del Activo de información:	Nombre del elemento del Servicio Crítico
1.2	Principales aplicaciones soportadas por el servicio	Aplicaciones principales incluidas como nuevo elemento crítico
1.3	Descripción, Comentarios y Observaciones acerca del Elemento de Servicio Crítico	Señala características del servicio, comentarios y observaciones pertinentes.
1.4	Fecha de la última actualización	Mes, Año
1.5	Costo (Valor Comercial) \$us.	Valor comercial del elemento de servicio o monto necesario para adquirir el bien
	Criticidad Actual	Valores (Sin valorar; Muy Baja; Baja; Media; Alta; Muy Alta)
1.6	Unidad de Negocio	Unidad de negocio a la que está asociada el activo (Sistema o recurso crítico)
1.7	Responsable en la Cuenta	Responsable principal de la Cuenta
1.8	Gestor del Servicio	Responsable de la relación con el cliente y de identificar las necesidades y expectativas del negocio.
1.9	Responsable Usuario	Interlocutor por parte del Usuario Final
1.10	¿Existen mecanismos para realizar la actividad de negocio o soportar el procesamiento con sistemas reducidos o alternos?	Mecanismo manual independiente al Sistema de Información. Conjunto de preguntas para determinar el RTO (Recovery Time Objetive) “¿Cuál es el tiempo de tolerancia a la interrupción?”
1.11	Si la respuesta anterior es afirmativa. ¿Cuánto tiempo se puede trabajar utilizando los procedimientos alternativos? (MTD)	Tiempo Estimado: xxxx Elegir de la lista; No Aplica; Días; Horas
1.12	Relación de ubicaciones (Sucursales o Agencias) donde se encuentran las personas que realizan la función de negocio	Agencias o Sucursales y número aprox. de usuarios en cada una de ellas.

Fuente: Elaboración Propia, 2019

El Cuadro No. 46, describe la Disponibilidad del Elemento de Servicio.

**Cuadro No. 46. BIA- Disponibilidad del Elemento de Servicio**

Item.	Campo	Descripción
2.1	Acuerdo de Nivel de Servicio existente	Indica si existe un SLA (Acuerdo de Nivel de Servicio) firmado.
	Calendario	Ejemplo 24x7 (365)
	Disponibilidad (%)	Ejemplo de Uptime: 0.99 (8 hr/mes, 2 hr/sem, 0.5 hr/día)
	Tiempo de Respuesta	Ejemplo: Crítica 4 Hr , Alta 8 Hr, Media 24 Hr, Baja 48 Hr

Fuente: Elaboración Propia, 2019

El **Cuadro No. 47**, describe los parámetros de recuperación.

**Cuadro No. 47.** BIA- Parámetros de Recuperación

Item.	Campo	Descripción
3.1	¿En cuánto tiempo se debe disponer de un nivel mínimo de prestación del ELEMENTO DE SERVICIO? (WR)	Desde la interrupción del servicio
3.2	¿En cuánto tiempo deben estar recuperadas totalmente las prestaciones del ELEMENTO DE SERVICIO? (RTO)	Desde la interrupción del servicio
3.3	¿Cuánta es la pérdida de información que puede soportar el negocio? (RPO)	0' => copia síncrona de datos > '0' => horas para la restauración del <i>backup</i>
3.4	Indicar el número mínimo imprescindible de usuarios conectados al mismo tiempo al Elemento de Servicio en situación de servicio degradado	Preguntas para dimensionar la solución alternativa necesaria (Sección 1.12)
3.5	¿Qué porcentaje sobre el total de usuarios son los anteriores?	Preguntas para dimensionar la solución alternativa necesaria (Sección 1.12)

Fuente: Elaboración Propia, 2019

El **Cuadro No. 48**, describe los niveles de impacto.

**Cuadro No. 48.** BIA- Niveles de Impacto

Item.	Campo	Descripción
4.1	Impacto de parada de actividad de negocio	Para determinar el Costo económico se debe tener en cuenta tanto las pérdidas de beneficios como los costos asociados a la parada
	Impacto Financiero	Valores para: (1 HORA, 1 DIA, 1 SEMANA, 1 MES), La escala permisible: (Elegir de la lista;--;1;2;3;4;5)
	Impacto Operativo	Valores para: (1 HORA, 1 DIA, 1 SEMANA, 1 MES), La escala permisible: (Elegir de la lista;--;1;2;3;4;5)
	Impacto Imagen y/ reputación	Valores para: (1 HORA, 1 DIA, 1 SEMANA, 1 MES), La escala permisible: (Elegir de la lista;--;1;2;3;4;5)
	Impacto Normativo, Legal	Valores para: (1 HORA, 1 DIA, 1 SEMANA, 1 MES), La escala permisible: (Elegir de la lista;--;1;2;3;4;5)
	Impacto Laboral, Talentos Humanos	Valores para: (1 HORA, 1 DIA, 1 SEMANA, 1 MES), La escala permisible: (Elegir de la lista;--;1;2;3;4;5)

Fuente: Elaboración Propia, 2019

El **Cuadro No. 49**, describe la interrupción del servicio.

**Cuadro No. 49.** BIA - Interrupción del Servicio

Item.	Campo	Descripción
5.1	Legislación: ¿Existe alguna legislación que no sería cumplida por falta de servicio? ¿Cuál?	p. ej: Pago de impuestos ASFI, APS, SIN, SOX, ISO9001, ISO2700
5.2	Relación de otros Elementos de Servicio imprescindibles para la realización de la actividad de negocio (Interfaces y necesidades de información de otros sistemas)	Interfaces y dependencias con otros sistemas (Validar con el FRM de Análisis de Riesgos)
5.3	Proveedores: ¿Existe algún contrato y/o acuerdo con proveedores de servicio? Indicar las dependencias de proveedores externos para brindar el servicio	Interfaces y dependencias con otros sistemas dependientes de proveedor
5.4	¿Existe alguna posibilidad, de recuperar los datos previamente introducidos en el sistema informático?	Independientemente de los respaldos que se realizan por parte de Sistemas de Información
5.5	En caso de respuesta afirmativa a la pregunta anterior ¿qué mecanismo se utilizaría para recuperarlos? (Breve descripción)	Introducción manual de datos, realimentación desde un sistema externo
5.6	Si existe mecanismo alternativo de recuperación (RPO) ¿hasta dónde se podrían recuperar los datos introducidos antes de un incidente? (todos los datos / hasta las últimas X horas)	Preguntas para determinar el RPO ( <i>Recovery Point Objective</i> ) “¿Qué tan actualizados necesitan estar los datos?”
5.7	¿Hay algún periodo de tiempo en el que la criticidad del Elemento de Servicio sea mayor? (Períodos de tiempo, y/o fechas)	Pregunta para hacer un mapa de criticidad variable a fin de establecer prioridades en la recuperación

Fuente: Elaboración Propia, 2019

El **Cuadro No. 50**, describe la línea de tendencia de los siguientes 12 meses.

**Cuadro No. 50.** BIA - Línea de Tendencia (Siguientes 12 meses)

Item.	Campo	Descripción
6.1	La carga de trabajo del Elemento de Servicio	Valores Permitidos: (Aumentara, Se Mantendrá, Disminuirá)
6.2	El número de usuarios	Valores Permitidos: (Aumentara, Se Mantendrá, Disminuirá)
6.3	El número de transacciones diarias	Valores Permitidos: (Aumentara, Se Mantendrá, Disminuirá)

Fuente: Elaboración Propia, 2019

## 6) Evaluar los objetivos de recuperación (MTD, WR, RTO, RPO)

Se evalúan los tiempos de recuperación y el tiempo máximo tolerable fuera de servicio para cada proceso dependiente de los activos de información. En el **Cuadro No. 51**, se

realiza la evaluación de los **Objetivos de recuperación** (MTD, WR, RTO, RPO), sobre los activos de Información .

**Cuadro No. 51.** Objetivos de recuperación (MTD, WR, RTO, RPO)

Dominios	ID	Elemento	Criticidad	MTD	WR	RTO	RPO
<b>Procesos</b>							
	P1	Proceso Cobranzas	Muy Alta	48	Horas	8	Horas
	P2	Proceso Comercialización	Muy Alta	48	Horas	8	Horas
	P3	Proceso Gestión de Siniestros	Muy Alta	48	Horas	8	Horas
<b>Documentos</b>							
	D11	Documento Uso Público	Baja				
	D12	Documento Uso Interno	Media				
	D13	Documento Confidencial	Alta				
	D14	Documento Secreto	Muy Alta				
<b>[SW] Aplicaciones</b>							
	SI21	Infraestructura de Colaboración	Muy Alta	8	Horas	4	Horas
	SW31	Sistema de Aplicación (ERP)	Muy Alta	2	Días	8	Horas
	SW32	Motor de base de Datos ( <i>SQL Server</i> )	Muy Alta	2	Días	8	Horas
	SW33	Servicio de Publicación ( <i>IIServer</i> )	Muy Alta	2	Días	8	Horas
	SW34	Sistemas Operativos de Red	Muy Alta	2	Días	8	Horas
	SW35	Suite Ofimática del Usuario	Media	2	Días	8	Horas
	SW36	Utilitarios	Baja	5	Días	48	Horas
<b>[HW] Equipos</b>							
	HW51	Servidor Físico/Virtual	Muy Alta	2	Días	8	Horas
	HW52	Switch (comutador)	Muy Alta	2	Días	8	Horas
	HW53	Router (Enrutador)	Muy Alta	4	Días	2	Días
	HW54	Firewall (Pared de Fuego)	Muy Alta	2	Días	8	Horas
	HW55	Fbridge/Transceiver (Conversor OE)	Muy Alta	4	Días	8	Horas
	HW56	PBX (Central Telefónica)	Muy Alta	2	Días	8	Horas
	HW57	Modem ADSL (Equipo de Modulación)	Muy Alta	4	Días	8	Horas

Dominios	ID	Elemento	Criticidad	MTD		WR		RTO		RPO
	HW58	Equipo Computador (PC Escritorio/Portátil)	Media	4	Días	8	Horas	2	Días	> de 24
	HW59	Equipos Utilitarios (Data Show, Impresora, Escáner)	Baja	4	Días	8	Horas	2	Días	No Aplica
<b>[COM] Comunicaciones</b>										
	COM71	Red Lan (Local/Wireless)	Alta	4	Días	8	Horas	5	Días	No Aplica
	COM72	Enlace F.O (Tx Voz/Datos)	Alta	4	Días	8	Horas	5	Días	No Aplica
	COM73	Enlace E1 (Tx Voz)	Alta	8	Horas	8	Horas	2	Días	No Aplica
	COM74	Enlace Internet (ADSL/OnLine)	Media	4	Días	8	Horas	2	Días	No Aplica
	COM75	Radio Enlace (Tx Datos, Respaldo)	Media	4	Días	4	Horas	5	Días	> de 24
	COM76	Link Nacional (Punto a Punto/FR)	Media	4	Días	8	Horas	5	Días	> de 24
	COM77	Red Privada Virtual (VPN Site2Site, Client2Site)	Media	4	Días	8	Horas	5	Días	> de 24
<b>[AUX] Auxiliares</b>										
	AUX91	Aire Acondicionado	Muy Alta	1	Días	4	Horas	2	Días	No Aplica
	AUX92	UPS (Sistema Ininterrumpido de Energía)	Muy Alta	2	Días	8	Horas	2	Días	No Aplica
	AUX93	Energía No Regulada	Alta	7	Días	2	Horas	2	Días	No Aplica
	AUX94	Sistemas Esenciales (Iluminación, Alarms)	Media	2	Días	8	Horas	4	Días	No Aplica
<b>Servicios Subcontratados</b>										
	SS101	Servicios Generales (Seguridad Física, Limpieza, Mantenimiento)	Media	2	Días	48	Horas	2	Días	No Aplica
	SS102	Holding (RRHH, Legal, Auditoria)	Media	2	Días	48	Horas	4	Días	> de 24
	SS103	Proveedores de Telecomunicaciones	Alta	2	Días	48	Horas	5	Días	No Aplica
<b>Sitios</b>										
	L111	Sitio Central	Alta	30	Días	5	Días	1	Meses	No Aplica
	L112	Sitio Alterno	Media	30	Días	2	Días	1	Meses	No Aplica

Dominios	ID	Elemento	Criticidad	MTD		WR		RTO		RPO
	L113	Agencias Locales/Regionales	Alta	30	Días	2	Días	1	Meses	No Aplica
<b>Personas</b>										
	P121	Usuario Interno (Local/Remoto/Regional)	Alta	30	Días	2	Días	1	Meses	> de 24
	P122	Usuario Externo (Internet/Móvil)	Media	4	Días	48	Horas	5	Días	> de 24
	P123	Soporte L1 ( <i>Help Desk</i> Técnico de Soporte)	Alta	4	Días	1	Días	1	Semanas	> de 24
	P124	Soporte L2 (Administradores IT)	Alta	4	Días	2	Días	2	Semanas	> de 24

Fuente: Elaboración Propia, 2019

## 7) Evaluar el impacto sobre el Servicio y los Activos de información

Se evalúa el impacto sobre el servicio: Directos (Financiero, Operativo) e Indirectos (Imagen, Normativo-Legal, Personal, Impacto Total), definidos en el **Cuadro No. 30.** Tabla de valoración de impactos.

En el **Cuadro No. 52**, se muestra la Evaluación de impactos sobre los activos de información.

Según el análisis, los dominios: Proceso (P3), Aplicaciones (SW31, SW34), Equipos (HW51, HW52, HW54), Comunicaciones (COM71, COM72, COM76), Auxiliares (AUX93), Sitios (L111), son los activos de información que más impactan a la empresa de manera directa o indirecta.

**Cuadro No. 52.** Análisis de Impacto sobre los activos de información (FOINLP)

Dominio	ID	Elemento	FIN	OPE	IMA	NOR	HUM	Σ
<b>Procesos</b>								
	P1	Proceso Cobranzas	18	15	14	14	15	76
	P2	Proceso Comercialización	15	14	15	15	16	75
	P3	Proceso Gestión de Siniestros	14	13	17	18	15	77
<b>Documentos</b>								
	D11	Documento Uso Publico						
	D12	Documento Uso Interno						
	D13	Documento Confidencial						

Dominio	ID	Elemento	FIN	OPE	IMA	NOR	HUM	Σ
	D14	Documento Secreto						
<b>[SW] Aplicaciones</b>								
	SI21	Infraestructura de Colaboración	13	13	13	10	10	59
	SW31	Sistema de Aplicación (ERP)	15	18	13	18	16	80
	SW32	Motor de base de Datos ( <i>SQL Server</i> )	9	16	7	15	11	58
	SW33	Servicio de Publicación ( <i>IIServer</i> )	9	16	7	15	11	58
	SW34	Sistemas Operativos de Red	14	18	14	18	14	78
	SW35	Suite Ofimática del Usuario	9	16	7	15	11	58
	SW36	Utilitarios	4	6	3	4	6	23
<b>[HW] Equipos</b>								
	HW51	Servidor Físico/Virtual	15	18	13	18	16	80
	HW52	Switch (comutador)	15	18	13	18	16	80
	HW53	Router (Enrutador)	15	12	9	14	12	62
	HW54	Firewall (Pared de Fuego)	14	17	13	17	16	77
	HW55	Fibridge/Transceiver (Conversor OE)	10	16	7	15	12	60
	HW56	PBX (Central Telefónica)	14	14	13	14	8	63
	HW57	Modem ADSL (Equipo de Modulación)	13	13	13	13	8	60
	HW58	Equipo Computador (PC Escritorio / Portátil)	13	13	12	10	10	58
	HW59	Equipos Utilitarios ( <i>Data Show</i> , Impresora, Escáner)	13	13	11	10	10	57
<b>[COM] Comunicaciones</b>								
	COM71	Red Lan (Local/Wireless)	16	14	16	14	14	74
	COM72	Enlace F.O (Tx Voz/Datos)	17	14	17	14	10	72
	COM73	Enlace E1 (Tx Voz)	13	15	15	10	15	68
	COM74	Enlace Internet (ADSL/ <i>OnLine</i> )	14	15	15	10	14	68
	COM75	Radio Enlace (Tx Datos, Respaldo)	10	10	13	10	10	53
	COM76	Link Nacional (Punto a Punto/FR)	14	16	15	15	16	76
	COM77	Red Privada Virtual ( VPN Site2Site, Client2Site)	9	6	14	6	6	41
<b>[AUX] Auxiliares</b>								
	AUX91	Aire Acondicionado	13	15	13	13	13	67
	AUX92	UPS (Sistema Ininterrumpido de Energía)	14	16	14	16	14	74
	AUX93	Energía No Regulada	15	17	15	17	15	79
	AUX94	Sistemas Esenciales (Iluminación, Alarmas)	15	9	6	10	6	46
<b>Servicios Subcontratados</b>								
	SS101	Servicios Generales (Seguridad Física, Limpieza, Mantenimiento)	10	14	10	14	10	58
	SS102	Holding (RRHH, Legal, Auditoria)	10	10	10	14	10	54
	SS103	Proveedores de Telecomunicaciones	10	17	14	14	14	69

Dominio	ID	Elemento	FIN	OPE	IMA	NOR	HUM	Σ
<b>Sitios</b>								
	L111	Sitio Central	14	17	14	14	17	76
	L112	Sitio Alterno	14	14	14	14	14	70
	L113	Agencias Locales/Regionales	14	14	14	10	14	66
<b>Personas</b>								
	P121	Usuario Interno (Local/Remoto/Regional)	10	6	6	10	10	42
	P122	Usuario Externo ( <i>Internet/Móvil</i> )	10	6	6	10	10	42
	P123	Soporte L1 ( <i>Help Desk</i> Técnico de Soporte)	10	10	10	10	10	50
	P124	Soporte L2 (Administradores IT)	14	14	14	14	10	66

Fuente: Elaboración Propia, 2019

## 8) Evaluar el Impacto en el Tiempo de los Activos de información

En el **Cuadro No. 53**, se muestra el **Análisis de Impacto en el Tiempo** sobre los activos de información, que brinda la priorización para las estrategias de recuperación.

Según el análisis en el tiempo: Los Dominios (Procesos, Aplicaciones, Equipos, Comunicaciones, Auxiliares, Servicios Subcontratados, Sitios, Personas) son los activos de información que más impactan a la empresa, de manera **Grave** a partir de 1 día y **Muy Grave** a partir de 1 Semana de indisponibilidad del Servicio o del activo de información.

**Cuadro No. 53.** Análisis de Impacto en el Tiempo

Dominio	ID	Elemento	1 HR	1 DIA	1 SEM	1 MES
<b>Procesos</b>						
	P1	Proceso Cobranzas	Muy Bajo	Medio	Grave	Muy Grave
	P2	Proceso Comercialización	Muy Bajo	Medio	Grave	Muy Grave
	P3	Proceso Gestión de Siniestros	Bajo	Grave	Muy Grave	Muy Grave
<b>Documentos</b>						
	D11	Documento Uso Público				
	D12	Documento Uso Interno				
	D13	Documento Confidencial				
	D14	Documento Secreto				
<b>[SW] Aplicaciones</b>						
	SI21	Infraestructura de Colaboración	Muy Bajo	Medio	Grave	Muy Grave
	SW31	Sistema de Aplicación (ERP)	Medio	Grave	Muy Grave	Muy Grave
	SW32	Motor de base de Datos ( <i>SQL Server</i> )	Medio	Grave	Muy Grave	Muy Grave

Dominio	ID	Elemento	1 HR	1 DIA	1 SEM	1 MES
	SW33	Servicio de Publicación ( <i>IIServer</i> )	Medio	Grave	Muy Grave	Muy Grave
	SW34	Sistemas Operativos de Red	Medio	Grave	Muy Grave	Muy Grave
	SW35	Suite Ofimática del Usuario	Muy Bajo	Medio	Grave	Muy Grave
	SW36	Utilitarios		Muy Bajo	Bajo	Medio
<b>[HW] Equipos</b>						
	HW51	Servidor Físico/Virtual	Medio	Grave	Muy Grave	Muy Grave
	HW52	<i>Switch</i> (conmutador)	Medio	Grave	Muy Grave	Muy Grave
	HW53	<i>Router</i> (Enrutador)	Bajo	Medio	Grave	Muy Grave
	HW54	<i>Firewall</i> (Pared de Fuego)	Medio	Grave	Muy Grave	Muy Grave
	HW55	<i>Fibridge/Transceiver</i> (Conversor OE)	Bajo	Medio	Grave	Muy Grave
	HW56	PBX (Central Telefónica)	Bajo	Medio	Grave	Muy Grave
	HW57	Modem ADSL (Equipo de Modulación)	Bajo	Medio	Grave	Grave
	HW58	Equipo Computador (PC Escritorio/Portátil)	Muy Bajo	Medio	Grave	Muy Grave
	HW59	Equipos Utilitarios ( <i>Data Show</i> , Impresora, Escáner)	Muy Bajo	Medio	Grave	Muy Grave
<b>[COM] Comunicaciones</b>						
	COM71	Red Lan (Local/Wireless)	Medio	Grave	Grave	Muy Grave
	COM72	Enlace F.O (Tx Voz/Datos)	Medio	Grave	Muy Grave	Muy Grave
	COM73	Enlace E1 (Tx Voz)	Medio	Medio	Grave	Muy Grave
	COM74	Enlace Internet (ADSL/ <i>OnLine</i> )	Medio	Medio	Grave	Muy Grave
	COM75	Radio Enlace (Tx Datos, Respaldo)	Muy Bajo	Medio	Grave	Muy Grave
	COM76	Link Nacional (Punto a Punto/FR)	Medio	Grave	Grave	Muy Grave
	COM77	Red Privada Virtual ( VPN Site2Site, Client2Site)	Muy Bajo	Bajo	Medio	Grave
<b>[AUX] Auxiliares</b>						
	AUX91	Aire Acondicionado	Bajo	Medio	Muy Grave	Muy Grave
	AUX92	UPS (Sistema Ininterrumpido de Energía)	Bajo	Grave	Muy Grave	Muy Grave
		Energía No Regulada				
	AUX94	Sistemas Esenciales (Iluminación, Alarmas)	Muy Bajo	Bajo	Medio	Grave
<b>Servicios Subcontratados</b>						
	SS101	Servicios Generales (Seguridad Física, Limpieza, Mantenimiento)	Muy Bajo	Medio	Grave	Muy Grave
		<i>Holding</i> (RRHH, Legal, Auditoria)				
		Proveedores de Telecomunicaciones				
<b>Sitios</b>						
	L111	Sitio Central	Medio	Grave	Muy Grave	Muy Grave
	L112	Sitio Alterno	Bajo	Medio	Grave	Muy Grave
	L113	Agencias Locales/Regionales	Bajo	Medio	Grave	Muy Grave

Dominio	ID	Elemento	1 HR	1 DIA	1 SEM	1 MES
<b>Personas</b>						
	P121	Usuario Interno (Local/Remoto/Regional)	Muy Bajo	Bajo	Medio	Grave
	P122	Usuario Externo ( <i>Internet/Móvil</i> )	Muy Bajo	Bajo	Medio	Grave
	P123	Soporte L1 ( <i>Help Desk Técnico de Soporte</i> )	Muy Bajo	Bajo	Medio	Grave
	P124	Soporte L2 (Administradores IT)	Bajo	Medio	Grave	Muy Grave

Fuente: Elaboración Propia, 2019

El Análisis de Riesgos junto al Análisis de Impacto al Negocio, proporcionan una entrada para la selección de Estrategias de Continuidad del Negocio.

### 3.6.4 P04 Estrategias de Continuidad de Negocio

#### Objetivo

Seleccionar las estrategias costo-efectivas para reducir las deficiencias que se encontraron durante los procesos de evaluación de riesgos y de análisis de impacto al negocio.

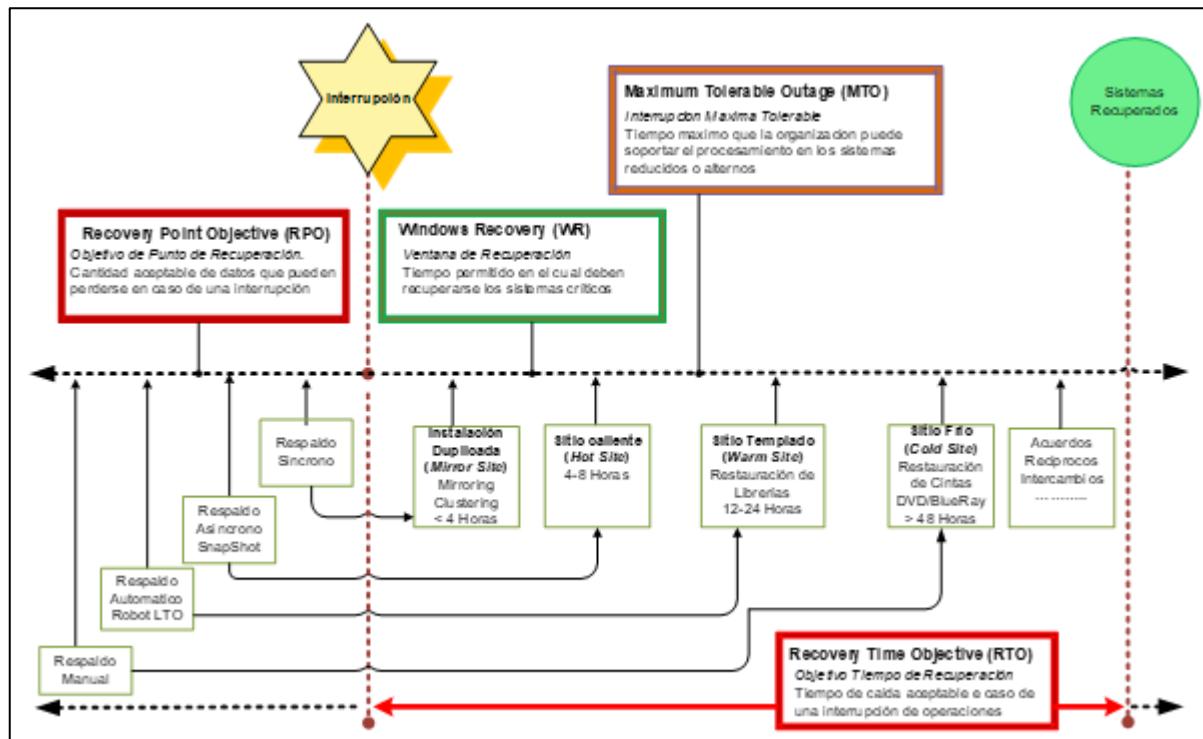
#### Metodología

La Figura No. 47, muestra el **proceso para desarrollar la Estrategia de Continuidad del Negocio.**



**Figura No. 47.** Proceso para desarrollar la Estrategia de Continuidad  
Fuente: Elaboración Propia, 2019

En la **Figura No. 48**, se muestra el escenario de una interrupción y recuperación del servicio, con el fin de ayudar en la definición de las estrategias.



**Figura No. 48.** Escenario de una interrupción y recuperación del servicio

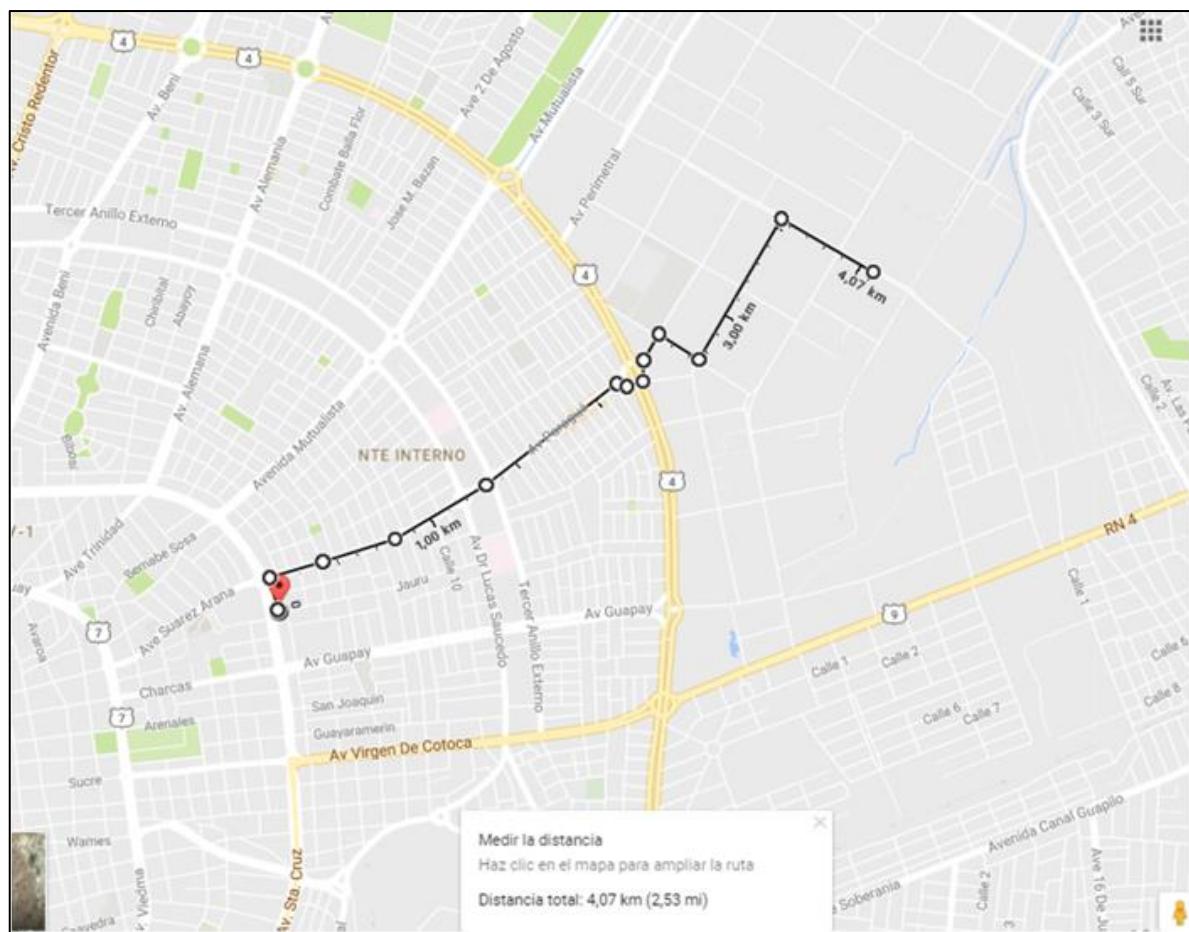
Fuente: Elaboración Propia, 2019

### Ubicación del sitio Alterno

**Dirección: Oficina TECORP S.A - Santa Cruz**

Parque Industrial Manzana 17, al lado de IMBA

En la **Figura No. 49**, se muestra el **Mapa de ubicación del Sitio Alterno**, la distancia entre el sitio principal y el sitio alterno es de 4,07 km. Distancia suficiente para no ser afectado por el mismo incidente del sitio principal.



**Figura No. 49.** Mapa de ubicación del Sitio Alterno

Fuente: Google Maps, 2019

## Estrategias de Continuidad

### 1) Sitio frio (*Cold Site*)

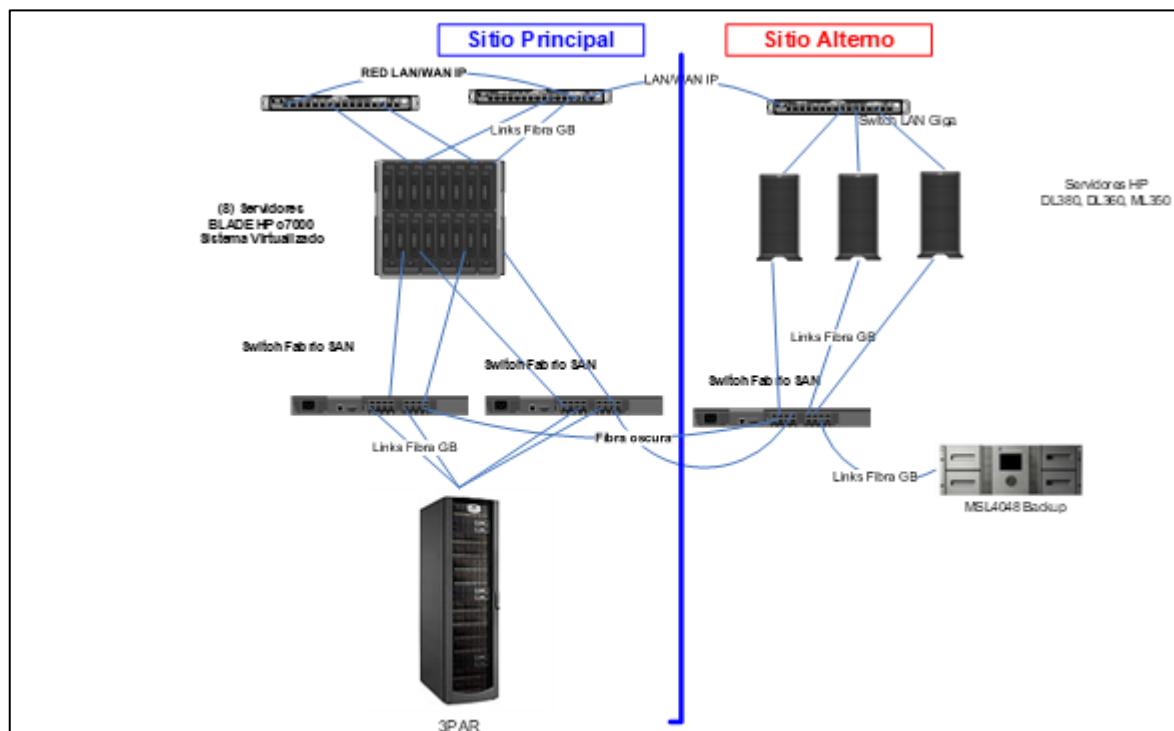
Tienen sólo el ambiente básico (Espacio físico en la sala de servidores, cableado eléctrico y energía, aire acondicionado) para operar una instalación de procesamiento de información. El sitio frio está listo para recibir los equipos, pero no ofrece ningún componente en el lugar antes que se requiera su uso. La activación del Sitio frío puede llevar varias semanas.

## 2) Sitio templado (*Warm Site*)

Alternativa de sitio de recuperación templada. Está parcialmente configurada, por lo general con conexiones de red y equipos periféricos seleccionados, como, por ejemplo, unidades de discos y otros controladores, pero sin el servidor principal. Algunas veces equipado con un servidor con menos prestaciones.

En la **Figura No. 50**, se muestra el **Diagrama de Configuración del Sitio Templado (*Warm Site*)**.

El sitio puede estar listo en cuestión de días; sin embargo, la ubicación y la instalación del servidor central y de otras unidades faltantes, puede tomar varios días y semanas.



**Figura No. 50.** Diagrama de Configuración del Sitio Templado (*Warm Site*)

Fuente: Elaboración Propia, 2019

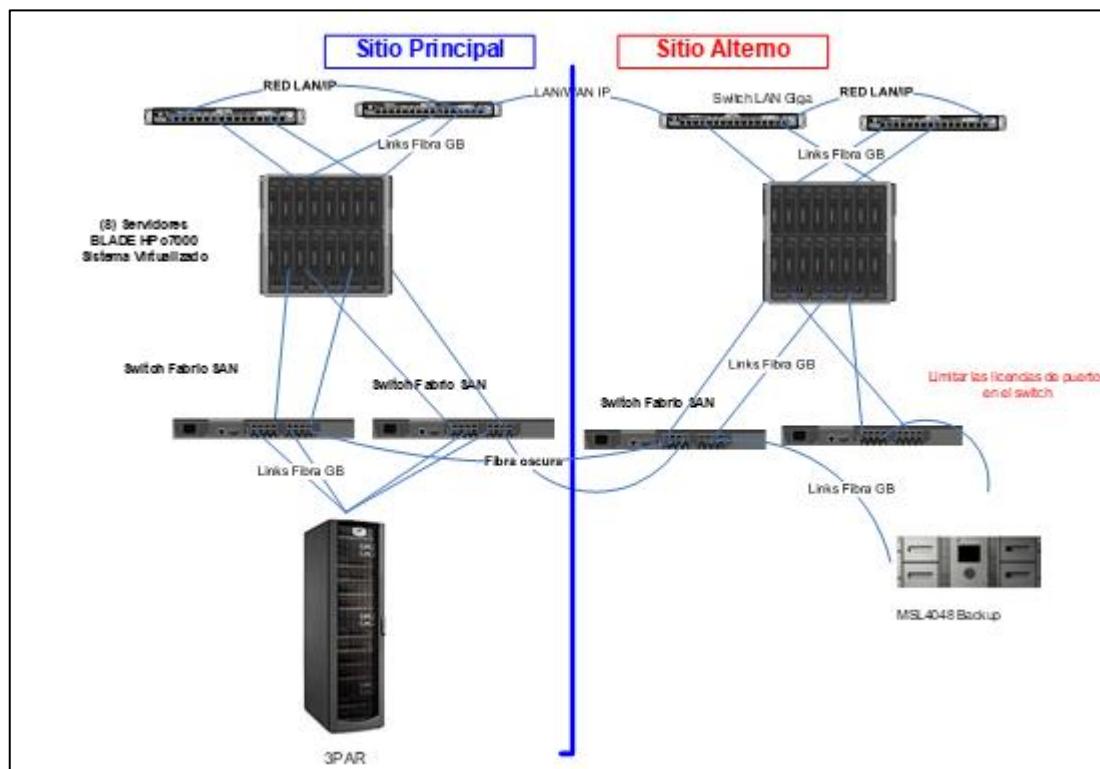
### 3) Sitio caliente (*Hot Site*)

Alternativa de sitio de recuperación caliente. Se configuran totalmente y están listos para operar dentro de varias horas. El equipo, red y *software* del sistema es compatible con la instalación primaria que está siendo respaldada.

En la **Figura No. 51**, se muestra el **Diagrama de Configuración del Sitio Caliente (*Hot Site*)**.

Las únicas necesidades adicionales son: personal, programas, bases de datos y documentación.

El sitio puede estar operativo en cuestión de horas (entre 4 y 8).



**Figura No. 51.** Diagrama de Configuración del Sitio Caliente (*Hot Site*)

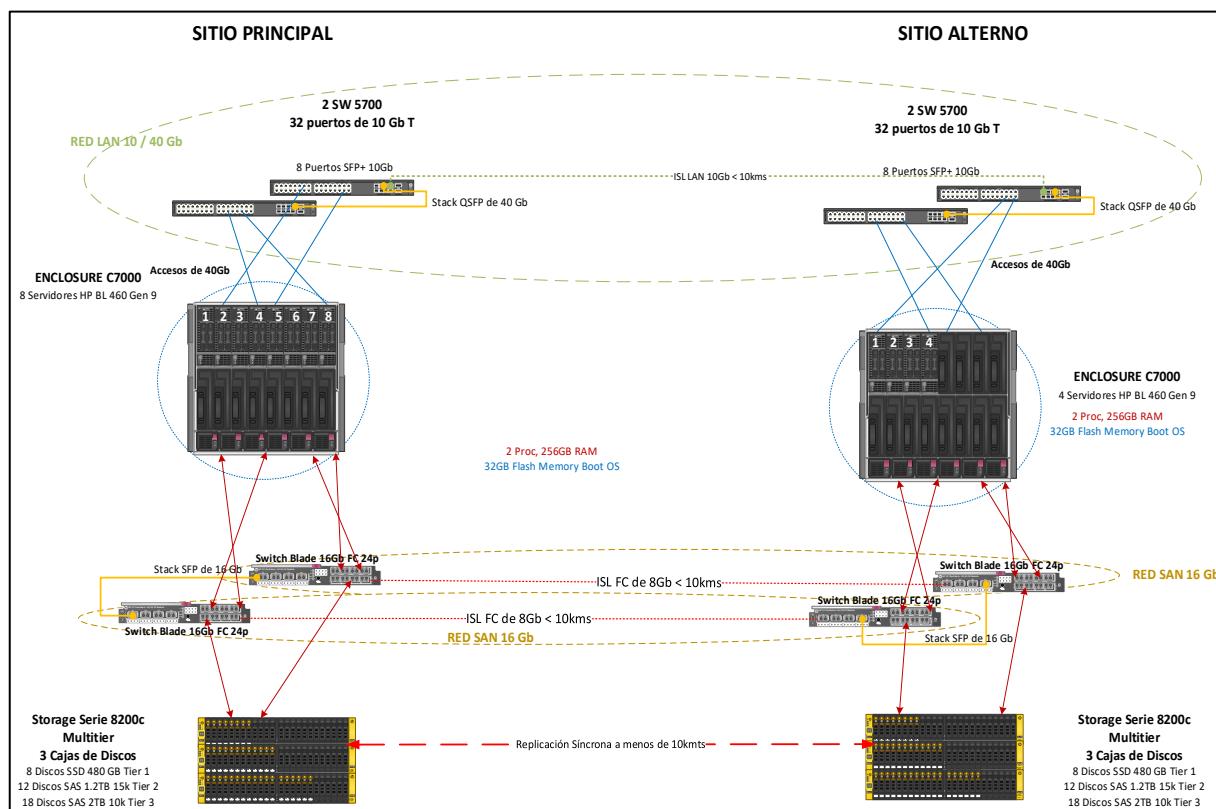
Fuente: Elaboración Propia, 2019

#### 4) Sitio espejo (*Mirror Site*)

Alternativa de recuperación de sitio espejo. Es un sitio que contiene una réplica exacta de otro. Las réplicas se suelen crear para facilitar la sincronización de grandes volúmenes de información entre los sitios y facilitar el acceso a la información aun cuando haya fallos en el servidor principal.

En la **Figura No. 52**, se muestra el **Diagrama de Configuración del Sitio espejo (*Mirror Site*)**.

El sitio espejo es una alternativa superior al sitio caliente, ya que cuenta con el personal necesario, programas, aplicaciones, la replicación de las bases de datos y toda la documentación necesaria en el sitio. El sitio puede promoverse y estar operativo en cuestión de minutos (entre 60 y 240 minutos).



**Figura No. 52.** Diagrama de Configuración del Sitio Espejo (*Mirror Site*)

Fuente: Elaboración Propia, 2019

## Selección de Estrategia de continuidad

El Grupo Empresarial de Inversiones Nacional Vida, luego de analizar las características y beneficios de las distintas estrategias, decide adoptar: La estrategia de continuidad ***Mirror Site***, provista por Servidores de Misión Crítica.

En el cuadro **Cuadro No. 54**, se muestra la división de los ambientes en función de los sitios.

**Cuadro No. 54.** División de los ambientes en función de los sitios.

Sitio	Ambiente
Principal	Ambiente de Producción
Alterno	Ambiente de Respaldo Ambiente de Desarrollo Ambiente de Pruebas

Fuente: Elaboración Propia, 2019

## Infraestructura mínima de recuperación

Todos los aspectos de aprovisionamiento de equipamiento tecnológico y cableado estructurado son cubiertos por la empresa TECorp, quien suscribió un acuerdo con los principales proveedores mayoristas (Datec, DMC, ITC, Sure) para la adquisición de servidores, equipos de telecomunicaciones, equipos de escritorio y licencias, cuando sea requerido por la contingencia.

## Otros recursos de recuperación

El aprovisionamiento de otros recursos se cubre por cada empresa, a través de la subcontratación y/o tercerización de servicios, tales como la contratación de personal, papelería, folletería y la adquisición de muebles y enseres donde sea requerido.

## Estrategia de Servidores de Misión Critica

### 1) Problemática Actual (Sitio Principal)

- La empresa cuenta con 20 servidores físicos, de los cuales 12 sólo tienen un único procesador (60% problemas de *performance*)
- De los servidores físicos, 13 no disponen de un disco de reserva y/o reparación (65% problemas de *HotSpare*) para evitar pérdida de información en caso de caída del disco
- Un Servidor físico no tiene arreglo de discos para el Sistema Operativo (5% problemas de *RAID* en la unidad de *O.S.*)
- De los servidores físicos, 13 tienen un arreglo con discos de baja capacidad (65% *RAID* de baja capacidad 74/146/300 Gb)
- 9 de los servidores físicos no tiene un arreglo de discos para datos (45% Problemas de *RAID* en la unidad de Datos)
- 6 Servidores físicos son w2k8 y precisan ser migrados (30% problemas del Sistema Operativo)
- 11 Servidores físicos precisan ser migrados a VMWare (55% problemas de Hipervisor)
- 13 Servidores físicos principales precisan ser renovados tecnológicamente a una nueva generación (65% problema de obsolescencia tecnológica en Servidores)
- 10 Servidores físicos presentan alarma de utilización de memoria y espacio en disco por encima del umbral (50% Problemas de falta de recursos de memoria y espacio en disco)
- De un total de 78 Servidores Virtuales, 7 son w2k3 y precisan ser migradas tan pronto como sea posible (9% problemas de Migración *ASAP* de Sistemas Operativos obsoletos)
- 38 Servidores virtuales utilizan Sistemas Operativos son w2k8, precisan ser migrados con urgencia (49% problemas de Migración Crítica de Sistemas Operativos obsoletos)

- No se dispone de un sistema de detección temprana y extinción de incendios
- No se cuenta con un sistema de monitoreo de temperatura y humedad en las salas de servidores y salas de telecomunicaciones.

## 2) Deficiencia en la Arquitectura Actual

- Se mantienen un lote de Servidores de Generaciones antiguas con altos riesgos de Fallos (ML110, ML310, G5)
- Bajo poder de Procesamiento (baja *performance*)
- Puntos únicos de Fallos (Redundancia) en Procesadores, ventiladores y Arreglo de Discos
- Espacio acotado de Almacenamiento en Disco y memoria
- Interrupción de los Servicios en Caso de Incidentes
- Imposibilidad de Recuperación de Desastres informáticos Severos o Críticos
- Existencia de múltiples Vulnerabilidades que podrían afectar al negocio en caso de ser materializadas
- Necesidad inmediata de renovación de equipamiento (Procesamiento, Almacenamiento, Obsolescencia tecnológico y Seguridad)

## 3) Premisas de diseño para la arquitectura mejorada

- Analizar las necesidades actuales y futuras
- Diseñar una solución de Servidores de misión crítica de Alta Disponibilidad para cumplir con la estrategia de la alta dirección, Sitio Espejado (*Mirror Site*)
- Evaluar el equipamiento con obsolescencia que requiere cambio inmediato
- Analizar la carga de recursos críticos del Sitio Principal y Regionales (LPZ, CBB)

- Definir los tipos de licencias requeridas y niveles de soporte

#### **4) Objetivos a Mejorar**

- Mantener una alta disponibilidad de los servicios y aplicaciones de misión crítica para mejorar la visibilidad interna y externa
- Optimizar la infraestructura de las empresas, otorgando alta disponibilidad y redundancia para garantizar la continuidad de las operaciones.
- Cumplir con los nuevos requerimientos de Continuidad del Negocio, para subsanar las observaciones de las auditorías externas de regulación (APS/ASFI)
- Disponer de una infraestructura de servidores virtualizada para realizar replicaciones de más de dos sitios a cualquier distancia, manteniendo la alta disponibilidad (*High Availability*) y buen desempeño (*Performance*)
- Migración y Mantenimiento no disruptivo (Balanceo de Cargas sin interrupción súbita) para mover los *Hosts* y datos libremente entre centros de datos sin afectar las aplicaciones empresariales
- Contar con una Infraestructura (*Server, Storage, Networking & Security Enterprise*) de nivel empresarial, de alta disponibilidad y completamente redundante para lograr tiempos de recuperación cercanos a 0 (RPO y RTO).

#### **5) Especificaciones para la solución de Servidores de Misión Crítica**

##### **Sistema *Enclosure Chassis***

- **Sitio Principal:** mínimo 8 Servidores x64 que soporte hasta 16 servidores *Blade*
- **Sitio Alterno:** mínimo 4 Servidores x64 que soporte hasta 16 servidores *Blade*

- Requisitos adicionales: Incluir el Sistema de Gestión y Monitoreo Redundante de la solución *Blade* de Alta Disponibilidad, ambos *Chasis* deben ser vistos en una sola consola de configuración con entorno *web*.

### **Servidores *Blade***

- **Sitio principal y alterno:**
  - 12 Servidores x64 de última generación
  - Para cada Servidor:
  - Procesador 2 Proc E5-2690 v3 de 12 núcleos (*core*) de 2.6Ghz o superior
  - Memoria de 256Gb de RAM DDR4 con 30Mb de Cache, 32 GB Flash Disc
  - 2 Puertos LAN de 10 GB y 2 Puertos SAN FC 8 GB
- Requisitos adicionales:
  - Incluir todos los accesorios necesarios para instalar en el futuro hasta 16 servidores en cada *Blade*
  - *Blade* de Rango medio con Alta Disponibilidad de 99.999% (cinco 9s)
  - Equipo de última generación
  - Indicar fecha de liberación para el *Enclosure* y los Servidores

### **Interconexión de la Red de Área de Almacenamiento SAN (*Storage Area Network*)**

4 SW SAN FC para total redundancia en ambos sitios. A continuación, las características solicitadas:

- **Sitio principal:** 2 SW SAN *Blade* de 16 Gb de 28 puertos FC
- **Sitio Alterno:** 2 SW SAN *Blade* de 8 Gb de 12 puertos FC
- Requisitos adicionales:

- Replica altamente redundante, con dos vías de FC para conectar las controladoras de los Storage (*MultiPath*).
- Todos los puertos de cada SW deberán ser licenciados, considerar las interfaces SFP+ (*Small Form-factor Pluggable*) de 16Gb y 4 QSFP (*Quad Small Form-factor Pluggable*) LR (*Long Range*) de 10Kms (Activos y No Activos)
- Incluir los accesorios necesarios para todos los puertos y los *Patch Cords*
- Equipos de última generación, indicar fecha de liberación

### **Interconexión de la Red de Área local LAN (*Local Área Network*)**

- **Sitio principal y alterno:**
  - SW Core LAN de 24 puertos de 10GbEth de tipo *Rack o blade*
  - Todos los puertos de cada SW deben estar activos y licenciados
  - Incluir los accesorios necesarios para todos los puertos y los *patch cords*
  - Equipos de última generación, indicar fecha de liberación
- **Almacenamiento Convergente (*Storage*)**
  - **Sitio principal y alterno:**
    - 2 Controladores redundantes Activo/Activo con al menos 64Gb de cache nativo RW
    - puertos de 10Gb mínimo para *FCoE* y/o *iSCSI*
    - 12 puertos FC de 16Gb en total (4 puertos embebidos, 8 adicionados para que permitan crear zonas de réplicas por FC nativo: *Multitier, Thin Provisioning, Virtualization, Data Deduplication*).

- Para cada *Storage*, adicionar 18 discos *SSD* de 2TB (*Tier Nivel 0, Ultra desempeño*), que posea protección y *spare* activos de ultra alto desempeño (*Multitier Nativo*).
- Indicar capacidad *RAW* y usable.
- Requisitos adicionales:
  - El *Storage* debe soportar hasta 10 cajas y cada caja debe alojar al menos 24 discos
  - Debe soportar mínimamente 750 TB para crecimiento futuro
  - La solución debe soportar replicación FC nativa, síncrona y/o asíncrona mejorada ilimitada entre *Storage* vía SAN Nativo.
  - El *Storage* debe ser de rango medio con alta disponibilidad de 99.999% (cinco 9s)
  - Detallar la capacidad de energía requerida por el *Storage* (consumo calculado en Watts)
  - Licenciar el 100% de la capacidad de los *Storage* en conexiones de servidores
  - Licencias el 100% de la capacidad del *Snapshot local* y remoto de cada *storage*
  - Licenciar el 100% de crecimiento de los discos soportados, incluido el crecimiento futuro en replicación del 100%
  - Incluir licencias “*Virtual Copy*” para cada *storage*.
  - Incluir todos los accesorios necesarios para todo el equipo (cables de poder, *Patch Cord, SFPs*, etc.)
  - Equipo de última generación, indicar fecha de liberación, velocidad de cada Controlador: Procesador, Mhz, Ram
  - Indicar transacciones IOPS Lectura y Escritura

## RACK inteligente

- **Sitio principal y alterno:**
  - *Rack* de 42U con la solución
  - Flujo de aire frio frontal
  - Expulsión de aire caliente trasera
  - PDU's administrables redundantes de AC

## Librería Backup

- **Sitio alterno:**
  - Librería de cintas con dos cabezales compatible con LT0 ULTRIUM 6
  - Soporte para Windows 2k8-2k12/Linux RHE.
  - Incluir 40 cintas LTO6
  - Incluir 2 cintas de limpieza
  - Equipo de última generación, indicar fecha de liberación

## Replicación

- **Sitio principal y alterno:**
  - Incluir las licencias de replicación para los dos *Storage SAN* a través de FC Nativa, para toda la capacidad ofertada.
  - Todos los puertos de cada SW deberán ser licenciados, considerar las interfaces SFP de 16Gb y 4 QSFP LR de 10KMS (Activos y No Activos)
  - *Transceiver LX* 10 Km para replicación ISL (*Inter-Switch Link*)
  - ISL LAN mínimo 10Gb, 2 Unid a 10 KM
  - ISL SAN mínimo 8/16Gb, 4 Unid a 10 KM
  - Equipo de última generación, indicar fecha de liberación

### ***Backup* y punto de restauración**

- **Sitio alterno:**

Incluir TODAS las licencias necesarias de los equipos para realizar *backups* y punto de restauración de contingencia o *Disaster Recovery* para todos los Servidores (servidores físicos, virtuales y *storages*) y compatibles con los sistemas operativos (*Windows 2k8-2k12/Linux RHE, Shadow Copy, Critical System, SQL Server 2014, Exchange 2013, IIS 8*).

### **Implementación**

- **Sitio principal y alterno:**

- Son 12 servidores físicos con sus sistemas operativos completamente configurados bajo la modalidad llave en mano.
- Replicación del Sitio Principal al Sitio Alterno (*Storage1* a *Storage2* a nivel Bloques, SAN Nativo)

### **Garantía Técnica**

- **Sitio principal y alterno:**

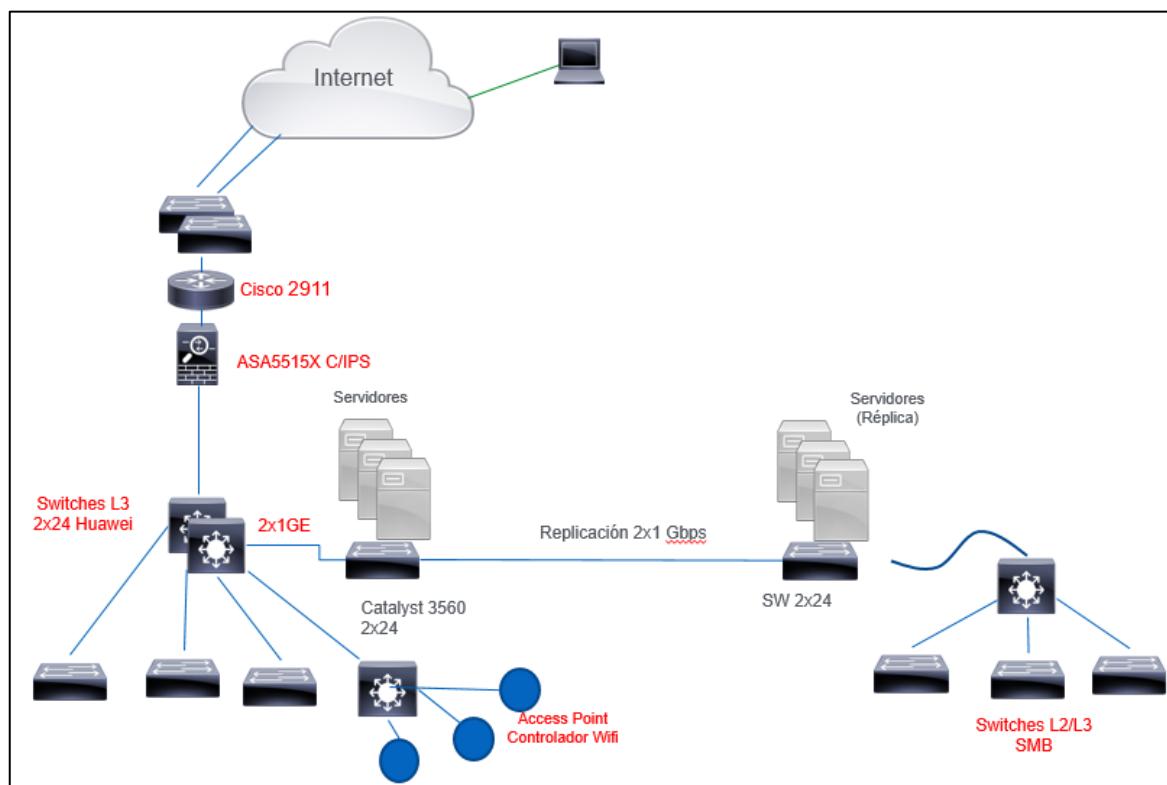
- Los equipos ofertados deben cumplir alta disponibilidad (RAS) de 99.999% al año como mínimo
- Contrato de soporte y mantenimiento 24x7x2
- Garantía 4 años en *Hardware*, con reemplazo de partes en 2 horas máximo
- Garantía de 4 años en *Software*: VMWare y todos los programas que requieren Soporte, Actualización y Respaldo
- Garantizar la provisión de repuestos y soporte de todo el proyecto de por lo menos 10 años
- Informar el costo de Soporte Anual una vez vencida la Garantía (Año 5)

## Estrategia de Ciberseguridad

### 1) Problemática Actual

- Seguridad limitada (*Firewall, Router, Switches* de Borde) sin gestión de eventos e incidentes de seguridad.
- Incidentes recurrentes (*Switches, Routers, Firewall, Wireless*, enlaces de Telecomunicaciones) que afectan la disponibilidad de la red Corporativa
- Obsolescencia Tecnológica (productos de *Networking End-To-Date*) que cumplieron su ciclo de vida)

En la **Figura No. 53**, se muestra el Diagrama de Red actual del Sitio Principal y Alterno



**Figura No. 53.** Diagrama de Red actual del Sitio Principal y Alterno

Fuente: Elaboración Propia, 2019

**2) Deficiencia en la Arquitectura Actual**

- Puntos únicos de Fallos (Redundancia) y única salida a Internet (sitio Principal)
- Seguridad limitada
- Imposibilidad de gestión de los eventos de seguridad.
- No se puede identificar la identidad de quien ingresa a consumir los servicios a través de la red (Quién, Cuándo, Dónde)

**3) Premisas de Diseño para la arquitectura mejorada**

- Analizar las necesidades actuales y futuras
- Diseñar un esquema de Red y Seguridad de alta disponibilidad y de nivel empresarial
- Evaluar el equipamiento con obsolescencia que requiere cambio inmediato
- Analizar la carga de recursos críticos (Sitio Principal, LPZ, CBB) para definir las licencias requeridas
- Evaluar la necesidad de *Software* especializado para analizar los eventos de seguridad
- Evaluar el Total de Usuarios y equipos que requieren una postura de Identidad al autenticar
- Definir los tipos de Licencias requeridas y niveles de soporte

**4) Objetivos a Mejorar**

- Alta disponibilidad (Eliminar puntos únicos de fallos)
- Balanceo de carga: Múltiples caminos activo-activo a Internet y conexión de regionales al Sitio Principal LPZ-SCZ, CBB-SCZ, SCZ01-SCZ02)
- Seguridad en múltiples capas (Vector interno, *Wireless*, *DMZ/Web* y Externo)
- Gestión de eventos e incidentes de seguridad.

- Identificación de la identidad del usuario (Autenticación) al consumir los servicios de la red (Quién, Cuándo, Dónde, A través de)
- Velocidad de acceso de la red a los servidores 2x40Gb
- Solución tecnológica diseñada de última generación
- Eliminación de los Incidentes, que afectan la disponibilidad de la red Corporativa

En la **Figura No. 54**, se muestra el **Diagrama de Red mejorado para el Sitio Principal y Alterno**

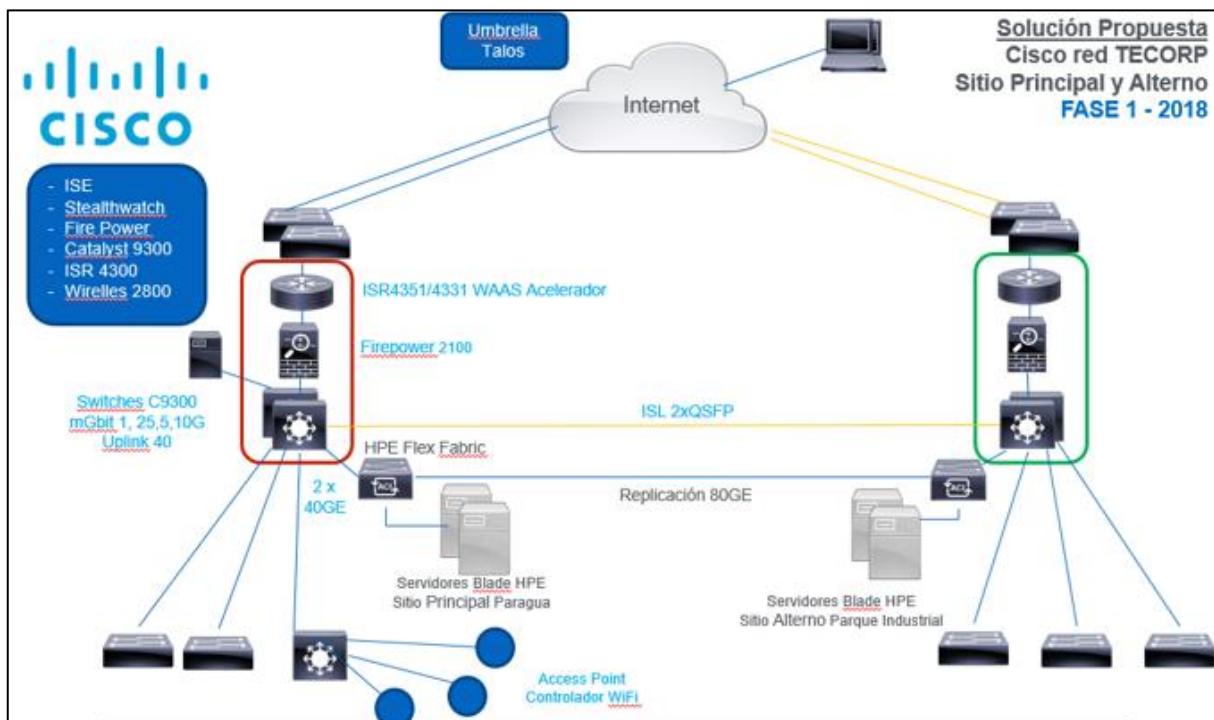


Figura No. 54. Diagrama de Red mejorado para el Sitio Principal y Alterno

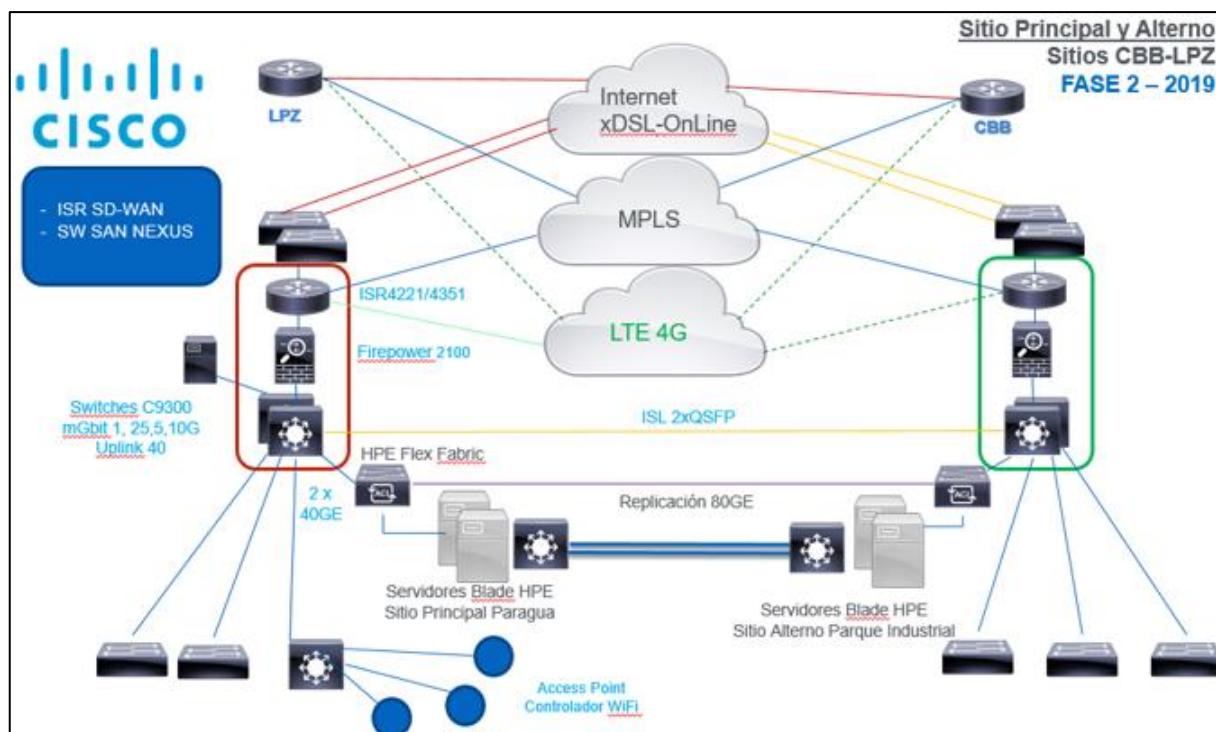
Fuente: Elaboración Propia, 2019

#### Beneficios Técnicos de la Arquitectura mejorada:

- **Switch:** Comutador *Enterprise* de última generación, 24p 10Gb, fuente redundante y *Stack*, *UpLink* 40Gb (Interface QSFP+)

- **Router:** ISR SD-WAN (Independencia de la Capa de Transporte xDSL, MPLS, LTE), WAAS (Optimización y Aceleración de Tráfico WAN)
- **Firewall:** IPS (Defensa de amenazas, *Malware* y Filtrado de Contenido)
- **Wireless:** AIR-AP2802I-A-K9 Serie 2800 (802.11ac wave 2 AP w/CA; 4x4:3; Int Ant; 2xGbE)

En la **Figura No. 55**, se muestra el **Diagrama de Red mejorado para el Sitio Principal y Regionales**



**Figura No. 55.** Diagrama de Red mejorado del Sitio Principal y Regionales  
Fuente: Elaboración Propia, 2019

### Beneficios Funcionales

- Se espera garantizar la Alta Disponibilidad Activa de los Servicios Críticos aún en condiciones de contingencia (Réplica Integral del Equipamiento Crítico)

- Balanceo de Carga de los enlaces de *backup* (Optimizando tiempos de respuesta y descongestionando los enlaces)
- Posibilidad de identificar la identidad del usuario (quien ingresa, a qué hora, desde donde y a través de qué dispositivo) a consumir los servicios a través de la red
- Reutilización de todo el equipamiento cambiado (Uso en las Regionales)
- Renovación tecnológica adecuada con equipamiento de última generación (Horizonte tecnológico cubierto para los próximos 5 años)
- Mejora de la comunicación y seguridad de los servicios publicados a los clientes externos y Servicios Bancarios: TE-MovilL, Desgravamen, BecSeguros, WebTransporte, Masivos y otros.

## **5) Especificaciones para la solución de *Networking* y Seguridad *Enterprise***

### **Red Inalámbrica Empresarial (*Wireless Enterprise*)**

- **Sitio principal y alterno:**
  - Wireless Enterprise 802.11ac wave 2 AP MIMO 4x4:3; Int Ant; 2xGbE
  - 20 puntos de Acceso (*Access Point*) Cisco AIR-AP1041N-A-K9
  - 1 Controlador Inalámbrico (*Controller*) Cisco 2500 PRG-P2-R4-WLC-01
  - Incluir Soporte de fábrica 5x8xNBD
  - Imagen debe Soportar *Advanced Security & Netflow*

### **Switches CORE Redundantes (*Top-Of-Rack*)**

- **Sitio principal y alterno:**
  - 4 SW *Enterprise L3 Multigigabit* formato *Rack*
  - 2 Módulos para *stack* (incluir cables e interfaces)
  - Fuente redundante

- *Autosensing* 10Gb/1Gb
- Con soporte de conexiones a 10GB SFP+ y QSFP+
  - o Cada *Switch* deberá tener los siguientes puertos:
- 24 puertos de 10Gb Ethernet
- 2 puertos de QSFP+ por cada *Switch* para *upLink*
- Incluir todos los transceiver necesarios para las interfaces ópticas QSFP+
- 8 *Network Modules* de 40Gb (QSFP+)
- *Patch Cords* de F.O OM4 LC/LC *duplex* de 15m
- *Patch Cords* de F.O OM4 LC/LC *duplex* de 8m
- o Ancho de banda y capacidad requerida de cada SW:
  - *Throughput* 714.2 Mpps o superior
  - *Routing/Switching* 960 Gbps o superior
- Requisitos adicionales:
  - Incluir Licencias para IP Base y *Routing*
  - La imagen debe Soportar *Advanced Security & Netflow*
  - Todos los puertos del SW deberán estar licenciados (Fibra y Cobre)
  - Deberá permitir configuración CLI y GUI
  - Equipo de última generación, indicar fecha de liberación
  - Indicar si está Listo para SDN (*Software Define Network*)
  - Soporte de fábrica 5x8xNBD

### **Router**

- **Sitio principal y alterno:**
  - *Router enterprise* con capacidad SD-WAN

- 16G DRAM, 16G eUSB *flash memory*, 200GB SSD
- Fuente redundante
- 2 GbEth port
- Optimizador y Acelerador de BW p/ +2000 Conn
- Incluir Soporte de fábrica 5x8xNBD
- Imagen debe Soportar *Advanced Security & Netflow*

### ***Firewal***

- 2 *Firewall* de última generación NGFW *Appliance*
- 16G DRAM, 16G eUSB *flash memory*, 200GB SSD
- Fuente Redundante
- 12-port GigaEth, 4-port TenGiga, SFP+
- Imagen debe soportar *Netflow*, incluir defensa de amenazas, *Malware* y Filtrado URL
- Incluir Soporte de fábrica 5x8xNBD

### **Aplicaciones de Seguridad**

- 700 licencias *Software* virtual para la Autenticación Segmentada basado en la Identidad
- 200 licencias *Software* de Inspección DNS y Reputación *OnCloud*
- *Software* de Gestión de Eventos de Seguridad que permita detectar amenazas en tiempo real y de manera anticipada, Análisis de la Seguridad y Visibilidad de la Red con indicadores de compromiso de seguridad, que muestre la actividad de amenazas de infiltrados, *malware* y ataques en múltiples etapas.  
Que soporte +10,000 eventos

- Configuración llave en Mano y Capacitación de Toda la Solución

### **3.6.5 P06 Desarrollo e Implementación del Plan de Continuidad del Negocio (BCP)**

#### **Objetivo**

Documentar los planes que serán usados durante un incidente y que permitan a la entidad continuar con su función.

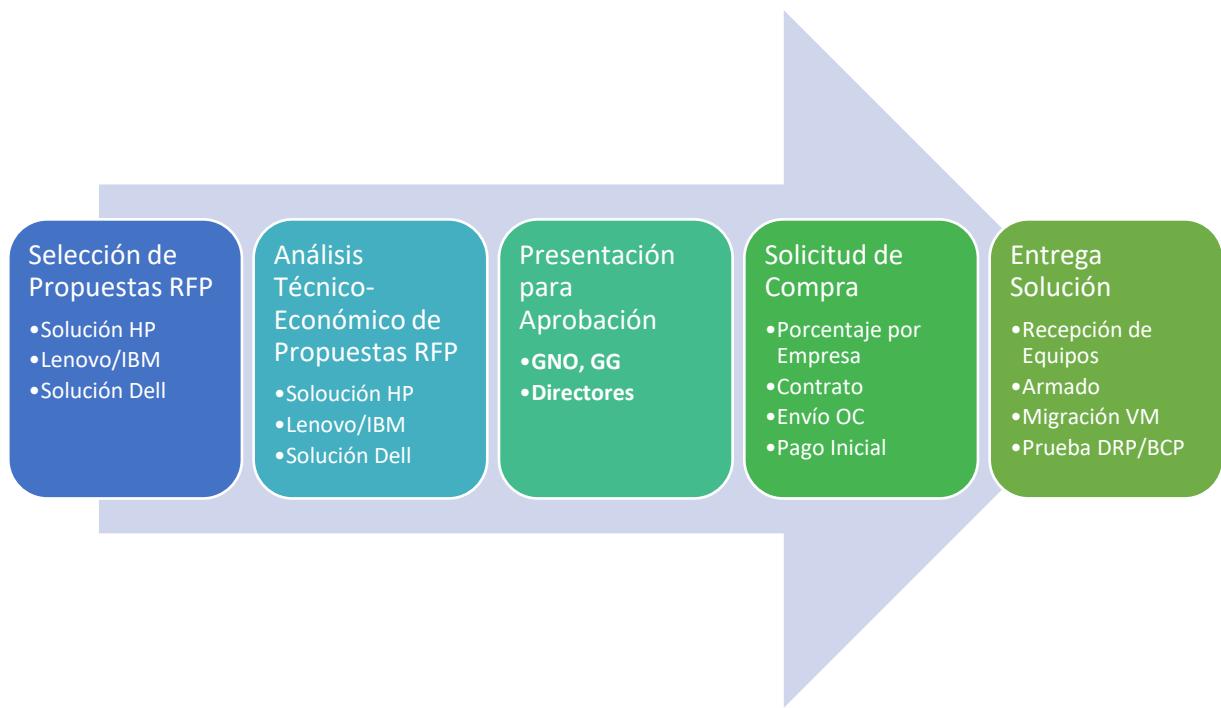
#### **1) Escenarios de fallas cubiertos**

El desarrollo e implementación del Plan de Continuidad del Negocio cubre los siguientes escenarios de fallas.

- **Recuperación de Desastres (DRP)**
  - Falla de un servidor físico (*Host*), migrar de manera automática todas las máquinas virtuales a otro servidor físico, incluyendo las direcciones del servidor de almacenamiento
  - Falla de las bandejas de la Torre de Discos (*Disk shelf*), conmutar automáticamente a la torre de discos del sitio alterno
  - Falla Almacenamiento de Datos (*Storage*), promover los volúmenes del *Storage* del sitio alterno, de solo lectura (RO) a Lectura/Escritura (RW)
- **Continuidad del negocio (BCP)**
  - Falla de todos los Servidores de Cómputo del sitio principal, se promueve todo al sitio alterno

#### **2) Acciones Posteriores**

En la **Figura No. 56**, se muestra la secuencia de tareas para la adquisición e implementación de la solución BCP.



**Figura No. 56.** Secuencia de tareas para la Adquisición de la Solución (BCP)

Fuente: Elaboración Propia, 2019

### Análisis técnico-económico de propuestas

- **Resumen Ejecutivo**

Con el objetivo de asegurar la disponibilidad de los Sistemas y garantizar la recuperación ante desastres, el Grupo Empresarial de Inversiones Nacional Vida S.A, realizó una invitación Directa para la provisión de una solución de Alta Disponibilidad comprendida por Servidores, *Storage, Switch y Backup* para el Sitio principal y Alterno.

Se entregó el documento con las especificaciones técnicas a cada proveedor para poder trabajar sus soluciones.

- **Solución HPE:** propuesta presentada por DMC y Datec
- **Solución Dell:** propuesta presentada por DMC
- **Solución Lenovo:** propuesta presentada por Datec

El presente documento entrega los resultados de la evaluación realizada a las propuestas presentadas por cada *distribuidor mayorista*, permitiendo evaluar independientemente cada sistema, a fin de cumplir los requerimientos técnicos

- **Metodología de evaluación**

El presente informe proporciona de manera rápida y precisa una visión de la propuesta presentada por cada proveedor, contra las valoraciones de la industria y la interpretación del consultor.

Se realizó un análisis de cada elemento, atributo y característica técnica de las soluciones, para determinar la diferencia entre cada propuesta y los requisitos técnicos elaborados.

El trabajo consistió en una serie de validaciones y comparaciones de características técnicas, junto con la revisión de los sitios tecnológicos de opinión (*Gartner*, DCIG, *Buyers Guide*, Sitios de los fabricantes: HP, Dell, Lenovo) a fin de verificar el nivel de cumplimiento.

Se evaluaron los aspectos tecnológicos de las 4 soluciones principales de cada diseño propuesto.

- Solución de Servidores (*Chasis*, Nodos *Blade*)
- Solución de Almacenamiento (*Storage*)
- Solución de *Switches* (SAN, LAN, CORE-TOR)
- Solución de *Backup*

- **Análisis financiero de soluciones tecnológicas**

Al concluir la evaluación de la Infraestructura Tecnológica (*Enclosure*, *Server Blade*, *Storage*, *Switches*, *Backup*) se evidencia que, desde la perspectiva financiera, la solución propuesta por la marca **HPE** es más económica que las soluciones propuestas por **Dell** y

**Lenovo.** En el Cuadro No. 55, se muestra el **Resumen de las propuestas financieras HPE, Dell, Lenovo.**

**Cuadro No. 55.** Resumen de Propuestas financieras HPE, Dell, Lenovo

Empresa	Opción	Solución	Enclosure Chasis	Servidores	Precio Final USD	%Diferencia	Garantía	VMWare
Datec	1	HPE	16	13	634,306.07	0%	3Y	STD
DMC	2	Dell	8	12	672,518.97	6%	3Y	STD
Datec	3	HPE + Lenovo	16	12	781,383.97	19%	3Y	STD

Fuente: Elaboración Propia, 2019

- **Evaluación técnica de solución tecnológica**

Las tres propuestas **HPE, Lenovo** y **Dell** son calificadas con igual puntuación:

Están catalogadas como líderes en el cuadrante mágico de *Gartner* en la categoría de Servidores Modulares. En la **Figura No. 57**, se muestra la posición de cada marca en el **Cuadrante Mágico de Gartner para Servidores Modulares**



**Figura No. 57.** Cuadrante Mágico de Gartner para Servidores Modulares  
**Fuente:** Gartner, 2017

- **Arquitectura Solución HPE (Datec Opción 1)**

Datec propone una solución mejorada de las especificaciones

**Sistema *Enclosure Blade*:**

**Sitio Principal:** HPE c7000 *enclosure*, soporte hasta 16 servidores *Blade*

- 8 Servidores x64 de última generación
- 2 Proc E5-2690 v4 de 12 cores de 2.6GHz o superior
- 256GB de RAM DDR4 30MB de Cache, 32 GB Flash Disc
- 2 Puertos LAN de 10 Gb y 2 Puertos SAN FC 8 Gb

**Sitio Alterno:** HPE c7000 *enclosure*, soporte hasta 16 servidores *Blade*

- 5 Servidores x64 de última generación
- 2 Proc E5-2690 v4 de 12 cores de 2.6GHz o superior

- 256GB de RAM DDR4 30MB de Cache, 32 GB *Flash Disc*
- 2 Puertos LAN de 10 Gb y 2 Puertos SAN FC 8 Gb

### **Interconexión de la Red de Área de Almacenamiento (*Storage Area Network*)**

- Se presenta una solución de *Data Center InterConnect* (DCI) a través de un *Switch Virtual Connect* embedido en el chasis del *Enclosure*

### **Interconexión de la Red de Área local LAN (*Local Área Network*)**

#### **Sitio principal y alterno:**

- 4 SW Core ToR HPE *FlexFabric* 5700 32XGT 8XG 2QSFP
- 32 RJ-45 1/10GBASE-T ports, 8 fixed 1000/10000 SFP+ ports, 2 QSFP+
- *Throughput up to 714.2 Mpps*
- *Routing/switching capacity 960 Gbps Stacking capabilities*
- *IRF 9 switches*
- 4 HPE 5700 40XG 2QSFP+ *Switch*
- 8 HPE A58x0AF 300W AC *Power Supply*
- 8 JmpCbl-ROW
- 8 HPE X130 10G SFP+ LC SR *Transceiver*
- 4 HPE X140 40G QSFP+ LC LR4 SM XCVR
- 4 HPE X240 40G QSFP+ QSFP+ 1m DAC Cable
- 1 HPE 4Y *Proactive Care 24x7 Service*

### **Almacenamiento Convergente de última Generación (Storage)**

#### **Sitio principal y alterno:**

- 2 HPE 3PAR *StoreServ* 8200 2N Fld Int Base
- 4 HPE 3PAR 8000 4-pt 16Gb FC *Adapter*

- 32 HPE 3PAR 8000 1.92TB SFF SSD
- 32 HPE 3PAR 8200 OS *Suite Drive* LTU
- 32 HPE 3PAR 8200 *Remote Copy Drive* LTU
- 32 HPE 3PAR 8200 *Data Opt St v2* Drive LTU
- 1 HPE 4Y *Proactive Care 24x7* Service
- 24 HPE *Premier Flex LC/LC OM4 2f 5m Cbl*

### **Librería Backup**

#### **Sitio alterno:**

- Librería de cintas:
  - ♦ 1 HPE MSL2024 0-Drive *Tape Library*
  - ♦ 2 HPE MSL LTO-6 Ultr 6250 FC *Drive Kit*
  - ♦ 2 HPE 5m Multi-mode OM3 LC/LC FC Cable
  - ♦ 2 HPE LTO-6 MP *Non Custom Labeled* 20 Pk (40 unidades)
  - ♦ 2 HPE *Ultrium Universal Cleaning Cartridge*
  - ♦ 1 HPE 4Y *Foundation Care 24x7 Service*
- Servidor de *backup*:
  - ♦ 1HP DL360 Gen9 8SFF CTO Server
  - ♦ 1HP DL360 Gen9 E5-2603v3 FIO Kit
  - ♦ 4HP 8GB 1Rx4 PC4-2133P-R Kit
  - ♦ 2HP 1.2TB 12G SAS 10K 2.5in SC ENT HDD
  - ♦ 1HP *Smart Array P440ar/2G FIO Controller*
  - ♦ 1HPE Ethernet 10Gb 2-port 562FLR-SFP+Adpt
  - ♦ 1 HPE 82E 8Gb *Dual-port* PCI-e FC HBA

- ♦ 2 HP 500W FS Plat Ht Plg Power Supply Kit
- ♦ 1 HPE iLO Adv incl 3yr TSU 1-Svr Lic
- ♦ 1 HPE 4Y Proactive Care 24x7 Service

## Implementación

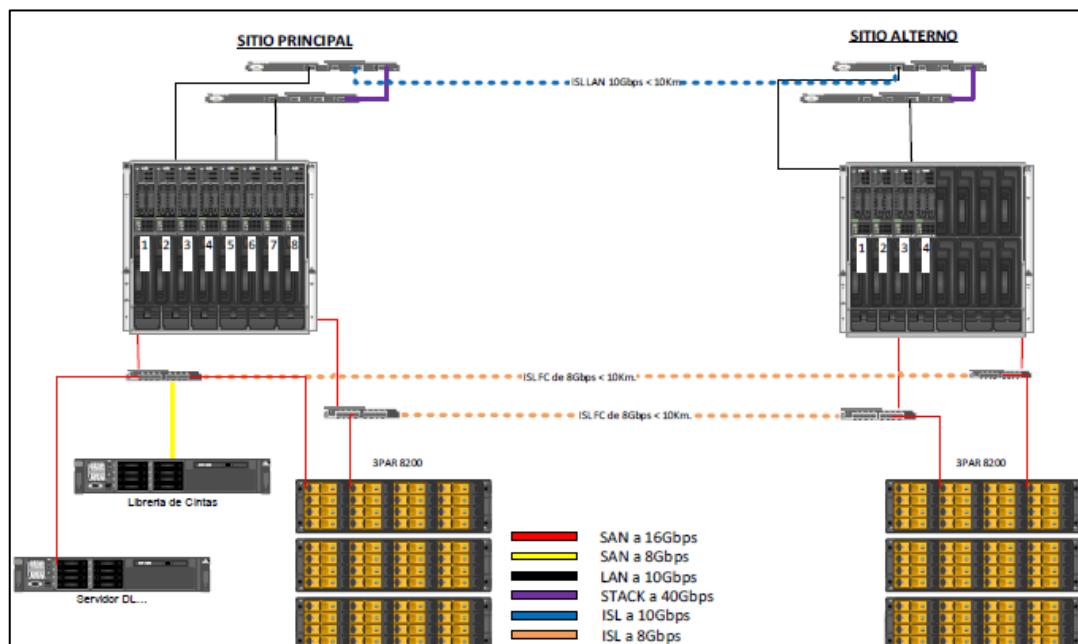
### Sitio principal y alterno:

- Son 13 servidores físicos con sus S.O. completamente configurados bajo la modalidad llave en mano.
- Replicación del Sitio Principal al Sitio Alterno (*storage1* a *storage2* a nivel Bloques, SAN Nativo)

### Garantía Técnica

Soporte 24x7x2, Garantía 4 años en *HARDWARE*, con reemplazo de partes en 2 horas

En la **Figura No. 58**, se muestra la **Arquitectura de la solución HPE** de Datec



**Figura No. 58.** Arquitectura de la solución HPE

Fuente: Propuesta económica Datec, 2017.

- **Arquitectura Solución Dell (DMC Opción 2)**

Dell propone una solución simétrica para ambos sitios:

***Chasis y Blade Server***

**Sitio Principal:**

- Un *Chasis* Dell PowerEdgeFX2s, con **8 Servidores** FC430, 2 procesadores *Intel Xeon E5-2680 v4* 2.4GHz, 35MB, 256 GB RAM (8x32GB RDIMM, 2400MT/s)

**Sitio Alterno:**

- Un *Chasis* Dell PowerEdgeFX2s, con **4 Servidores** FC430, 2 procesadores *Intel Xeon E5-2680 v4* 2.4GHz, 35MB, 256 GB RAM (8x32GB RDIMM, 2400MT/s)

**Backup Dell LTO 6**

- Servidor Dell DL160 Gen9 con 32 GB RAM (PC4-2133P-R), 2 Discos HP 1.2TB 6G SAS 10K
- Dell *Backup & Disaster Recovery Suite* (21-50TB) Per Front End Terabyte License/24X7

**Alcance**

- Sitio (Santa Cruz, Bolivia) que es el sitio Secundario
- NetVault *Backup Server / Consola* (R530)
- Integración con solución de Cinta TL1000
- Configuración de ambiente de respaldo

**A respaldar**

- Todo el ambiente virtualizado, a partir de Hipervisores *VMware* contenido 78 VMs *Windows*, 9 *SQL Servers* 2008, 2012 y 2014 a través de *plugin*, 1 DB2 9.7 a través de *plugin*.

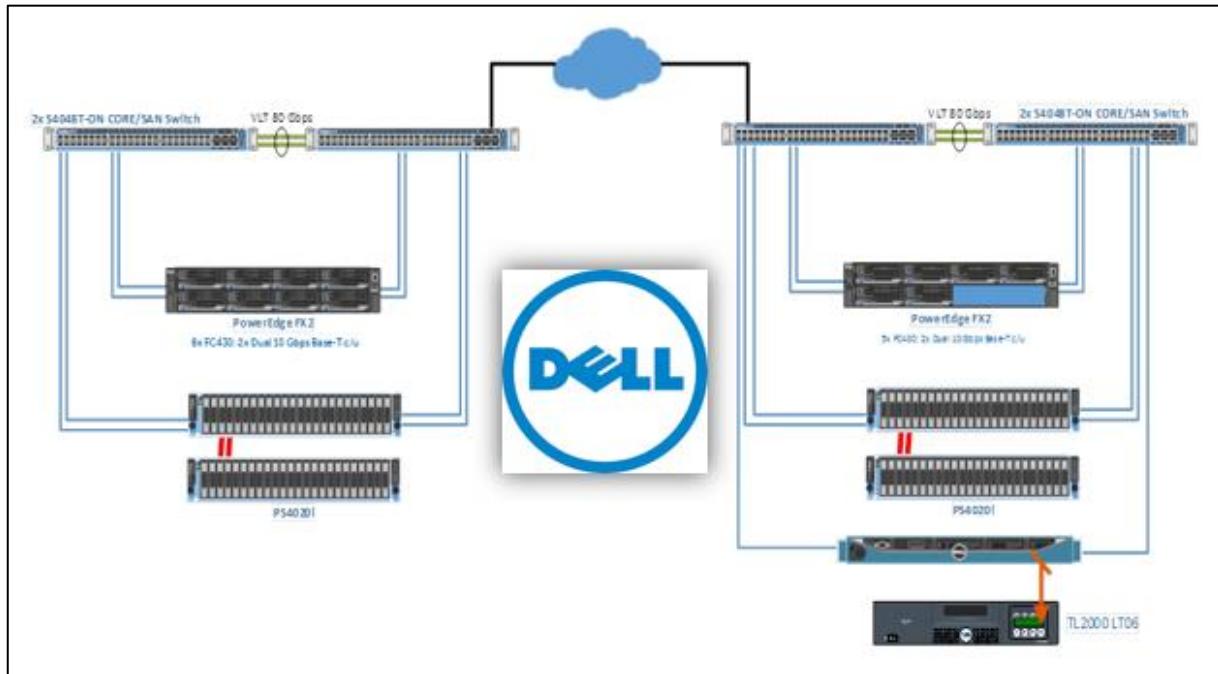
***Storage Compellent SC4020i (RAW 76.32 TB):***

- ***Hardware & Drives***
  - ♦ *SC4020 10Gb iSCSI - 4ports (Single drives)*
  - ♦ *6Gb Mini-SAS to Mini-SAS Cable, 0.6M, Qty 2, LC-LC Optical Cable, 5M*
  - ♦ *IO,10Gb iSCSI,4X SFP+ Optical Adaptor*
  - ♦ ***SSD (Raw TB):*** 12 Dell 960GB, SAS, 6Gb, 2.5" **SSD**, RI, Total 11.52 TB
  - ♦ ***SAS (Raw TB):*** 36 Dell 1.8TB, SAS 12 Gb, 2.5, **10K**, HDD, Total 64.8 TB
- ***Software***
  - ♦ *SW, Storage Center OS Core Base License*
  - ♦ *SW, Storage Optimization Bundle Base License*
  - ♦ *SW, Remote Data Protection Bundle Base License*

***Switch de interconexión SAN/LAN/TOR***

- Dell propone un diseño con 4 *Switch CORE* de 48 puertos 100M/1G/10G BASE-T *top-of-rack (ToR)* con seis puertos (QSFP+) *Uplink* de 40GbE con un rendimiento de velocidad de línea (*line-rate performance*), sin bloqueo (*non-blocking*), Sistema operativo Dell *Networking*
- Para el sitio principal, cada par de *Switch* será interconectado por un *UpLink Trunk* de 80Gbps a través de 2 puertos QSFP+ y con el sitio alterno a través de un *UpLink* de 40Gbps a través de 1 puertos QSFP+
- La solución de *Switch DELL Integrada* está diseñada para aplicaciones de centros de datos y entornos informáticos de alto rendimiento
- *Throughput* 737.28 Mpps (Excede el Requisito Min 714.2 Mpps)
- *Routing/Switching* 1,468 Gbps (Excede el Requisito Min 960 Gbps)

En la **Figura No. 59**, se muestra la **Arquitectura de la solución Dell**



**Figura No. 59.** Arquitectura de la solución Dell

Fuente: Propuesta económica DMC, 2017.

- **Arquitectura Solución Mixta HPE+Lenovo (DATEC Opción 3)**

#### *Enclosure y Server*

- **Sitio principal:** Datec propone una solución Mixta
  - Un *Chasis HPE Blade C7000*, con **8 Servidores BL460c G9 E5v4** (**Excede el requisito Min v3**) 10/20Gb, 2 procesadores, 256 GB RAM (8x32GB 2Rx4 PC4-2400T-R)
  - **SAN:** 2x *Brocade 4/24 SAN Switch Supp*
  - **LAN:** 2x *HPE FlexFabric 5700 40XG 2QSFP+ Switch*
  - 32 puertos SFP+ 1/10G y 2 Puertos QSFP+ 40G
  - *Throughput* 714.2 Mpps (Cumple el Requisito Min 714.2 Mpps)
  - *Routing/Switching* 960 Gbps (Cumple el Requisito Min 960 Gbps)

- **Sitio alterno:** Datec propone
  - ♦ Un *Chasis Blade C7000*, con **4 Servidores** BL460c G9 E5v4 10/20Gb, 2 procesadores, 256 GB RAM (8x32GB 2Rx4 PC4-2400T-R)
  - ♦ **SAN:** 2x *Brocade 4/12 SAN Switch Supp*
  - ♦ **LAN:** 2x *HPE FlexFabric 5700 Switch Series*
  - ♦ 32 puertos 1/10 BaseT y 2 Puertos QSFP+ 40G
  - ♦ *Throughput* 714.2 Mpps (Cumple el Requisito Min 714.2 Mpps)
  - ♦ *Routing/Switching* 960 Gbps (Cumple el Requisito Min 960 Gbps)

#### **Storage:**

- **IBM Storwize V5020** de doble controladora con 32GB de memoria caché, conectividad FC a 16Gbps con 4 puertos:
- 7 *FlashDrive* de 3.2TB, 41 discos SAS de 1.8TB de 10Krpm.
- *Software base, ThinProvisioning, DataMigration, FlashCopy, EasyTier, RemoteMirror*

#### **Solución de Backup:**

- Servidor HP DL160 Gen9
- Módulos de Memoria de 8GB 1Rx4 PC4-2133P-R Kit
- Discos HP 1.2TB 6G SAS 10K
- IBM TS3100 de doble cabezal con LTO7 FC a 8Gbps, capacidad de albergar 24 cartuchos de cintas, se incluyen 20 cintas

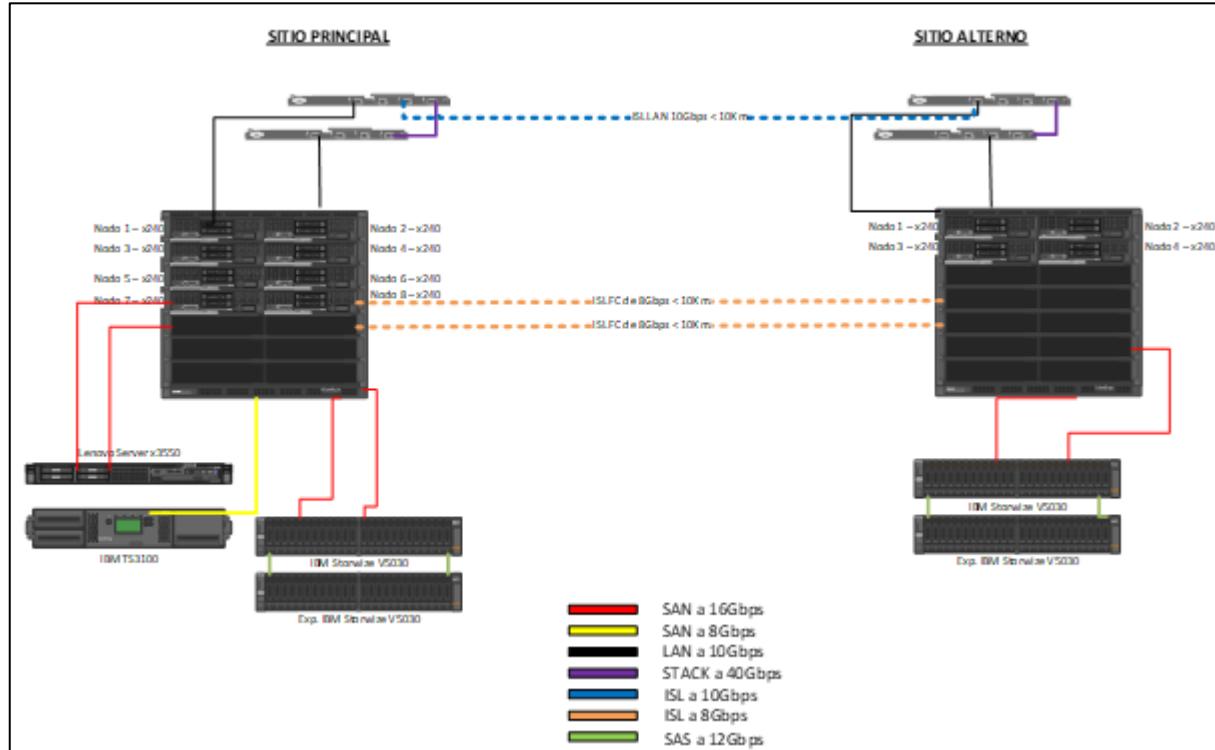
#### **Virtualización:**

- Se incluye 1 Lic VMware vSphere 6 *Standard for 2 processor* para cada Servidor
- Se incluye 1 Lic VMware vCenter Server 6 *Standard for vSphere* para cada Sitio

## Garantía:

- Incluye garantía de **3 años** de partes y mano de obra en oficinas del cliente (en área urbana) soporte 24x7 *Foundation Care* del Fabricante.
- Los servicios de instalación del Hardware presentado están incluidos

En la **Figura No. 60**, se muestra la **Arquitectura de la Solución mixta HPE/Lenovo**



**Figura No. 60.** Arquitectura de la Solución mixta HPE/Lenovo

Fuente: Propuesta económica Datec, 2017.

- **Valoración independiente**

Se han considerado todos los elementos de juicio entregados al consultor para la evaluar las propuestas Tecnológicas, presentadas por HPE, Lenovo y Dell, a fin de cumplir los requerimientos mandatorios del Proyecto Modelo de Gestión de Continuidad.

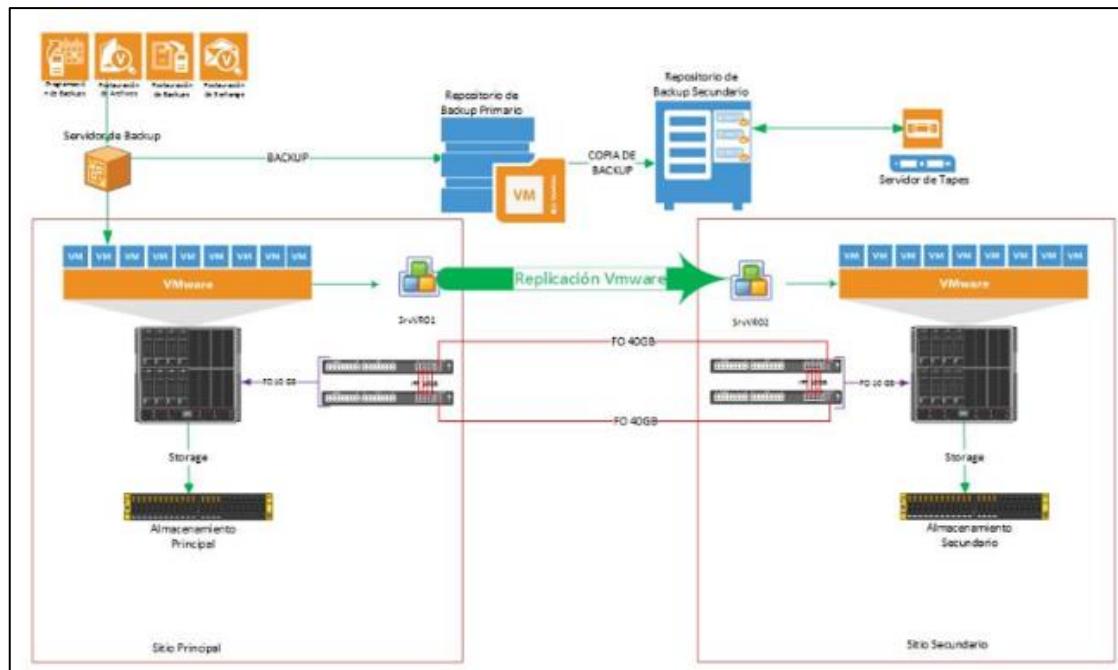
Se evaluaron los aspectos tecnológicos de los 4 elementos principales de cada diseño propuesto, analizando cada elemento, atributo y característica técnica de las soluciones para determinar la diferencia entre cada propuesta y los requisitos del Cliente.

La evaluación concluye que las soluciones propuestas por **HPE**, **Lenovo** y **Dell** cubren las necesidades tecnológicas del Grupo Empresarial de Inversiones Nacional Vida

La propuesta de solución tecnológica **HPE** presentada por **Datec** es económicamente la más baja, por lo tanto, se denomina **FAVORABLE**. Ya que cubre ampliamente las necesidades del Grupo de Inversiones, sin incumplir los requisitos técnicos mandatorios.

### 3) Implementación del proyecto de servidores de misión crítica

En la **Figura No. 61**, se muestra el Diagrama de la Solución de Servidores del Sitio Principal y Alterno, implementado. Se ha realizado la implementación de los equipos propuestos en el diagrama quedando la topología del Nacional Seguros de la siguiente manera:



**Figura No. 61.** Diagrama Solución de Servidores, Sitio Principal y Alterno

Fuente: Elaboración Propia, 2019

#### 4) Procedimiento de Copias de respaldo

##### Objetivo

Definir el procedimiento detallado paso a paso para la ejecución periódica de *backups* y respaldo de la información de bases de datos de sistemas en producción, salvaguardar los respaldos en medios electrónicos y entrega a custodia, con el fin de restaurar la información en caso de ser necesaria, además, permite cumplir con los estándares generales que fueron derivados de la norma de *backup* de bases de datos de sistemas en producción.

##### Alcance

El procedimiento se limita a la ejecución diaria de *backups*, apoyado por una herramienta automatizada que facilita la gestión de *backup*, el resguardo de los archivos de datos en medios de soporte, rotulado de los medios, registro de formularios de seguimiento de *backups* y la entrega de los medios al custodio.

##### Estrategia de *Backups*

Se establece como norma general:

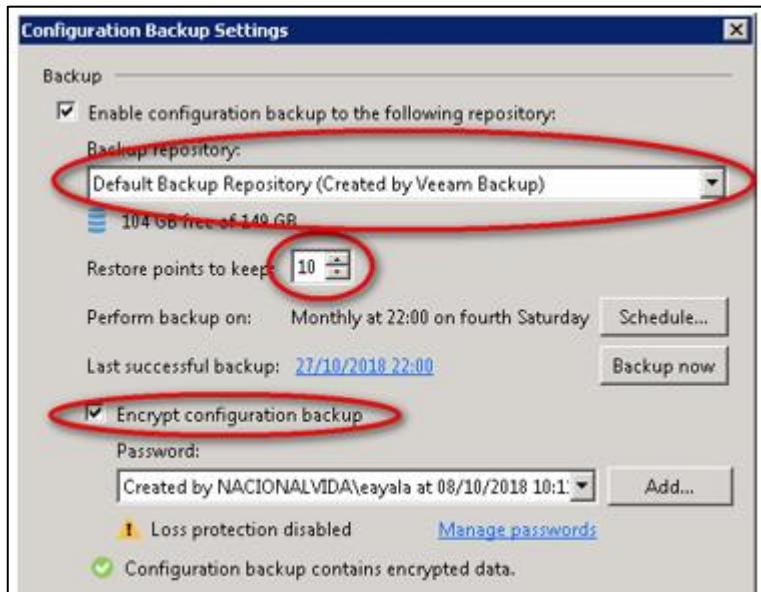
- Realizar una copia COMPLETA con periodicidad mensual.
- Realizar una copia INCREMENTAL Reversa con periodicidad semanal.

Las copias incrementales reversas se inyectan en el archivo de copia completa, de modo que el último archivo de *backup* es siempre una copia de seguridad del estado más reciente de la máquina virtual.

##### Ejecución de *Backups*

El *backup* de los servidores virtuales se realiza 1 vez por semana y se mantiene 10 copias al mes, todos los respaldos ejecutados están encriptados mediante una clave con seguridad MD5.

En la **Ilustración 1**, se muestra la Configuración del *Backup* en el repositorio



**Ilustración 1.** Configuración del *Backup* en el repositorio

Fuente: *Backup de servidores área de IT*, 2019

Un respaldo es una copia completa y los 9 restantes son copias diferenciales, pudiendo restaurar el servidor hasta 5 meses hacia atrás. En la **Ilustración 2**, se muestra la

### Configuración de un trabajo semanal (JOB) de *backup* a Disco.

	SC01SRAPP6
	1 day ago (20:10 sábado 17/11/2018)
	8 days ago (20:11 sábado 10/11/2018)
	15 days ago (20:11 sábado 03/11/2018)
	22 days ago (20:10 sábado 27/10/2018)
	29 days ago (20:11 sábado 20/10/2018)
	36 days ago (7:34 domingo 14/10/2018)
	43 days ago (20:11 sábado 06/10/2018)
	50 days ago (20:10 sábado 29/09/2018)
	57 days ago (20:11 sábado 22/09/2018)
	64 days ago (20:10 sábado 15/09/2018)

**Ilustración 2.** Configuración de un trabajo semanal (JOB) de *backup* a disco

Fuente: *Backup de servidores área de IT*, 2019

Se configura 1 tarea adicional 1 vez al mes, para realizar una copia de seguridad de los medios de respaldos a cinta. En la **Ilustración 3**, se muestra la **Configuración de un trabajo mensual (JOB) de backup a Cinta**

SC01SRAPP6 on Tape						
15 days ago (20:11 sábado 03/11/2018)	Full	Media Pool 1	Media set # 14	03/11/2018 22:38		
43 days ago (20:11 sábado 06/10/2018)	Full	Media Pool 1	Media set # 12	01/09/2018 22:05		
78 days ago (20:10 sábado 01/09/2018)	Full	Media Pool 1	Media set # 12	01/09/2018 22:05		

**Ilustración 3.** Configuración de un trabajo mensual (JOB) de backup a Cinta

Fuente: *Backup de servidores área de IT, 2019*

Se crean tareas de *backup* con el *software* de gestión de *backup* y se programan semanalmente para su ejecución automática. En la **Ilustración 4**, se muestra la

### Configuración de tareas semanales (Task) de backup de Servidores

NAME	TYPE	OBJECTS	STATUS	LAST RES...	NEXT RUN ↑	TARGET
SC01SRSP02	VMware Back...	1	Stopped	Success	21/11/2018 06:30:00 p.m.	SC01STNV03
SC01SRBDLT02	VMware Back...	1	Stopped	Success	21/11/2018 09:30:00 p.m.	SC01STNV02
SC01SRAPP3	VMware Back...	1	Stopped	Success	21/11/2018 09:40:00 p.m.	SC01STNV02
SC01SRBD5_	VMware Back...	1	Stopped	Success	21/11/2018 10:00:00 p.m.	SC01STNV02
SC01SRBD4	VMware Back...	1	Stopped	Success	21/11/2018 10:10:00 p.m.	sc01stnv01
SC01SRBDLT01	VMware Back...	1	Stopped	Success	21/11/2018 10:30:00 p.m.	SC01STNV02
SC01SRSW01	VMware Back...	1	Stopped	Success	21/11/2018 11:00:00 p.m.	SC01STNV02
SC01SRWEB	VMware Back...	1	Stopped	Success	22/11/2018 01:30:00 a.m.	SC01STNV02
SC01SRMNT01	VMware Back...	1	Stopped	Success	22/11/2018 02:30:00 a.m.	SC01STNV02
SC01SRFS02	VMware Back...	1	Stopped	Success	22/11/2018 04:00:00 a.m.	SC01STNV03
FILESERVER	VMware Back...	1	Stopped	Success	22/11/2018 05:00:00 a.m.	sc01stnv01
SC01SRTMG	VMware Back...	1	Stopped	Success	22/11/2018 09:00:00 p.m.	SC01STNV02
SC01SRTB01	VMware Back...	1	Stopped	Success	22/11/2018 09:30:00 p.m.	sc01stnv01
ARES	VMware Back...	1	Stopped	Success	22/11/2018 10:40:00 p.m.	SC01STNV03
SC01SRDT01	VMware Back...	1	Stopped	Success	22/11/2018 11:30:00 p.m.	SC01STNV02
SC01SRJBOS03	VMware Back...	1	Stopped	Success	23/11/2018 03:00:00 a.m.	SC01STNV03
SC01SRFE02	VMware Back...	1	Stopped	Success	23/11/2018 03:30:00 a.m.	SC01STNV02

**Ilustración 4.** Configuración de tareas semanales (Task) de backup de Servidores

Fuente: *Backup de servidores área de IT, 2019*

Todos los respaldos o copias son almacenados en los servidores *Storage NAS*, estos se distribuyen de acuerdo a su peso.

Se cuentan con 3 servidores *Storage NAS*, los que están configurados de forma predeterminada (en modo *StandAlone*) y se divide la carga de los servidores virtuales entre el

pool de servidores de *backup* físico (*Storage NAS*). En la **Ilustración 5**, se muestra la

### Distribución del Pool de servidores de *backup* físicos (*Storage NAS*).

NAME ↓	TYPE	HOST	PATH	CAPACITY	FREE
sc01stnv01	Windows	SC01STNV01	E:\Backups	14.6 TB	8.3 TB
SC01STNV02	Windows	SC01STNV02	E:\Backups	14.6 TB	4.7 TB
SC01STNV03	Windows	SC01STNV03	E:\Backups	14.6 TB	8.6 TB

**Ilustración 5.** Distribución de Pool de servidores de *backup*

Fuente: *Backup* de servidores área de IT, 2019

Se dispone de un Servidor de *Backup* (HPE ML 110 con 16GB de Memoria) el que soporta todas las pruebas de restauración de virtuales. En la **Ilustración 6**, se muestra un ejemplo de las **Pruebas de restauración de trabajos de *backup***, realizadas en el servidor de *Backup*

JOB NAME	SESSION TYPE	STATUS	START TIME ↑	END TIME
SC01SR3PAR	Full VM Restore	Success	21/11/2018 11:32	21/11/2018 12:08
SC01SRAPPNV03	Full VM Restore	Success	21/11/2018 9:51	21/11/2018 10:40
SC01SRPDC1 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 9:41	21/11/2018 12:34
FILESERVER (Reverse Incremental)	Full VM Restore	Success	21/11/2018 5:00	21/11/2018 5:12
SC01SRTK01 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 4:50	21/11/2018 5:01
SC01SRPDC (Reverse Incremental)	Full VM Restore	Success	21/11/2018 4:20	21/11/2018 4:58
SC01SRFS02 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 4:00	21/11/2018 4:44
SC01SRPH02 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 3:30	21/11/2018 5:35
SRSTS02 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 2:30	21/11/2018 2:32
SRSTS01 (Reverse Incremental)	Full VM Restore	Success	21/11/2018 2:10	21/11/2018 2:14
SC01SRUPON (Reverse Incremental)	Full VM Restore	Success	21/11/2018 2:10	21/11/2018 2:15
SPLUNK (Reverse Incremental)	Full VM Restore	Success	21/11/2018 1:50	21/11/2018 1:56
SC01SREXHY2 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 23:00	20/11/2018 23:25
SC01SRBDRDNV01 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 22:30	20/11/2018 23:37
SC01SRBI03 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 22:05	20/11/2018 22:49
SC01SRBI02 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 21:55	20/11/2018 22:16
SC01SRBI01 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 21:45	20/11/2018 22:09
sc01srts01 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 21:30	20/11/2018 21:37
sc01srbdrlt01 (Reverse Incremental)	Full VM Restore	Success	20/11/2018 21:10	20/11/2018 21:17

**Ilustración 6.** Pruebas de restauración de trabajos de *backup*

Fuente: *Backup* de servidores área de IT, 2019

En el **Anexo No. 26**, se muestran las características de la Cotización de Datatel, Enlace Inter-Sitio con Fibra Oscura 40Gbps/80Gbps (6 hilos) para interconectar el Sitio Principal y el Sitio Alterno

En el **Anexo No. 27**, se muestra acta de entrega y aceptación del Proyecto BCM, que corresponde a la aprobación formal por parte de los gerentes generales y gerentes de operaciones (Alta Dirección), por la finalización del Desarrollo e Implementación del proyecto Modelo de Gestión de Continuidad del Negocio (BCM) en Noviembre/2018, el documento se clasificó como Confidencial.

### **Ejecución de Pruebas de Continuidad**

Se adjunta el reporte enviado por el Gerente de IT y Seguridad al equipo de IT y a los funcionarios de Nacional Seguros (contraparte técnica, GNO, GG) a través del correo electrónico.

### **Reporte**

F. Programada : 21-Dic-2018

Inicio Programado : 09:00am

Inicio Real : 09:38am , Finalización : 11:36am

Tiempo Total : 01 hr 58 min

Ambientes : Producción y Desarrollo

Total Recuperadas : 101 VMs Sistemas Críticos y/o en Producción

Retiradas : 002 vCenter01, Replication01 (No son Necesarias)

Serv. Descartados : 135 VMs Pre-Producción y Pruebas

Total Server : 238 VMs

### **Equipo de Continuidad y Recuperación**

Alexis García Sandoval (Responsable)

German Espenhain (Ejecutor)

Edwar Ayala (Verificador)

Roberto Kantor (Colaborador)

Freddy Aparicio (Veedor en Entrenamiento)

### **Actividades Realizadas**

1. Se autoriza la Prueba BCP                    09:30am
2. Inicio de la Prueba BCP                    09:38am
3. Se realiza el Corte de la Fibra
4. Se conecta al SW Flex Fabric 5700 port-6, port-8 (Tardó 30 seg. aprox. en subir)
5. Los equipos utilizados son GESPENHAIN, EAYALA Interface de 1Gbps
6. Ingreso al VCENTER02 09:57am: <https://172.16.24.133/vsphere-client/>
7. Ingreso a *vSphere Replication* 09:58
8. Inicio de Recuperación

Recuperación Servidor SC01SRPDC

Uso de Datos disponibles más recientes

*Datacenter*

Servidor Pool de Recuperación

Revisión de Tarjeta de Red, Activación VLAN01

Encendido

Conexión Remota

Verificar Servicios> DNS, DHCP,

Roles FSMO Activados en el PDC

Comando> netdom query fsmo

Recuperación Servidor EP01, EP02, Fileserver2

STD VM Ware Replication

ENT *SiteRecoveryManager*

**Fase 1** – Recuperación finalizada 11:10am

**Fase 2** - Editar Config. (VLAN Conectado, Conectar al Encender) 11:23am

Resolver Problemas con la VLAN 14 en el Host 172.16.24.136

**Fase 3** - Verificación de Servicios 11:26am

Servicios: PDC, DNS, DHCP

Sistemas: eLife, eSalud, eProperty, BDLT01

**Fase 4** - Verificación de Ingreso a las Aplicaciones 11:36am

eSalud, UponSoft (Testeados Al azar)

eLife, eProperty

### Cierre de la Prueba

Actualización de Formularios

Comunicación y Envío de Resultados

### Notas:

Se mejoró notablemente la velocidad de la prueba en relación a la última ejecución

Tiempo de la última Prueba: 4hr 37 min, Total **277** min, realizado el 05-Oct-2018

Tiempo de la Prueba Actual: 1hr 58 min, Total **118** min, realizado el 21-Dic-2018

### Sugerencias para la Próxima Prueba:

1. Instalar Todas las Aplicaciones en los Equipos de Testeo
2. Coordinar con Desarrollo de Software el testeo de las aplicaciones
3. Verificar la Configuración de VLAN de Cada Host
4. Evaluar Habilidades del Equipo Ejecutor de Manera Individual

(Seguridad, Grado de Conocimiento, Velocidad de Trabajo, Trabajo bajo Presión, Capacidad de Comunicación)

5. Invitar a un veedor Independiente: (Auditor Interno, Externo)
6. Comunicar los Resultados de las Pruebas a Toda la empresa y Partes Interesadas

En el **Anexo No. 28**, se muestran los Resultados de la ejecución de la Prueba del Plan de Continuidad del Negocio.

### **3.7 Validación metodológica y estadística del proceso pre-experimental**

#### **3.7.1 Soporte metodológico y estadístico**

Para llevar a cabo la comprobación de la validez de la propuesta del modelo de Gestión y Continuidad del Negocio (BCM), el autor mediante el soporte metodológico y estadístico selecciona la prueba Chi Cuadrada de Pearson.

Se realiza un pre-experimento a partir de la comparación de los criterios de la guía de observación, referidos a las variables de la investigación: Riesgos y amenazas de ciberseguridad y el Tiempo Objetivo de Recuperación; obtenidos a partir del diagnóstico de la investigación (*pre-test*), contrastado con los mismos criterios después de aplicar la propuesta de solución Modelo de Gestión de Continuidad del Negocio (*post-test*), para verificar la transformación en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica y con ello validar el modelo.

- **Objetivo del pre-experimento**

Verificar la validez de la propuesta, con los datos de la observación y aplicando el Modelo de Gestión y Continuidad del Negocio (BCM) para comprobar si existe suficiente evidencia estadística que corrobore la transformación positiva.

- **Hipótesis**

Hipótesis de investigación (**H<sub>1</sub>**): Existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la aplicación de un Modelo de Gestión de Continuidad.

Hipótesis Nula (**H<sub>0</sub>**): No existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la aplicación de un Modelo de Gestión de Continuidad.

- **Tablas de contingencia**

Las frecuencias observadas y esperadas ocupan 2 filas y las pruebas Pre-test y post-Test ocupan 2 columnas, para investigar las frecuencias esperadas y observadas, se calcula el estadístico (Spiegel & Stephens, 2002, pág. 265).

$$\chi^2 = \sum_j \frac{(Observado j - Esperado j)^2}{Esperado j}$$

- **Grados de libertad**

El número de grados de libertad está dado por  $v = k - 1$

El número de categorías o clases  $k=(\text{filas}-1) \times (\text{columnas}-1)$ , es  $k=2$ , por lo que, se tiene que el grado de libertad  $v = (2 - 1) * (2 - 1) = (1) * (1) = 1$

- **Nivel de significancia**

La investigación tiene como nivel  $\alpha_1 = 0.01$ , es decir un 1% de margen de error y 99% de confianza

Del **Cuadro No. 56**, Se obtienen los valores percentiles para la distribución Chi Cuadrada, para un grado de libertad:

valor crítico<sub>1</sub>= 1-  $\alpha_1 = (1- 0.01)$ , donde  $\chi^2_{.99} = \mathbf{6.63}$

**Cuadro No. 56.** Valores percentiles para la distribución Chi Cuadrada

<b>v</b>	$\chi^2_{.995}$	$\chi^2_{.99}$	$\chi^2_{.975}$	$\chi^2_{.95}$	$\chi^2_{.90}$
<b>1</b>	7.88	6.63	5.02	3.84	2.71
2	10.60	9.21	7.38	5.99	4.61
3	12.80	11.30	9.35	7.81	6.25
4	14.90	13.30	11.10	9.49	7.78
5	16.70	15.10	12.80	11.10	9.24
6	18.50	16.80	14.40	12.60	10.60
7	20.30	18.50	16.00	14.10	12.00
8	22.00	20.10	17.50	15.50	13.40
9	23.60	21.70	19.00	16.90	14.70
10	25.20	23.20	20.50	18.30	16.00

Fuente: (Spiegel & Stephens, 2002, pág. 525)

- **Prueba de  $\chi^2$  de hipótesis**

Si  $\chi^2 > 0$ , la frecuencia observada difiere significativamente de la frecuencia esperada, considerando que las clasificaciones son independientes entre sí.

Si el valor  $\chi^2_{(\text{Calculado})} > \chi^2_{(\text{valor crítico de la tabla})}$ , se rechaza la hipótesis nula  $H_0$

Con este criterio de decisión se valida la  $H_1$ , se comprueba que se dio un cambio o transformación positiva.

- **Corrección de Yates por Continuidad**

Cuando se aplican resultados para distribuciones continuas a datos discretos se pueden hacer ciertas correcciones por continuidad. Existe una corrección cuando se utiliza la distribución Chi Cuadrada. La corrección de Yates, consiste en reescribir la ecuación, solo cuando el número de grados de libertad es  $v=1$  (Spiegel & Stephens, 2002, pág. 265).

$$\chi^2_{(\text{Corregida})} = \sum_j \frac{(O\text{bservado } j - E\text{sperado } j - 0.5)^2}{E\text{sperado } j}$$

- **Coeficiente de contingencia**

Medida del grado de relación, asociación o dependencia de las clasificaciones en una tabla de contingencia.

Cuando está próximo a 1, indica asociación alta, fuerte, o casi perfecta, dependiendo de la cercanía al número uno (Spiegel & Stephens, 2002, pág. 266).

$$C = \sqrt{\frac{\chi^2}{\chi^2 + N}}$$

- **Validación del desarrollo del pre-experimento**

Se realiza una evaluación entre lo observado y lo esperado de la variable independiente: Riesgos y amenazas de ciberseguridad (Fuentes de Riesgo, Amenazas de Ciberseguridad, Identificación, Análisis, Evaluación, Política) y la variable dependiente: Tiempo Objetivo de Recuperación (Compromiso y apoyo de la dirección, Estrategia de Tecnología, Seguridad y Continuidad), para determinar si existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la adopción de un Modelo de Gestión de Continuidad.

En el **Anexo No. 29**, se detalla el resultado del procesamiento estadístico, con la corrección de Yates y el coeficiente de contingencia; evaluando los criterios de entrada obtenidos en el diagnóstico con los criterios de salida del cambio o trasformación obtenida mediante la propuesta del modelo de Gestión de Continuidad (BCM).

- **Variable independiente** (Riesgos y amenazas de ciberseguridad)

Referido al criterio de observación A, B (Dimensión - Fuentes de Riesgos) no deciden en la trasformación del campo de acción, en tanto no depende del

modelo propuesto, sino del grado de conocimiento y dominio de las fuentes de riesgo y del perfil del Riesgo inherente de la Organización.

- **Variable dependiente:** (Tiempo Objetivo de Recuperación)

Para el criterio de observación K,  $\chi^2_c > \chi^2_t$ , en el **Cuadro No. 57** se confirma la trasformación de esta variable.

**Cuadro No. 57.** Calculo del  $\chi^2$  de la variable dependiente

K	Resultados de la última Prueba realizada al BCM	T1	T2	T3	T4	=	$\chi^2$	Coef.	11.30
	RTO Observado	16	13	3.5	2	=	57.31	0.98	Si
	RTO Esperado	4	4	4	4				

Fuente: Elaboración propia, 2019

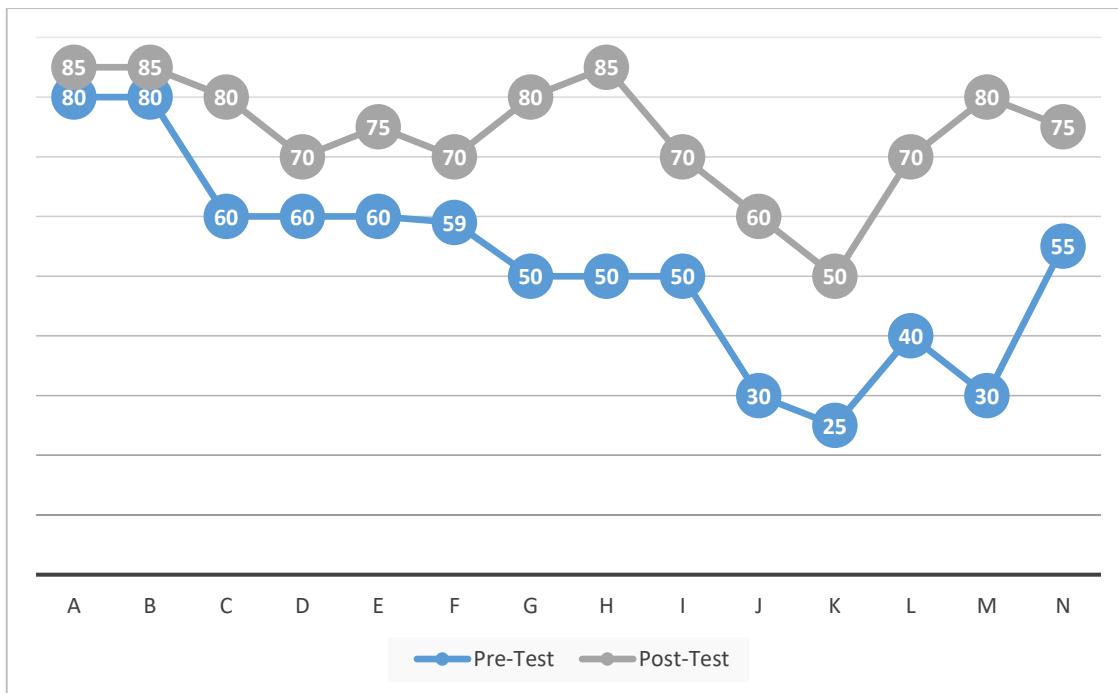
$$\begin{aligned} \chi^2_c = & \frac{(Observado T1 - Esperado T1)^2}{Esperado T1} + \frac{(Observado T2 - Esperado T2)^2}{Esperado T2} \\ & + \frac{(Observado T3 - Esperado T3)^2}{Esperado T3} + \frac{(Observado T4 - Esperado T4)^2}{Esperado T4} \end{aligned}$$

$$\chi^2_c = 57.31 > \chi^2_t = 11.30$$

- **Conclusión**

El análisis realizado a cada uno de los criterios de observación después de aplicar Chi Cuadrada, concluye que en el **85.7%** de los criterios (12), se demuestra un cambio positivo en la trasformación, por lo que se acepta la hipótesis de investigación (**H<sub>1</sub>**): Existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la adopción de un Modelo de Gestión de Continuidad, y se rechaza la hipótesis nula (**H<sub>0</sub>**).

En la **Figura No. 62**, se muestra la transformación de los criterios de observación.



**Figura No. 62.** Transformación de los criterios de observación

Fuente: Elaboración propia, 2019

Se concluye que la teoría y el experimento concuerdan.

## CONCLUSIONES

1. Con la sistematización a diferentes autores y a través del método de Análisis Documental, se caracterizaron los riesgos, amenazas y ciberseguridad, abordando las tendencias de las amenazas de ciberseguridad. Se transitó por las definiciones de tiempo objetivo de recuperación y sus tendencias y se analizaron los principios normativos de las normas internacionales, resoluciones administrativas y buenas prácticas de la industria.
2. Se evaluaron los procesos de misión crítica en el contexto investigado mediante la aplicación de instrumentos de investigación: entrevista y encuesta para identificar el Tiempo Objetivos de Recuperación. Como problema crítico se identificó **P4**: Los Tiempos Objetivos de Recuperación de incidentes no responden a la meta definida por la alta dirección.
3. Con un enfoque de sistemas, se elaboró la estructura del Modelo de Gestión de Continuidad del Negocio. Se desarrollaron, a partir de la aplicación de la norma ISO 22301, las diferentes cláusulas y sus objetivos: Contexto de la Organización, Liderazgo, Planificación, Recursos y Operación.
4. Se validó metodológicamente y estadísticamente el Modelo de Gestión de Continuidad de Negocio propuesto, con la aplicación de la prueba Chi Cuadrada de Pearson, validándose la hipótesis de investigación (**H<sub>1</sub>**): Existe una mejora en el Tiempo Objetivo de Recuperación de los Servicios de Misión Crítica con la aplicación de un Modelo de Gestión de Continuidad.

## **RECOMENDACIONES**

- 1 Socializar los resultados de la presente investigación con la comunidad de estudiantes y docentes de la Facultad de Ciencias de la Computación y Telecomunicaciones y la Unidad de Postgrado.
- 2 Se recomienda en las investigaciones futuras extender de GCN a SGCN con la implementación de la evaluación de desempeño y la elaboración de las acciones de mejora continua.
- 3 Se recomienda revisar los documentos de Análisis de Riesgos, Análisis de Impacto, Estrategias de continuidad y Plan de Continuidad, en cuanto a su contenido y posibles mejoras o cambios, con una frecuencia de revisión anual y/o en caso que se produzcan cambios significativos en la tecnológica y/o cuando el riesgo empresarial así lo requiera, para garantizar que sean adecuados, eficaces y suficientes.
- 4 Se sugiere extender el modelo de Gestión de Continuidad para incorporar las nuevas empresas: Clínica Metropolitana de las Américas y Fenix Seguros de Paraguay.
- 5 Para cumplir con los requisitos exigidos de disponibilidad se sugiere evaluar la Sala de Servidores del Sitio Principal y del Sitio Alterno y con ello garantizar los niveles adecuados de protección.
- 6 Para investigaciones futuras, se recomienda que el método de investigación sea el método cuantitativo.
- 7 Extender en trabajos futuros el proceso de Gestión de Incidentes y el Sistema de Comando de Incidentes.

## REFERENCIA BIBLIOGRÁFICA

- Acosta, C. R. (06 de 09 de 2018). *Seguridad en América*. Obtenido de  
<https://www.seguridadenamerica.com.mx/noticias/articulos/17055/cómo-prepararnos-para-enfrentar-las-crisis-en-las-organizaciones>
- Bankoff, G., Frerks, G., & Hilhorst, D. (2004). *Mapping Vulnerability: Disasters, Development and People*. UK: Earthscan.
- BCI. (27 de Julio de 2018). *Business Continuity Institute*. Recuperado el 2018, de Business Continuity Institute
- Capite, D. d. (2007). *Self-Defending Networks: The Next Generation of Network Security*. USA: CiscoPress.
- CSX Cybersecurity Nexus. (2015). *Fundamentos de Ciberseguridad*. Rolling Meadows, IL 60008 USA: ISACA.
- Gartner. (05 de 07 de 2018). *Seis tendencias en ciberseguridad y gestión de riesgos*. Recuperado el 29 de Sep de 2018, de <https://www.muycanal.com/2018/07/05/seis-tendencias-en-ciberseguridad-y-gestion-de-riesgos>
- Gestión. (10 de 2012). *Nuevo Estándar Internacional en Continuidad del Negocio: ISO 22301:2012*. Recuperado el 29 de Sep de 2018, de  
<https://www.gestion.com.do/ediciones/octubre-2012/item/300-nuevo-estandar-internacional-en-continuidad-del-negocio-iso-22301-2012>
- GIAC Information Security, C. (2002). Threat and the Need for Defense in Dept. En *GIAC SECURITY ESSENTIALS with the Common Body of Knowledge*. USA.
- González Villalobos, J. A. (2015). *Elaboración de un Plan de Auditoría para la evaluación de cumplimiento en Sistemas para Gestión de la Continuidad del Negocio basado en la*

- normativa ISO 22301.* (Tesis de Maestría), Ciudad Universitaria Rodrigo Facio, Costa Rica.
- Grupo Nacional Vida. (2018). *Quiénes Somos.* Recuperado el 29 de Sep de 2018, de <http://www.nacionalseguros.com.bo/grupo-nacional-vida/quienes-somos>
- ISACA. (2016). *CISM Certified Information Security Manager, Manual de Preparacion.* Illinois, USA: ISACA.
- ISACA. (2016). *Manual CISM (Certified Information Security Manager)* (15 ed.). Estados Unidos de America: ISACA Knowledge Center. Recuperado el 05 de Oct de 2018
- ISO 22301. (2012). *Sistema de Gestión de Continuidad del Negocio - Requisitos.* IBNORCA.
- ISO 27005. (2010). *Gestión del Riesgo en la Seguridad de la Información.* IBNORCA.
- ISO 31000. (2014). *Gestión del Riesgo - Principios y Directrices.* IBNORCA.
- ISO Guia 73. (2009). *Gestión del Riesgo - Vocabulario.* ISO.
- ISO IEC 27000. (2018). *Information security management systems - Overview and vocabulary.* Switzerland: ISO copyright office.
- ISO IEC 27001. (2013). *Sistemas de Gestión de Seguridad - Requisitos.* IBNORCA.
- ISO Tools. (19 de 03 de 2019). *¿Qué necesita saber a la hora de implementar la norma ISO 31000?* Recuperado el 2018, de <https://www.isotools.org/2018/03/19/que-necesita-saber-a-la-hora-de-implementar-la-norma-iso-31000/>
- Jeimy J. Cano, P. (2016). *Cyberattacks The Instability of Security and Control knowledge.* (ISACA, Ed.) Obtenido de <https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge.aspx>

- Kaspersky Lab. (s.f.). *THREAT PREDICTIONS FOR 2018*. Recuperado el 24 de Sep de 2018, de [https://media.kasperskycontenhub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB\\_Predictions\\_2018\\_eng.pdf](https://media.kasperskycontenhub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf)
- LRM 31000. (2008). *Certified Risk Manager ISO 31000*. PECB ISO 31000.
- McAfee. (29 de 11 de 2017). *McAfee Labs 2018 Threats Predictions Report' Previews Five Cybersecurity Trends*. Recuperado el 21 de Sep de 2018, de <https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/>
- Meadows, Rolling. (2009). *Manual de preparación al examen CISA* (19ma ed.). ISACA. Recuperado el 25 de Sep de 2018
- Néstor Garrido. (21 de 08 de 2018). *Seguridad en América*. Recuperado el 27 de Sep de 2018, de <http://www.seguridadenamerica.com.mx/noticias/articulos/16844/gestiOn-de-crisis-elemento-vital-para-la-continuidad-del-negocio>
- NIST SP 800-34 Rev. 1. (2010). *Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*. Computer Security Division, Information Technology Laboratory, USA. Recuperado el 08 de Julio de 2017, de <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
- Peña Castro, L. A. (2016). *Guia Metodologica para Elaborar un BCP en entidades del Estado*. (Tesis de Maestría), Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, Colombia.
- Romero Romero, Y. A. (2014). *Guía general para la elaboración de Planes de Recuperación de Desastres desde el PMI en las áreas de Tecnología Informática de las empresas pequeñas y medianas en BOGOTA D.C.* (Tesis de Maestría), Universidad de la Salle, Bogota, Colombia.

- Sarabia Zapata, A. V. (2015). *Modelo de Gestión de Continuidad de Infraestructura Tecnologica para la Operacion de Servicios de TI en Empresas financieras Sobre la Base de las normas ISO 22301 e ISO 27001. Aplicacion a un Caso de Estudio Banco KLM.* (Tesis de Maestría), UDLA, Ecuador.
- Spiegel, M. R., & Stephens, L. J. (2002). *Estadística* (3ra ed.). Mexico D.F.: McGraw-Hill.
- Stephen Northcutt, J. N. (2001). *Guia Avanzada de Deteccion de Intrusos* (Segunda ed.). (T. V. S.L, Trad.) Madrid: Pearson Educacion.

## BIBLIOGRAFÍA

1. Centro de investigación y seguridad informática, A. (s.f.). *Encuesta de seguridad informática en Argentina*. Recuperado el 16 de junio de 2018, de <http://www.cisi.ar>
2. CERT, Carnegie Mellon University. (s.f.). *CERT Statistics*. Recuperado el 3 de junio de 2018, de Sitio web de CERT: <http://www.cert.org/stats/>
3. CERT, Carnegie Mellon University. (s.f.). *CERT® Advisory CA-1999-02 Trojan Horses*. (Carnegie Mellon University) Recuperado el 09 de junio de 2018, de <http://www.cert.org/advisories/CA-1999-02.html>
4. CWE, Mitre. (19 de 11 de 2018). *Common Weakness Enumeration*. Obtenido de <http://cwe.mitre.org/>
5. David W. Chapman Jr., A. F. (2002). *Firewall PIX de Cisco Secure* (Primera edición en español ed.). (C. Press, Ed., & R. V. Llorente, Trad.) Madrid: Pearson Education S.A.
6. Gartner. (25 de 07 de 2017). *Definition: Business Continuity Management*. Recuperado el 26 de Sep de 2018, de <https://www.gartner.com/doc/3770865>
7. Gartner. (05 de 07 de 2018). *Seis tendencias en ciberseguridad y gestión de riesgos*. Recuperado el 29 de Sept de 2018, de <https://www.muycanal.com/2018/07/05/seis-tendencias-en-ciberseguridad-y-gestion-de-riesgos>
8. Gestión. (10 de 2012). *Nuevo Estándar Internacional en Continuidad del Negocio: ISO 22301:2012*. Recuperado el 29 de Sept 2018, de <https://www.gestion.com.do/ediciones/octubre-2012/item/300-nuevo-estandar-internacional-en-continuidad-del-negocio-iso-22301-2012>
9. GIAC Information Security, C. (2002). *Threat and the Need for Defense in Dept*. En GIAC SECURITY ESSENTIALS with the Common Body of Knowledge. USA.

10. Gjerdrum, D. (09 de 02 de 2016). *Risk & Insurance*. Recuperado el 29 de sep de 2018, de <http://riskandinsurance.com/a-brief-history-of-iso-31000-and-why-it-matters/>
11. ISOTools. (2014, 01 29). *ISO 22301: Antecedentes y origen*. Recuperado el 20 de Sep de 2018, de <https://www.isotools.org/2014/01/29/iso-22301-antecedentes-y-origen/>
12. Ivan Pepelnjak, J. G. (2003). *Arquitectura MPLS y VPN* (Primera edición en español ed.). (C. Press, Ed.) Madrid: Pearson Education S.A.
13. kaspersky Lab. (s.f.). *Qué es un troyano*. Recuperado el 09 de junio de 2018, de [http://www.kaspersky.com/sp/threats\\_faq#trojan](http://www.kaspersky.com/sp/threats_faq#trojan)
14. Loucks, J., Macaulay, J., Noronha, A., & Wade, M. (2016). *Digital Vortex*. United States: Dbt Center Press.
15. Merilee Ford, H. K. (1998). *Tecnologías de interconectividad de redes* (En español ed.). (C. Press, Ed., & C. C. Pedraza, Trad.) Naucalpan de Juarez, Mexico: Prentice Hall.
16. Netec Global Knowledge. (13 de 11 de 2017). *Netec*. Recuperado el 20 de Sep de 2018, de <https://www.netec.com/single-post/2017/11/13/%C2%BF Ciberseguridad o Seguridad de la Información>
17. Odom, W. (2004). *CCNA ICND Exam Certification Guide*. USA: Cisco Press.
18. Panda Security. (s.f.). *Qué es un Gusano Informático*. Recuperado el 09 de junio de 2018, de <http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/worm/>
19. SANS. (19 de 11 de 2018). *Top 25 Software Errors*. Obtenido de <http://www.sans.org/top25-software-errors/>

20. Shepard, S. (2002). *Convergencia de las Telecomunicaciones*. Madrid, España: McGraw-Hill.
21. Tanembaum, A. S. (1997). *Redes de Computadoras* (Tercera ed.). (D. M. Peake, Trad.) México, D.F: Prentice Hall.
22. Toapanta Iza, J. O. (2014). *Evaluación del Nivel de madurez de la Continuidad del Negocio: Caso G4S Secure Solutions*, (Tesis de Maestría), Sangolqui, Ecuador.

## ANEXOS

**Anexo No. 1.** Guía de análisis Documental

**Objetivo:** Caracterizar los principios normativos en el campo de trabajo a través de las normas internacionales, considerando además los requisitos legales, resoluciones administrativas regulatorias y las buenas prácticas de la industria.

**Criterios de Análisis:**

- 1) Riesgos y amenazas de Ciberseguridad
  - Riesgos
  - Amenazas
  - Ciberseguridad
  - Tendencias
- 2) Tiempo Objetivo de Recuperación
  - Interrupción Máxima Aceptable (MAO: *Maximum Acceptable Outage*)
  - Objetivo mínimo de Continuidad del Negocio (MBCO: *Minimum Business Continuity*)
  - Punto Objetivo de Recuperación (RPO: *Recovery Point Objective*)
  - Tiempo Objetivo de Recuperación (RTO: *Recovery Time Objective*)
  - Tendencias
    - Ventana de Interrupción (IW: *Interruption Window*)
    - Objetivo de Prestación del Servicio (SDO: *Service Delivery Objetive*)
    - Cortes máximos Tolerables
- 3) Norma ISO 22301
  - Origen
  - Características principales
  - Tendencias
- 4) Norma ISO 31000
  - Origen
  - Características principales
  - Tendencias
- 5) Gestión de Continuidad del Negocio
  - Continuidad del Negocio (BC).
  - Plan de continuidad del negocio (BCP).
  - Gestión de Continuidad del Negocio (BCM).

- Sistema de Gestión de Continuidad del Negocio (BCMS).
- 6) Análisis de Riesgo
- 7) Análisis de Impacto
- 8) Estrategias de Recuperación
- 9) Plan de Continuidad del Negocio y Recuperación de Desastres (BCP/DRP)

**Fuentes de información primarias utilizadas:**

- 1 NB/ISO 31000:2014 Gestión del Riesgo
- 2 NB/ISO 22301:2012 Sistema de Gestión de Continuidad del Negocio – Requisitos
- 3 NB/ISO 22313:2015 Sistema de Gestión de Continuidad del Negocio – Directrices
- 4 ISACA

**Anexo No. 2.** Guía de Observación

**Criterios de Observación:**

<b>CRITERIOS DE OBSERVACIÓN</b>		<b>S</b>	<b>GM</b>	<b>AM</b>	<b>N</b>
		80-100	60-79	10-59	<10%
<b>DIMENSIÓN - Fuentes de Riesgos</b>					
<b>A</b>	Grado de conocimiento y dominio de las fuentes de riesgo	<i>1.1.1</i>			
<b>B</b>	Perfil del Riesgo inherente de la Organización	<i>1.1.2</i>			
<b>DIMENSIÓN - Amenazas de Ciberseguridad</b>					
<b>C</b>	Amenazas de Ciberseguridad que podrían generar un impacto adverso al negocio	<i>1.2.1</i>			
<b>DIMENSIÓN - Identificación</b>					
<b>D</b>	Tipos de Vectores de fuga de Información	<i>1.3.1</i>			
<b>E</b>	Activos de información evaluados en el proceso de Análisis de Riesgos	<i>1.3.2</i>			
<b>DIMENSIÓN - Análisis</b>					
<b>F</b>	Grado de conocimiento de las Vulnerabilidades Detectadas	<i>1.4.1</i>			
<b>G</b>	Continuidad y Disponibilidad como metas corporativas	<i>1.4.2</i>			
<b>H</b>	Arquitectura Tecnológica y de Seguridad considera los Riesgos y Amenazas de Ciberseguridad	<i>1.4.3</i>			
<b>DIMENSIÓN - Evaluación</b>					
<b>I</b>	Interrupciones o incidentes mayores en lo últimos 5 años que han afectado los procesos críticos del negocio	<i>1.5.1</i>			

<b>DIMENSIÓN - Política</b>						
<b>J</b>	Tiempo Objetivo de Recuperación como meta Corporativa	2.1.1				
<b>K</b>	Resultados de la última Prueba realizada al SGCN/GCN/CN	2.1.2				

<b>DIMENSIÓN - Compromiso y Apoyo de la Dirección</b>						
<b>L</b>	La dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estrategias con los recursos necesarios	2.2.1				
<b>M</b>	% del Presupuesto Operativo Anual de TI y Seguridad	2.2.2				

<b>DIMENSIÓN - Estrategia de Tecnología, Seguridad y Continuidad</b>						
<b>N</b>	Grado de conocimiento del Plan Estratégico de TI, Seguridad y Continuidad para la implementación de Controles y Salvaguardas	2.3.1				
<b>Observador</b>						
<b>Lugar o área Observada</b>						
<b>Fecha de realización</b>						

<b>Abrev</b>	<b>Criterio</b>	<b>Normo tipo del criterio observado</b>
<b>S</b>	Si se cumple plenamente	cuando el criterio aparece entre el 80 y el 100%
<b>GM</b>	En gran medida	cuando el criterio aparece entre el 60 y el 79%
<b>AM</b>	En alguna Medida	cuando el criterio aparece entre el 10 y el 59%
<b>N</b>	No se aprecia	cuando el criterio aparece en menos del 10%

**Anexo No. 3. Cuestionario de Entrevistas a Directores y Gerentes Generales**

<b>Inicio</b>			
<b>Objetivos de la Entrevista</b>	Caracterizar el contexto del negocio, las expectativas de las partes interesadas e Identificar el Tiempo Objetivo de Recuperación deseado por la Alta Dirección y la estrategia de recuperación adoptada por las empresas del Grupo Empresarial de Inversiones		
<b>Instrucciones</b>			
<b>Grupo de Personas Entrevistado</b>	Directores y Gerentes Generales		
<b>Empresa</b>			
<b>Cargo</b>	<input type="checkbox"/> 1 Presidente <input type="checkbox"/> 2 Vicepresidente <input type="checkbox"/> 3 Director <input type="checkbox"/> 4 Gerente General o Corporativo		
<b>Edad</b>	<input type="checkbox"/> 1 25 a 34 años <input type="checkbox"/> 2 35 a 44 años <input type="checkbox"/> 3 45 a 54 años <input type="checkbox"/> 4 55 a 64 años <input type="checkbox"/> 5 65 años o mas	<b>Genero</b>	<input type="checkbox"/> 1 Masculino <input checked="" type="checkbox"/> 2 Femenino
<b>Antigüedad</b>	<input type="checkbox"/> 1 de 1 a 5 años <input type="checkbox"/> 2 de 6 a 10 años <input type="checkbox"/> 3 de 11 a 15 años <input type="checkbox"/> 4 de 16 a 20 años <input type="checkbox"/> 5 más de 21 años	<b>Nivel de Estudios</b>	<input type="checkbox"/> 1 Universitario Incompleto <input type="checkbox"/> 2 Universitario Completo <input type="checkbox"/> 3 Postgrado <input type="checkbox"/> 4 Maestría <input type="checkbox"/> 5 Doctorado

## Desarrollo

### Preguntas Planificadas

1 Puede Ud. Explicarme cuál es el perfil de riesgo Inherente de la organización  
 (Riesgos propios del Negocio)

Exposición de Información (Cobertura de Pólizas, Contratantes, Registros de Salud, Siniestros)

2 ¿Qué Amenazas de Ciberseguridad considera Ud. que podrían generar un Impacto adverso al negocio?


- Secuestro de Información (*Ransomware*)
- Pesca de Usuarios (*Phishing*)
- Fuga de Información (*Data Leak*)
- Todas las Anteriores
- Ninguna de las Anteriores

3 ¿La Continuidad y disponibilidad de los servicios Críticos de la empresa se consideran una meta Corporativa?

4 ¿La Arquitectura TI y de Seguridad considera los Riesgos y Amenazas de Ciberseguridad que podrían afectar la Misión y Visión Empresarial?

5 Conoce si en los últimos 5 años han habido interrupciones que han afectado los procesos críticos del negocio  
 ¿recuerda alguno?

6 El Tiempo Objetivo de Recuperación como meta Corporativa esperada debería ser medido

Mayor Tiempo considera un Menor presupuesto


- Meses
- Semanas
- Días
- Horas
- Minutos

7 ¿Conoce los resultados de la última Prueba realizada al Sistema de Gestión de Continuidad del Negocio?

8 ¿Considera que la Dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estratégicas con los recursos necesarios?

**9** ¿Cuál es el % del Presupuesto Tecnología y Seguridad con respecto a la facturación total del Grupo empresarial?

- Mayor al 4%  
Entre 3% y 4%  
Entre 2% y 3%  
Entre 1% y 2%  
Menor al 1%

**10** ¿Conoce el Plan Estratégico de Proyectos de Tecnología y Seguridad para la Implementación de Controles y Salvaguardas (Integrando Alcance, Tiempo, Costo, Calidad, Riesgos)?

- Conozco  
No Conozco

**Anexo No. 4. Cuestionario de Encuestas a Gerentes de Línea y Ejecutivos**

Inicio			
<b>Objetivo</b>	Caracterizar las vulnerabilidades, amenazas y recopilar información de las restricciones que afectan a las empresas del Grupo de Inversiones		
<b>Instrucciones</b>			
<b>Empresa</b>			
<b>Cargo</b>	<input type="checkbox"/> 1 Gerente de Operaciones <input type="checkbox"/> 2 Gerente de Línea <input checked="" type="checkbox"/> 3 Jefe de Área	<input type="checkbox"/> 4 Supervisor o Administrador de Área <input type="checkbox"/> 5 Analista <input type="checkbox"/> 6 Otro	
<b>Edad</b>	<input type="checkbox"/> 1 menos de 25 años <input type="checkbox"/> 2 25 a 34 años <input type="checkbox"/> 3 35 a 44 años <input type="checkbox"/> 4 45 a 54 años <input type="checkbox"/> 5 más de 55 años	<b>Genero</b>	<input type="checkbox"/> 1 Masculino <input type="checkbox"/> 2 Femenino
<b>Antigüedad</b>	<input type="checkbox"/> 1 menos de 1 año <input type="checkbox"/> 2 de 1 a 5 años <input type="checkbox"/> 3 de 6 a 10 años <input type="checkbox"/> 4 de 11 a 15 años <input type="checkbox"/> 5 de 16 a 20 años más de 20 años	<b>Nivel de Estudios</b>	<input type="checkbox"/> 1 Técnico Superior <input type="checkbox"/> 2 Universitario Incompleto <input type="checkbox"/> 3 Universitario Completo (Licenciatura) <input type="checkbox"/> 4 Postgrado (Diplomado/Pos título) <input type="checkbox"/> 5 Maestría

## Desarrollo

### Cuestionario de Preguntas Planificadas

- 1** Indique Ud. Cuáles son las Fuentes de Riesgos preocupa n a Su Organización  
(Seleccione Todos los que Ud. Considere relevantes)

- 1 Pirata Informático
- 2 Criminal de Computación
- 3 Terrorismo
- 4 Espionaje Industrial
- 5 Intrusión

- 6 Empleados con entrenamiento deficiente
- 7 Empleados Malintencionados/Negligentes
- 8 Empleados Deshonestos/Despedidos
- 9
- 10

- 2** Indique Ud. Cuáles Amenazas de Ciberseguridad han impactado a su organización  
(Seleccione Todos los que Ud. Considere relevantes)

- 1 Piratería Informática
- 2 Ingeniería Social
- 3 Acceso forzado al Sistema (Ataque Diccionario)
- 4 Espionaje cibernético (ventaja competitiva)
- 5 Suplantación de Identidad (Abuso de Derechos)
- 6 Ataque de negación de Servicio (*DoS, DDoS*)
- 7 Penetración en el Sistema
- 8 Manipulación del Sistema (Error u omisión)
- 9 Hurto de Información
- 10 Ingreso de Datos falsos o corruptos (BBDD, Programas)

- 11 Código Malicioso (Virus, Bomba Lógica, Troyano)
- 12 Errores en el Sistema (*BUGs*)
- 13 Sabotaje del Sistema
- 14 Acto fraudulento (Repetición, personificación, Interceptación)
- 15 Soborno de Información
- 16 Acceso no Autorizado al Sistema (Información Clasificada)
- 17 Guerra de Información (*warfare*)
- 18 Hurto de Medios o Documentos
- 19 Mal funcionamiento del *Software*
- 20 Mal funcionamiento del *Hardware*

- 3** Indique Ud. Cuáles son los vectores de fuga de información que existen en su organización  
(Seleccione Todos los que Ud. Considere relevantes)

- 1 Internet Público
- 2 Área de Publicación (Zona DMZ)
- 3 Red de Datos Interna

- 6 Red de Telefonía Celular
- 7 Aplicaciones de *Software*
- 8 Bases de Datos

- 4 Red de Datos Inalámbrica  
5 Red de Telefonía Básica

- 9 Personal  
10 Instalaciones

**4** Indique Ud. Cuáles son los Activos de Información Evaluados en el Análisis de Riesgos realizado en Su Organización (Seleccione Todos los que Ud. Considere relevantes)

- 1 Procesos Críticos  
2 Datos de interés para el negocio  
3 Datos de interés comercial  
4 Código Fuente  
5 Registros de la Organización  
6 Inmobiliario  
7 Enlaces Telefonía  
8 Enlaces Telecomunicaciones  
9 Copias de Respaldo de Usuarios  
10 Servicios de Información

- 11 Equipos de Usuarios  
12 Impresoras / Escáner  
13 Aplicaciones Ofimáticas Estándar  
14 Bases de datos Transaccionales/de Análisis  
15 Servidores Físicos/Virtuales  
16 Central de Telefonía  
17 Equipamiento de *Networking*  
18 Instalaciones Sitio Principal  
19 Instalaciones Sitio Alterno  
20 Otros

**5** Indique cuáles son las vulnerabilidades detectadas en su Organización

- 1 Contraseñas débiles  
2 Habilitación de Servicios innecesarios  
3 *Software* Nuevo sin testear  
4 Descarga y uso no controlado de *Software*  
5 Ausencia de Copias de Respaldo  
6 Ausencia de Protección Lógica  
7 Líneas de comunicación sin protección  
8 Tráfico sensible sin protección  
9 Conexión deficiente de Cables  
10 Punto únicos de Fallos

- 11 Arquitectura insegura de la red  
12 Transferencia de Mensajes en Texto Claro  
13 Gestión inadecuada de la Red (permisos de acceso)  
14 Conexiones en Red Pública sin Protección  
15 Ausencia de Personal  
16 Insuficiencia o escasez de personal  
17 Entrenamiento Insuficiente  
18 Procedimientos Inadecuados  
19 Ausencia de Mecanismos de Monitoreo  
20 Trabajo no supervisado

**6** Conoce si en los últimos 5 años han habido interrupciones que han impactado los procesos críticos del negocio

- 1 menos de 3 al año
- 2 menos de 5 al año
- 3 menos de 10 al año
- 4 múltiples interrupciones
- 5 se desconocen las interrupciones

**7** El tiempo Objetivo de Recuperación de los últimos incidentes e interrupciones, es:

- Menor a 1 semana
- Menor a 48 horas
- Menos a 8 horas
- Menor a 4 horas
- Menor a 1 hora

**8** El tiempo Objetivo de Recuperación de la Última Prueba de Continuidad realizada, es:

- Menor a 1 semana
- Menor a 48 horas
- Menos a 8 horas
- Menor a 4 horas
- Menor a 1 hora

**9** El Presupuesto Anual asignado a Desarrollo de *Software*, Tecnología Informática y Seguridad es Equitativo:

- Igual para las 3 áreas
- Es Mayor para el área de Desarrollo
- Es Mayor para el área de Tecnología
- Es Mayor para el área de Seguridad
- Desconozco el Presupuesto

**10**

¿Considera que el Presupuesto Tecnología y Seguridad asignado es suficiente para Garantizar la Recuperación en el Tiempo objetivo definido por el Grupo empresarial?

Muy Alto

Alto

Adecuado

Bajo

Muy Bajo

**Anexo No. 5.** Operacionalización de las variables

VARIABLE	DIMENSIONES	INDICADORES
1. Riesgos y amenazas de Ciberseguridad	1.1. Fuentes de Riesgo	1.1.1. Grado de conocimiento y Dominio de las fuentes de Riesgo 1.1.2. Perfil del riesgo inherente de la organización
	1.2. Amenazas de Ciberseguridad	1.2.1. Amenazas de Ciberseguridad que podrían generar un impacto adverso al negocio
	1.3. Identificación	1.3.1. Tipos de Vectores de Fuga de Información 1.3.2. Activos de Información evaluados en el proceso de Análisis de Riesgos
	1.4 Análisis	1.4.1 Grado de conocimiento de las Vulnerabilidades detectadas 1.4.2. Continuidad y Disponibilidad se consideran metas corporativas 1.4.3 La Arquitectura Tecnológica y de Seguridad considera los Riesgos y Amenazas de Ciberseguridad que podrían afectar la Misión y Visión Empresarial
	1.5 Evaluación	1.5.1 Cantidad de interrupciones en los últimos 5 años que han afectado los procesos críticos del negocio
2. Tiempo Objetivo de Recuperación	2.1. Política	2.1.1. Grado de conocimiento del Tiempo Objetivo de Recuperación definido como meta Corporativa 2.1.2. Grado de conocimiento de los resultados de la última Prueba realizada al Sistema de Gestión de Continuidad del Negocio
	2.2. Compromiso y Apoyo de la Dirección	2.2.1. Compromiso de la Dirección con los Objetivos de TI y Seguridad, apoya las estratégicas con los recursos necesarios 2.2.2. % del Presupuesto Tecnología y Seguridad con respecto a la facturación total del Grupo empresarial
	2.3. Estrategia de Tecnología, Seguridad y Continuidad	2.3.1. Grado de conocimiento del Plan Estratégico de Proyectos de Tecnología, Seguridad y Continuidad para la Implementación de Controles y Salvaguardas

**Fuente:** Elaboración propia

**Anexo No. 6. Resultado de la Guía de Observación (*Pre-Test*)**

**Criterios de Observación:**

CRITERIOS DE OBSERVACIÓN			S	GM	AM	N
			80-100	60-79	10-59	<10%
<b>DIMENSIÓN - Fuentes de Riesgos</b>						
A	Grado de conocimiento y dominio de las fuentes de riesgo	1.1.1	X			
B	Perfil del Riesgo inherente de la Organización	1.1.2	X			
<b>DIMENSIÓN - Amenazas de Ciberseguridad</b>						
C	Amenazas de Ciberseguridad que podrían generar un impacto adverso al negocio	1.2.1		X		
<b>DIMENSIÓN - Identificación</b>						
D	Tipos de Vectores de fuga de Información	1.3.1		X		
E	Activos de información evaluados en el proceso de Análisis de Riesgos	1.3.2		X		
<b>DIMENSIÓN - Análisis</b>						
F	Grado de conocimiento de las Vulnerabilidades Detectadas	1.4.1			X	
G	Continuidad y Disponibilidad son metas corporativas	1.4.2			X	
H	Arquitectura Tecnológica y de Seguridad considera los Riesgos y Amenazas de Ciberseguridad	1.4.3				X
<b>DIMENSIÓN - Evaluación</b>						
I	Interrupciones o incidentes mayores en lo últimos 5 años que han afectado los procesos críticos del negocio	1.5.1				X
<b>DIMENSIÓN - Política</b>						
J	Tiempo Objetivo de Recuperación como meta Corporativa	2.1.1			X	
K	Resultados de la última Prueba realizada al BCM	2.1.2			X	
<b>DIMENSIÓN - Compromiso y Apoyo de la Dirección</b>						
L	La dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estrategias con los recursos necesarios	2.2.1			X	
M	% del Presupuesto Operativo Anual de TI y Seguridad	2.2.2			X	
<b>DIMENSIÓN - Estrategia de Tecnología, Seguridad y Continuidad</b>						
N	Grado de conocimiento del Plan Estratégico de TI, Seguridad y Continuidad para la implementación de Controles y Salvaguardas	2.3.1				X
<b>Abrev</b>	<b>Criterio</b>	<b>Normo tipo del criterio observado</b>				
S	Si se cumple plenamente	cuando el criterio aparece entre el 80 y el 100%				
GM	En gran medida	cuando el criterio aparece entre el 60 y el 79%				
AM	En alguna Medida	cuando el criterio aparece entre el 10 y el 59%				
N	No se aprecia	cuando el criterio aparece en menos del 10%				

**Anexo No. 7.** Triangulación de los instrumentos

Indicadores	Instrumentos (Cuestionario/ Guías de...)		
	Encuesta	Entrevista	Observación
1.1.1.	1		A
1.1.2		1	A
1.2.1.	2	2	B
1.3.1.	3		C
1.3.2.	4		D
1.4.1.	5		E
1.4.2.		3	F
1.4.3		4	G
1.5.1.	6	5	H
2.1.1.	7	6	I
2.1.2.	8	7	J
2.2.1		8	K
2.2.2.	9 10	9	L
2.3.1.		10	M

**Fuente:** Elaboración Propia, 2018

**Anexo No. 8.** Restricciones de la autoridad de supervisión ASFI

**Nota:** A manera de muestra

DETALLE	PERIODICIDAD	FECHA LÍMITE	RESPONSABLE DE PREPARAR INFORMACIÓN	RESPONSABLE DE ENVÍO NSVS	OBSERVACIONES
<b>Detalle de Deuda Vigente, Pagos y Amortizaciones efectuadas</b>	Trimestral	30 días siguientes a la fecha de cierre del respectivo trimestre	Finanzas	Tesorería	Aplica únicamente cuando la Compañía tenga emisiones de Deuda Vigentes inscritas en ASFI y BOLSA.
<b>Estados Financieros Auditados Externamente (informe corto)</b>	Anual	120 días calendarios siguientes al cierre de cada ejercicio anual	Contabilidad	Jefe Administrativo Oficina Central	Enviar Balance General, el Estado de Resultados, el Estado de Flujo de Efectivo, el Estado de Evolución de Patrimonio y sus respectivas notas. (Informe Corto)  Nota: Deberán ser auditados por empresas de auditoria externa inscritas en RMV.
<b>Estados Financieros Trimestrales</b>	Trimestral	30 días siguientes a la fecha de cierre del respectivo trimestre	Contabilidad	Analista de Contabilidad	Balance General, el Estado de Resultados, el Estado de Flujo de Efectivo, el Estado de Evolución de Patrimonio y sus respectivas notas. NOTA: Deben consignar la firma del Representante Legal así inscrito en el RMV como quien los elabora.
<b>Matricula de Registro de Comercio Actualizada</b>	Anual	180 días después del cierre de gestión	Contabilidad/Legal	Jefe Administrativo Oficina Central	Area contable completa la información del formulario y encuesta anual y se entrega al departamento legal para que se realice el trámite en FUNDEMPRESA.

**Anexo No. 9.** Restricciones de la autoridad de supervisión APS

**Nota:** A manera de muestra

DETALLE	PERIODICIDAD	FECHA LÍMITE	RESPONSABLE DE PREPARAR INFORMACIÓN	RESPONSABLE DE ENVÍO NSVS	OBSERVACIONES
<b>Estados Financieros Auditados Externamente</b>	Anual	28 de Febrero	Contabilidad	Jefe Administrativo Oficina Central	Balance General, el Estado de Resultados, el Estado de Flujo de Efectivo, el Estado de Evolución de Patrimonio y sus respectivas notas.
<b>Matricula de Registro de Comercio Actualizada</b>	Anual	180 días después del cierre de gestión	Administración en coordinación con Contabilidad	Jefe Administrativo Oficina Central	Se envía la Matricula que nos certifica FUNDAEMPRESA.
<b>Constancia de Pago de Aportes</b>	Mensual	15 de cada mes	Contabilidad	Analista de Contabilidad en coordinación con Jefe de Recaudaciones y Tesorería	Formulario de Declaración de Aportes y comprobante de depósito bancario.
<b>Estados Financieros Mensuales</b>	Mensual	15 de cada mes	Contabilidad	Analista Contable	Balance General, el Estado de Resultados, el Estado de Flujo de Efectivo, el Estado de Evolución de Patrimonio y sus respectivas notas. Deben consignar la firma del Representante Legal así como quien los elabora.
<b>Reportes de Disponibilidades</b>	Mensual	5to día hábil de cada mes	Contabilidad	Analista Contable	Generar la información y enviar al Ente Regulador de manera física y magnética.

**Anexo No. 10.** Acta de Constitución del Proyecto (*Project Charter*)

ACTA DEL PROYECTO ( <i>Project Charter</i> )	
Fecha: Julio , 2017	Nombre del Proyecto: Desarrollo e implementación del Plan de Modelo de Gestión de Continuidad del Negocio para las empresas del Grupo VIDA
Áreas del Conocimiento:  Alcance, Tiempo, Costos	Área de Aplicación:  Gerencia de TI y Seguridad
Fecha de Inicio del proyecto:  Septiembre, 2017	Fecha tentativa de Finalización:  Etapa 1: Diciembre, 2018 Etapa 2: Diciembre, 2019
<p>Objetivos del proyecto:</p> <p>Objetivo General: Identificar los procesos críticos e integrar los requerimientos de seguridad con los requerimientos de la continuidad del negocio, a fin de desarrollar e implementar un modelo de Gestión de Continuidad del Negocio, para asegurar la recuperación y reanudación oportuna de los procesos definidos como críticos para Nacional Seguros.</p> <p>Objetivos Específicos:</p> <ul style="list-style-type: none"> <li>• Establecer el contexto del Negocio</li> <li>• Definir las restricciones que afectan a la organización</li> <li>• Conducir el proceso de Análisis de Riesgo</li> <li>• Elaborar el Análisis de Impacto al negocio</li> <li>• Establecer estrategia de continuidad</li> <li>• Implementar el Plan de Continuidad</li> <li>• Elaborar políticas, normas, procesos, procedimientos y planes DRP/BCP</li> <li>• Entrenar a las partes interesadas</li> <li>• Probar el Plan</li> </ul>	
<p>Descripción del producto:</p> <p>Desarrollar y gestionar un proyecto de Continuidad del negocio a nivel del Grupo Vida, que permita asegurar que las empresas del grupo puedan proveer garantía de que en el caso de una interrupción, los procesos y procedimientos del plan de continuidad del negocio, asegurarán el reinicio de los servicios críticos a su debido tiempo, asegurando de esta manera niveles de servicio aceptables para los procesos mientras se minimiza el impacto sobre el negocio.</p>	
<p>Necesidad del proyecto / Oportunidad:</p> <p>Todas las actividades de la organización son susceptibles a la interrupción ya sea por eventos internos y externos, tales como la falta de tecnología, incendios, inundaciones, falta de servicios públicos, epidemias y ataques maliciosos.</p> <p>Debido a la necesidad de mantener un nivel de servicio, seguridad y confiabilidad en los sistemas informáticos de la Compañía y además poder cumplir con las regulaciones legales y contractuales impuestas por las autoridades de supervisión, poder otorgar confianza y seguridad a los clientes e inversionistas.</p> <p>Atendiendo las recomendaciones de auditoria, practicada por parte de la empresa KPMG Ruiz Mier.</p>	

<p><b>Resultados Esperados:</b></p> <p>El Plan de continuidad debe ser capaz de:</p> <ul style="list-style-type: none"> <li>Mantener la disponibilidad de los servicios críticos del cliente</li> <li>Evitar el daño de mercado, imagen y reputación</li> <li>Proteger los activos críticos de la compañía incluyendo personal y propiedad intelectual</li> <li>Cumplir con los requerimientos legales y regulatorios</li> </ul>	
<p><b>Beneficios / impacto en la organización:</b></p> <p>Responder a incidentes que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado</p> <ul style="list-style-type: none"> <li>Cumplir con los entes reguladores ASFI (<i>Autoridad de Supervisión del Sistema Financiero</i>) y APS (<i>Autoridad de Supervisión de Pensiones y Seguros</i>)</li> <li>Subsanar las observaciones de auditoría</li> <li>Establecer una Plataforma para la normalización de los proyectos de acuerdo a las mejores prácticas del PMI</li> <li>Mejorar la toma de decisiones dentro de los proyectos de la organización</li> <li>Establecer un proceso normalizado que permita el seguimiento y la ejecución de los proyectos</li> <li>Tomar el control del estado de avance de los proyectos</li> <li>Estimular la rendición de cuentas por las partes responsables</li> </ul>	
<p><b>Restricciones:</b></p> <p>No se dispone de una base de datos de proyectos similares</p> <p>No se cuenta con un PM Interno, ni con un Auditor Líder</p> <p>No se dispone de un presupuesto para seleccionar una estrategia de continuidad</p> <p>No están definidas las responsabilidades del proyecto</p> <p>No se han definido las fechas de reuniones y entregables</p> <p>Subsanar la observación de auditoría externa</p>	
<p>Identificación de Grupos de interés y partes interesadas</p> <p>Presidencia Ejecutiva</p> <p>Gerencia General (Nacional Vida, Patrimoniales, Conecta, TECorp)</p> <p>Gerencia de Operaciones (Nacional Vida, Patrimoniales, Conecta, TECorp)</p> <p>Gerente de Tecnologías de la Información y Seguridad (TECorp)</p> <p>Auditor (Holding GNI)</p> <p>Asesor Legal (Holding GNI)</p> <p>Comité de Seguridad y Crisis (Nacional Vida, Patrimoniales, Conecta, TECorp)</p>	<p>Firma:</p>

### Anexo No. 11. Lista de Actividades

Nota: A manera de muestra

ITEM	EDT	TAREA
1	1	<b>Programa de Gestión de Continuidad del Negocio (BCM)</b>
2	1.1	<b>Etapa I - Plan de Gestión de Continuidad (BCM)</b>
3	1.1.1	Fase 1 - Gestión del Proyecto (PM)
4	1.1.1.1	Acta de Constitución del Proyecto ( <i>Project Charter</i> )
5	1.1.1.2	Estructura Detallada de Trabajo (WBS)
6	1.1.1.3	Plan de Dirección del Proyecto
7	1.1.1.4	Diccionario EDT ( <i>WBS Dictionary</i> )
8	1.1.1.5	Aprobación del Proyecto
9	1.1.1.6	Elaboración de Contrato
10	1.1.2	Fase 2 - Evaluación de Riesgos (RA)
11	1.1.2.1	Establecer el Contexto
12	1.1.2.2	Identificación de Riesgos
13	1.1.2.3	Análisis de Riesgos
14	1.1.2.4	Evaluación de Riesgos
15	1.1.2.5	Comunicación y Consulta
16	1.1.2.6	Informe de Tratamiento de Riesgos
17	1.1.2.7	Monitoreo y Revisión
18	1.1.3	Fase 3 - Análisis de Impacto
19	1.1.3.1	Identificar Instalaciones
20	1.1.3.2	Identificar Procesos y Criticidad
21	1.1.3.3	Establecer Procesos Críticos
22	1.1.3.4	FRM de Interrupción Tolerable del Negocio (RPO, RTO, MTD)
23	1.1.3.5	Informe de Evaluación de Impacto (BIA)
24	1.1.3.6	Monitoreo y Revisión
25	1.1.4	Fase 4 - Selección de Estrategia de Continuidad
26	1.1.4.1	Proyecto Sitio Alterno
27	1.1.4.1.1	Evaluar <i>Mirror Site</i> (Estrategia Sitio Espejado)
28	1.1.4.1.2	Evaluar <i>Hot Site</i> (Estrategia Sitio Caliente)
29	1.1.4.1.3	Evaluar <i>Warm Site</i> (Estrategia Sitio Templado)
30	1.1.4.1.4	Evaluar <i>Cold Site</i> (Estrategia Sitio Frio) Infraestructura Mín. de Recuperación
31	1.1.4.1.5	Informe de la Estrategia de Continuidad
32	1.1.4.2	Presupuesto Comercial
33	1.1.4.3	Selección de Estrategia
34	1.1.4.3.1	Aprobación de Alternativa

Fuente: Elaboración Propia, 2018.

**Anexo No. 12.** Estimación de Tiempos

ÍTEM	EDT	TAREA	Optimista (Días)	Más Probable (Días)	Pesimista (Días)	PERT (Días)
1	1	<b>Programa de Gestión de Continuidad del Negocio (BCM)</b>	369.00	560.00	776.00	578.67
2	1.1	<b>Etapa I - Plan de Gestión de Continuidad (BCM)</b>	62.00	94.00	146.00	102.33
3	1.1.1	Fase 1 - Gestión del Proyecto (PM)	11.00	18.00	36.00	19.83
10	1.1.2	Fase 2 - Evaluación de Riesgos (RA)	14.00	22.00	33.00	22.50
18	1.1.3	Fase 3 - Análisis de Impacto	16.00	24.00	36.00	24.67
25	1.1.4	Fase 4 - Selección de Estrategia de Continuidad	21.00	30.00	41.00	35.33
26	1.1.4.1	Proyecto Sitio Alterno	16.00	22.00	29.00	27.17
32	1.1.4.2	Presupuesto Comercial	3.00	5.00	7.00	5.00
33	1.1.4.3	Selección de Estrategia	2.00	3.00	5.00	3.17

35	1.2	<b>Etapa II - Plan de Implementación del BCP</b>	307.00	466.00	630.00	476.33
36	1.2.1	Fase 5 - Implementar el BCP	129.00	201.00	279.00	202.00
37	1.2.1.1	Adquisiciones	51.00	76.00	93.00	74.67
38	1.2.1.1.1	Gestión de Licitación	18.00	26.00	35.00	26.17
45	1.2.1.1.2	Gestión de Compras	33.00	50.00	58.00	48.50
49	1.2.1.2	Implementación	74.00	117.00	174.00	119.33
50	1.2.1.2.1	Implementación de Componentes de Hardware	20.00	27.00	36.00	27.33
54	1.2.1.2.2	Implementación de Componentes de Software	26.00	44.00	70.00	45.33
62	1.2.1.2.3	Afinamiento y Fortalecimiento	15.00	21.00	28.00	21.17
67	1.2.1.2.4	Documentación y Registros	13.00	25.00	40.00	25.50
71	1.2.1.3	Pruebas de Calidad	4.00	8.00	12.00	8.00
76	1.2.2	Fase 6 - Entrenamiento y Pruebas	10.00	18.00	26.00	18.00
77	1.2.2.1	Incidentes	4.00	6.00	8.00	6.00
82	1.2.2.2	Pruebas DRP	4.00	8.00	12.00	8.00
87	1.2.2.3	Pruebas BCP	2.00	4.00	6.00	4.00

90	1.2.3	Fase 7 - Estrategia de Ciberseguridad	168.00	247.00	325.00	246.83
92	1.2.3.1.1	Implementación de Componentes de <i>Hardware</i>	65.00	90.00	120.00	90.83
97	1.2.3.1.2	Implementación de Componentes de <i>Software</i>	55.00	85.00	115.00	85.00
102	1.2.3.1.3	Capacitación y Pruebas	18.00	27.00	40.00	27.67
105	1.2.4	Fase 8 - Revisión y Cierre del Proyecto	6.00	9.00	15.00	9.50

**Fuente:** Elaboración Propia, 2018

**Anexo No. 13.** Estimación de Costos

EDT	TAREA	Optimista (USD)	Más Probable (USD)	Pesimista (USD)	PERT (USD)
1	<b>Programa de Gestión de Continuidad del Negocio (BCM)</b>	<b>797,308.59</b>	<b>862,662.73</b>	<b>922,928.77</b>	<b>863,013.11</b>
1.1	<b>Etapa I - Plan de Gestión de Continuidad (BCM)</b>	<b>18,354.92</b>	<b>27,928.72</b>	<b>43,682.27</b>	<b>28,958.68</b>
1.1.1	<b>Fase 1 - Gestión del Proyecto (PM)</b>	<b>3,530.67</b>	<b>5,777.46</b>	<b>11,554.91</b>	<b>6,365.90</b>
1.1.2	<b>Fase 2 - Evaluación de Riesgos (RA)</b>	<b>4,311.41</b>	<b>6,788.08</b>	<b>10,136.58</b>	<b>6,933.39</b>
1.1.3	<b>Fase 3 - Análisis de Impacto</b>	<b>5,195.16</b>	<b>7,798.71</b>	<b>11,709.99</b>	<b>8,016.66</b>
1.1.4	<b>Fase 4 - Estrategia de Continuidad</b>	<b>5,317.69</b>	<b>7,564.48</b>	<b>10,280.79</b>	<b>7,642.73</b>
1.1.4.1	Proyecto Sitio Alterno	<b>4,560.80</b>	<b>6,371.68</b>	<b>8,446.06</b>	<b>6,415.60</b>
1.1.4.2	Presupuesto Comercial	<b>344.83</b>	<b>574.71</b>	<b>804.60</b>	<b>574.71</b>
1.1.4.3	Selección de Estrategia	<b>412.05</b>	<b>618.08</b>	<b>1,030.14</b>	<b>652.42</b>
1.2	<b>Etapa II - Plan de Implementación del BCP</b>	<b>778,953.67</b>	<b>834,734.01</b>	<b>879,246.50</b>	<b>834,054.43</b>
1.2.1	<b>Fase 5 - Implementar el BCP</b>	<b>524,668.40</b>	<b>559,158.75</b>	<b>598,118.44</b>	<b>559,903.64</b>
1.2.1.1	<b>Adquisiciones</b>	<b>466,209.86</b>	<b>495,970.06</b>	<b>529,435.91</b>	<b>496,587.67</b>
1.2.1.1.1	Gestión de Licitación	<b>5,892.40</b>	<b>8,575.10</b>	<b>11,578.77</b>	<b>8,628.60</b>
1.2.1.1.2	Gestión de Compras	<b>460,317.46</b>	<b>487,394.96</b>	<b>517,857.14</b>	<b>487,959.07</b>
1.2.1.2	<b>Implementación</b>	<b>48,101.40</b>	<b>52,222.30</b>	<b>57,030.74</b>	<b>52,336.89</b>
1.2.1.2.1	Implementación de Componentes de Hardware	<b>7,480.16</b>	<b>7,920.17</b>	<b>8,415.18</b>	<b>7,929.33</b>
1.2.1.2.2	Implementación de Componentes de Software	<b>23,015.87</b>	<b>24,369.75</b>	<b>25,892.86</b>	<b>24,397.95</b>
1.2.1.2.3	Afinamiento y Fortalecimiento	<b>16,111.11</b>	<b>17,058.82</b>	<b>18,125.00</b>	<b>17,078.57</b>
1.2.1.2.4	Documentación y Registros	<b>1,494.25</b>	<b>2,873.56</b>	<b>4,597.70</b>	<b>2,931.03</b>
1.2.1.3	<b>Pruebas de Calidad</b>	<b>10,357.14</b>	<b>10,966.39</b>	<b>11,651.79</b>	<b>10,979.08</b>
1.2.2	<b>Fase 6 - Entrenamiento y Pruebas</b>	<b>1,700.28</b>	<b>3,170.68</b>	<b>4,641.07</b>	<b>3,170.68</b>
1.2.2.1	Incidentes	<b>459.77</b>	<b>689.66</b>	<b>919.54</b>	<b>689.66</b>
1.2.2.2	Pruebas DRP	<b>919.54</b>	<b>1,839.08</b>	<b>2,758.62</b>	<b>1,839.08</b>
1.2.2.3	Pruebas BCP	<b>320.97</b>	<b>641.94</b>	<b>962.91</b>	<b>641.94</b>

<b>1.2.3</b>	<b>Fase 7 - Estrategia de Ciberseguridad</b>	<b>252,584.99</b>	<b>272,404.58</b>	<b>276,486.99</b>	<b>269,781.72</b>
1.2.3.1.1	Implementación de Componentes de <i>Hardware</i>	171,288.94	184,181.66	186,023.48	182,339.84
1.2.3.1.2	Implementación de Componentes de <i>Software</i>	79,394.08	85,369.98	86,223.68	84,516.28
1.2.3.1.3	Capacitación y Pruebas	1,901.96	2,852.94	4,239.83	2,925.59
<b>1.2.4</b>	<b>Fase 8 - Revisión y Cierre del Proyecto</b>	<b>756.88</b>	<b>1,135.32</b>	<b>1,892.21</b>	<b>1,198.40</b>

**Fuente:** Elaboración Propia, 2018.

**Anexo No. 14.** Activos críticos identificados

- P1 Proceso Crítico 1
- P2 Proceso Crítico 2
- P3 Proceso Crítico 3
- D11 Documento Uso Público
- D12 Documento Uso Interno
- D13 Documento Confidencial
- D14 Documento Secreto
- SI21 Infraestructura de Colaboración
- SW31 Sistema de Aplicación (ERP)
- SW32 Motor de Base de Datos (*SQL Server*)
- SW33 Servicio de Publicación (IIS)
- SW34 Sistemas Operativos de Red
- SW35 Suite Ofimática del Usuario
- SW36 Utilitarios
- SW37 Máquina Virtual
- SW38 *Hipervisor*
- HW51 Servidor Físico
- HW52 *Switch* (comutador)
- HW53 *Router* (Enrutador)
- HW54 *Firewall* (Pared de Fuego)
- HW55 *Fibridge/Transceiver* (Conversor OE)
- HW56 PBX (Central Telefónica)
- HW57 Modem ADSL (Equipo de Modulación)
- HW58 Equipo Computador (PC Escritorio/Portátil)
- HW59 Equipos Utilitarios (*Data Show*, Impresora, Escáner)
- HW60 *Storage SAN* (*Storage Area Network*)
- HW61 *Backup NAS* (*Network attached Storage*)
- COM71 Red Lan (Local/Wireless)
- COM72 Enlace F.O (Tx Voz/Datos)
- COM73 Enlace E1 (Tx Voz)
- COM74 Enlace Internet (ADSL/OnLine)
- COM75 Acelerador de Ancho de banda
- COM76 Enlace Nacional (Punto a Punto)
- COM77 Red Privada Virtual (VPN *Site2Site*, *Client2Site*)
- AUX91 Aire Acondicionado
- AUX92 UPS (Sistema Ininterrumpido de Energía)
- AUX93 Energía No Regulada
- AUX94 Sistemas Esenciales (Iluminación, Alarmas)
- SS101 Servicios Generales (Seguridad Física, Limpieza, Mantenimiento)
- SS102 *Holding* (RRHH, Legal, Auditoria)
- SS103 Proveedores de Telecomunicaciones
- L111 Sitio Central
- L112 Sitio Alterno
- L113 Agencias Locales/Regionales

- P121 Usuario Interno (Local/Remoto/Regional)
- P122 Usuario Externo (Internet/Móvil)
- P123 Soporte L1 (*Help Desk* Técnico de Soporte)
- P124 Soporte L2 (Administradores Infraestructura Tecnológica)

**Anexo No. 15.** Grado de Dependencia de Activos

Nota: A manera de muestra

Dominio	Descripción	Grupo	ID	Activo	#	Dependencia	[D]	[I]	[C]	[A]	[T]
[B]	Capa de Negocio										
		Procesos									
		P1		Proceso Crítico 1			100%	100%	100%	100%	10%
				D11	Doc. Uso Publico		50%	25%	50%		
				D12	Doc. Interno		50%	25%	50%	50%	10%
				D13	Doc. Confidencial		50%	25%	80%	100%	10%
				D14	Doc. Secreto		50%	25%	100%	100%	10%
				SW31	Sistema de Aplicación (ERP)		100%	100%	100%	100%	10%
				P121	Usuario Interno (Local/Remoto/Regional)		50%	25%	50%		10%
				P122	Usuario Externo (Internet/Móvil)		50%	25%	50%		10%
		Documentos									
		D11		Documento Uso Publico			50%	10%	1%		
				SW31	Sistema de Aplicación (ERP)		5%	10%	1%		
				HW58	Equipo Computador (PC Escritorio/Portátil)		5%	10%	1%		
				P122	Usuario Externo (Internet/Móvil)		25%	50%	5%		
[SI]	Servicios Internos										
		SI21		Infraestructura de Colaboración			100%	50%	70%	50%	50%
				SW34	Sistemas Operativos de Red		100%	50%	70%	50%	50%
				SW35	Suite Ofimática del Usuario		50%	25%	35%		
[EQ]	Equipamiento										
		[SW] Aplicaciones									
			SW31	Sistema de Aplicación (ERP)							
				SW32	Motor de base de Datos (SQL Server)		50%	50%	50%	10%	10%

Dominio	Descripción	Grupo	ID	Activo	#	Dependencia	[D]	[I]	[C]	[A]	[T]
					SW33	Servicio de Publicación (IIServer)	50%		10%	10%	10%
					P124	Soporte L2 (Administradores Infraestructura IT)	10%		10%		
	<b>[HW] Equipos</b>										
		HW51		Servidor Físico/Virtual							
					HW52	Switch (comutador)	90%				
					L111	Sitio Central	100%				
					L112	Sitio Alterno	100%				
					L113	Agencias Locales/Regionales	100%				
					P124	Soporte L2 (Administradores Infraestructura IT)	10%			50%	50%
	<b>[COM] Comunicaciones</b>										
		COM71		Red LAN (Local/Wireless)							
					HW52	Switch (comutador)	50%				
					P123	Soporte L1 (Help Desk Técnico de Soporte)	10%				
	<b>[AUX] Auxiliares</b>										
		AUX91		Aire Acondicionado							
					AUX93	Energía No Regulada	100%				
[SS]	<b>Servicios Subcontratados</b>										
			SS102	Holding (RRHH,Legal, Auditoria)							
					HW58	Equipo Computador (PC Escritorio/Portátil)	50%				
					HW59	Equipos Utilitarios (Data Show, Impresora, Escáner)	10%				
[L]	<b>Instalaciones</b>										
		L111		Sitio Central							
					AUX91	Aire Acondicionado	90%				

Dominio	Descripción	Grupo	ID	Activo	#	Dependencia	[D]	[I]	[C]	[A]	[T]
					AUX92	UPS (Sistema Ininterrumpido de Energía)	90%				
					AUX93	Energía No Regulada	50%				
					AUX94	Sistemas Esenciales (Iluminación, Alarmas)	50%				
[P]	Personal										
		P121				Usuario Interno (Local/Remoto/Regional)					
					SI21	Infraestructura de Colaboración	50%	10%	50%	0%	0%
					HW58	Equipo Computador (PC Escritorio/Portátil)	50%			0%	
					HW59	Equipos Utilitarios (Data Show, Impresora, Escáner)	10%				
					COM71	Red LAN (Local/Wireless)	50%			0%	
Total			8	144			52	5	2	7	48

Fuente: Elaboración Propia, 2018.

**Anexo No. 16.** Valoración de las amenazas sobre la plataforma tecnológica

Nota: A manera de muestra

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
[B]	<b>Capa de Negocio</b>							
		<b>Procesos</b>					0%	50% 50%
			A.07	Uso no previsto	1		50%	50%
		<b>Documentos</b>					50%	100% 100%
			E.02	Errores del Administrador del Sistema	1	20%	20%	20%
			E.15	Alteración o Modificación de la Información	1		1%	
			E.18	Destrucción de la Información	1	1%		
			A.05	Suplantación de Identidad del usuario	10		10%	50%
			A.06	Abuso de privilegios de acceso	10		10%	50%
			A.11	Acceso no autorizado	100		10%	50%
			A.15	Modificación de la Información	10		100%	
			A.18	Destrucción de la Información	10	50%		
			A.19	revelación de la Información (Dataleaks)	10			90%
			A.19	revelación de la Información (Dataleaks)	10			100%
[SI]	<b>Servicios Internos</b>							
		<b>Infraestructura de Colaboración</b>					100%	100% 100%
			I.05	Avería de origen físico o lógico	1	50%		
			E.01	Errores y fallos de los usuarios	1	1%	10%	10%
			E.02	Errores del Administrador del Sistema	1	20%	20%	20%
			E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, Spyware)	1	10%	10%	10%
			E.09	Errores de re-encaminamiento	1			10%
			E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )	1		20%	
			E.18	Destrucción de la Información	1	50%		
			E.19	Fuga de Información ( <b>Confidencialidad</b> )	1			10%

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
			E.20	Vulnerabilidad de los Programas	1	1%	20%	20%
			E.21	Errores de Mantenimiento / Actualización ( <i>software</i> )	10	1%	1%	
			A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )	1		50%	50%
			A.06	Abuso de privilegios de acceso	1		10%	10%
			A.07	Uso no previsto	1	20%	10%	10%
			A.08	Difusión de Software Dañino	1	100%	100%	100%
			A.09	Re-encaminamiento de mensajes	1			100%
			A.11	Acceso no autorizado	1		10%	50%
			A.15	Modificación de la Información ( <i>Defacement</i> )	1		50%	
			A.18	Destrucción de la Información	1	50%		
			A.19	revelación de la Información ( <i>Wikileaks</i> )	1			50%
			A.22	Manipulación del software	5		100%	100%
[EQ]	Equipamiento							
		<b>[SW] Aplicaciones</b>				100%	100%	100%
			I.05	Avería de origen físico o lógico	1	50%		
			E.01	Errores y fallos de los usuarios	1	1%	10%	10%
			E.02	Errores del Administrador del Sistema	1	20%	20%	20%
			E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, <i>Spyware</i> )	1	10%	10%	10%
			E.09	Errores de re-encaminamiento	1			10%
			E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )	1		100%	
			E.18	Destrucción de la Información	1	50%		
			E.19	Fuga de Información ( <b>Confidencialidad</b> )	1			10%
			E.20	Vulnerabilidad de los Programas	1	1%	20%	20%
			E.21	Errores de Mantenimiento / Actualización ( <i>software</i> )	10	1%	1%	
			A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )	1		50%	50%
			A.06	Abuso de privilegios de acceso	1		10%	10%

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
			A.07	Uso no previsto	1	100%	10%	10%
			A.08	Difusión de Software Dañino	1	100%	100%	100%
			A.09	Re-encaminamiento de mensajes	1			100%
			A.11	Acceso no autorizado	1		10%	50%
			A.15	Modificación de la Información ( <i>Defacement</i> )	1		50%	
			A.18	Destrucción de la Información	1	50%		
			A.19	revelación de la Información ( <i>Wikileaks</i> )	1			50%
			A.22	Manipulación del software	5		100%	100%
	<b>[HW] Equipos</b>					100%	20%	100%
			N.01	Fuego	0.1	100%		
			N.02	Daños por Agua	0.1	50%		
			N.*	Desastres Naturales	0.1	100%		
			I.01	Fuego	0.5	100%		
			I.02	Daños por agua	0.5	50%		
			I.*	Desastres Industriales	0.5	100%		
			I.05	Avería de origen físico o lógico	1	50%		
			I.06	Corte del Suministro Eléctrico	1	100%		
			I.07	condiciones inadecuadas de temperatura/humedad	1	100%		
			E.02	Errores del Administrador del Sistema	1	20%	20%	20%
			E.23	Errores de Mantenimiento / Actualización ( <i>hardware</i> )	1	10%		
			E.24	Caída del Sistema por agotamiento de Recursos <b>(Disponibilidad)</b>	10	50%		
			E.25	Perdida de Equipos	1	100%		
			A.06	Abuso de privilegios de acceso	1		10%	50%
			A.07	Uso no previsto	1	100%	1%	10%
			A.11	Acceso no autorizado	1		10%	50%
			A.23	Manipulación del Hardware	0.5	50%		50%

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
			A.24	Denegación de Servicio (DoS)	2	100%		
			A.25	Robo de Equipos	1	100%		100%
			A.26	Ataque destructivo (Vandalismo/terrorismo)	1	100%		
		<b>[COM] Comunicaciones</b>				50%	20%	100%
			I.08	Fallo en servicios de comunicaciones (Interrupción Accidental o Deliberada)	1	50%		
			E.02	Errores del Administrador del Sistema	1	20%	20%	20%
			E.09	Errores de re-encaminamiento	1			10%
			E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )	1		1%	
			E.19	Fuga de Información ( <b>Confidencialidad</b> )	1			10%
			E.24	Caída del Sistema por agotamiento de Recursos ( <b>Disponibilidad</b> )	1	50%		
			A.05	Suplantación de Identidad del usuario ( <i>Phishing</i> )	1		10%	50%
			A.06	Abuso de privilegios de acceso	1		10%	50%
			A.07	Uso no previsto	1	10%	10%	10%
			A.09	Re-encaminamiento de mensajes	1			10%
			A.10	Alteración de Secuencia	1		50%	
			A.11	Acceso no autorizado	1		10%	50%
			A.12	Análisis de Trafico	1			1%
			A.14	Interceptación de la Información ( <i>sniffers</i> )	1			100%
			A.15	Modificación de la Información ( <i>Defacement</i> )	1		10%	
			A.19	revelación de la Información ( <i>Wikileaks</i> )	1			50%
			A.24	Denegación de Servicio (DoS)	10	50%		
			A.26	Ataque destructivo (Vandalismo/terrorismo)	1	50%		
		<b>[AUX] Elementos Auxiliares</b>				100%	0%	0%
			N.01	Fuego	0.1	100%		
			N.02	Daños por Agua	0.1	50%		

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
			N.*	Desastres Naturales	0.1	100%		
			I.01	Fuego	0.5	100%		
			I.02	Daños por agua	0.5	50%		
			I.*	Desastres Industriales	0.5	100%		
			I.05	Avería de origen físico o lógico	1	10%		
			I.06	Corte del Suministro Eléctrico	1	50%		
			I.07	condiciones inadecuadas de temperatura/humedad	5	100%		
			I.09	Interrupción de otros servicios o suministros esenciales	1	10%		
			E.23	Errores de Mantenimiento / Actualización ( <i>hardware</i> )	1	10%		
			A.07	Uso no previsto	1	10%		
			A.23	Manipulación del Hardware	1	50%		
			A.25	Robo de Equipos	1	10%		
			A.26	Ataque destructivo (Vandalismo/terrorismo)	1	10%		
[SS]	<b>Servicios Subcontratados</b>					50%	0%	50%
			E.28	Indisponibilidad del Personal (Enfermedad, Huelga)	0.5	10%		
			A.19	revelación de la Información	1			50%
			A.25	Robo de Equipos	1	50%		
			A.29	Extorsión	0.5	10%		
			A.30	Ingeniería Social	0.5	10%		
[L]	<b>Instalaciones</b>					100%	50%	50%
			N.01	Fuego	1	100%		
			N.02	Daños por Agua	1	100%		
			N.*	Desastres Naturales	0.5	100%		
			I.01	Fuego	1	100%		
			I.02	Daños por agua	1	100%		
			I.*	Desastres Industriales	1	100%		
			E.19	Fuga de Información ( <b>Confidencialidad</b> )	1			10%

Dominio	Descripción	Grupo	ID	Amenazas	Frecuencia	[D]	[I]	[C]
			E.15	Alteración o Modificación de la Información ( <b>Integridad</b> )	1		1%	
			E.18	Destrucción de la Información	1	100%		
			A.07	Uso no previsto	1	10%	50%	50%
			A.11	Acceso no autorizado	5		10%	10%
			A.26	Ataque destructivo (Vandalismo/terrorismo)	0.1	100%		
[P]	Personal					50%	100%	100%
		Usuarios de Sistemas						
			E.19	Fuga de Información ( <b>Confidencialidad</b> )	1			10%
			E.28	Indisponibilidad del Personal (Enfermedad, Huelga)	1	30%		
			A.19	revelación de la Información	10			50%
			A.25	Robo de Equipos	1	50%		
			A.29	Extorsión	0.5	50%	100%	100%
			A.30	Ingeniería Social	0.5	50%	100%	100%
<b>Total Amenazas</b>		<b>129</b>						

**Fuente:** Elaboración Propia, 2018.

**Anexo No. 17.** Identificación de Vulnerabilidades**Nota:** A manera de muestra

Dominio	Grupo	ID	Vulnerabilidad	Amenaza
<b>Capa de Negocio</b>				
	<b>Procesos</b>			
		BP.01	Ausencia Proc. Registro y retiro de Usuarios	Abuso de los derechos
		BP.03	Ausencia o insuficiencia de disposiciones en los contratos con clientes y/o terceras partes	Abuso de los derechos
		BP.05	Ausencia de auditorías regulares	Abuso de los derechos
		BP.06	Ausencia Proc. Identificación y valoración de Riesgos	Abuso de los derechos
		BP.10	Ausencia de Proc. Control de Cambios	Incumplimiento en el Mantenimiento del Sistema
		BP.14	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
		BP.15	Ausencia de Planes de Continuidad	Falla del equipo
		BP.16	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
		BP.20	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
		BP.21	Ausencia o insuficiencia en las disposiciones (Seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
		BP.23	Ausencia de Política sobre la utilización de computadoras portátiles	Hurto de Equipo
		BP.24	Ausencia de Control de los activos que se encuentran fuera de las instalaciones	Hurto de medios o documentos
		BP.25	Ausencia o insuficiencia de Política de escritorios limpios	Hurto de medios o documentos
		BP.29	Ausencia de Proc. Presentación de Informes sobre las debilidades en la seguridad	Uso no autorizado del Equipo
	<b>Documentos</b>			
		D.02	Ausencia Proc. Revisión (supervisión) de los derechos de acceso	Abuso de los derechos

Dominio	Grupo	ID	Vulnerabilidad	Amenaza
		D.04	Ausencia Proc. Monitoreo de los recursos de procesamiento de Información	Abuso de los derechos
		D.13	Ausencia de Proc. Autorización de la información disponible al publico	Datos provenientes de fuentes no confiables
		D.19	Ausencia Proc. Manejo de Información Clasificada	Error en el uso
		D.26	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
<b>Servicios Internos</b>				
<b>Infraestructura de Colaboración</b>				
		SI.05	Ausencia de pistas de auditoria	Abuso de los Derechos
		SI.07	Software ampliamente distribuido	Corrupción de Datos
		SI.09	Interfaz de usuario compleja	Error en el Uso
		SI.10	Ausencia de Documentación del Sistema	Error en el Uso
		SI.11	Configuración incorrecta de parámetros	Error en el Uso
		SI.13	Ausencia de Mecanismos de Identificación y autenticación	Falsificación de Derechos
		SI.14	Tablas de Contraseñas sin protección	Falsificación de Derechos
		SI.15	Gestión deficiente de las contraseñas	Falsificación de Derechos
		SI.16	Habilitación de Servicios innecesarios	Procesamiento ilegal de datos
		SI.17	Software nuevo o inmaduro	Mal funcionamiento del Software
		SI.19	Ausencia de Control de Cambios	Mal funcionamiento del Software
		SI.21	Ausencia de Copias de Respaldo	Manipulación con Software
		SI.23	Falla en la producción de Informes de gestión	Uso no autorizado del equipos
		SI.27	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Uso no autorizado del Equipo
<b>Equipamiento</b>				
	<b>[SW] Aplicaciones</b>			
		SW.01	Ausencia o insuficiencia de Pruebas	Abuso de los Derechos
		SW.02	Defectos bien conocidos en el software	Abuso de los Derechos

Dominio	Grupo	ID	Vulnerabilidad	Amenaza
		SW.03	Ausencia de "Terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los Derechos
		SW.05	Ausencia de pistas de auditoria	Abuso de los Derechos
		SW.06	Asignación errada de los derechos de acceso	Abuso de los Derechos
		SW.10	Ausencia de Documentación del Sistema	Error en el Uso
		SW.12	Fechas incorrectas	Error en el Uso
		SW.13	Ausencia de Mecanismos de Identificación y autenticación	Falsificación de Derechos
		SW.14	Tablas de Contraseñas sin protección	Falsificación de Derechos
		SW.15	Gestión deficiente de las contraseñas	Falsificación de Derechos
		SW.16	Habilitación de Servicios innecesarios	Procesamiento ilegal de datos
		SW.18	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del Software
		SW.19	Ausencia de Control de Cambios	Mal funcionamiento del Software
		SW.20	Descarga y Uso no controlado del Software	Manipulación con Software
		SW.21	Ausencia de Copias de Respaldo	Manipulación con Software
		SW.23	Falla en la producción de Informes de gestión	Uso no autorizado del equipos
<b>[HW] Equipos</b>				
		HW.01	Mantenimiento insuficiente	Incumplimiento en el mantenimiento
		HW.02	Ausencia de esquemas de reemplazo	Destrucción de equipos o de medios
		HW.03	Susceptibilidad a la humedad, el Polvo	Polvo, Corrosión, Congelamiento
		HW.05	Ausencia de Control de Cambio	Error en el Uso
		HW.06	Susceptibilidad a las variaciones de Voltaje	Perdida de Suministro de Energía
		HW.07	Susceptibilidad a las variaciones de Temperatura	Fenómenos meteorológicos
		HW.08	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los Derechos
		HW.09	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
<b>[COM] Comunicaciones</b>				
		COM.01	Ausencia de pruebas de envío o recepción de mensajes	Negación de Acciones

Dominio	Grupo	ID	Vulnerabilidad	Amenaza
		COM.02	Líneas de comunicación sin Protección	Escucha encubierta
		COM.03	Trafico sensible sin protección	Escucha encubierta
		COM.04	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
		COM.05	Punto único de fallas	Falla del equipo de telecomunicaciones
		COM.06	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de Derechos
		COM.07	Arquitectura insegura de la red	Espionaje remoto
		COM.08	Transferencias de contraseñas en texto claro	Espionaje remoto
		COM.09	Gestión inadecuada de la red (Fallas de enrutamiento)	Saturación del sistema de información
		COM.10	Conexiones de red pública sin protección	Uso no autorizado del equipos
<b>[AUX] Elementos Auxiliares</b>				
		AUX.01	Mantenimiento insuficiente	Incumplimiento en el mantenimiento
		AUX.02	Susceptibilidad a la humedad, el Polvo	Polvo, Corrosión, Congelamiento
		AUX.03	Ausencia de Control de Cambio	Error en el Uso
		AUX.04	Susceptibilidad a las variaciones de Voltaje	Perdida de Suministro de Energía
		AUX.05	Susceptibilidad a las variaciones de Temperatura	Fenómenos meteorológicos
		AUX.06	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
<b>Servicios Subcontratados</b>				
		SS.01	Ausencia del Personal	Incumplimiento en la disponibilidad del Personal
		SS.02	Uso incorrecto del Software o Hardware	Error en el uso
		SS.03	Falta de Conciencia acerca de la Seguridad	Error en el uso
		SS.04	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
		SS.05	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
		SS.06	Ausencia o insuficiencia de disposiciones en los contratos con clientes y/o terceras partes	Abuso de los derechos
		SS.07	Ausencia de auditorías regulares	Abuso de los derechos
		SS.08	Ausencia o insuficiencia en las disposiciones (Seguridad de la información) en los contratos Terciarizados	Procesamiento ilegal de datos

<b>Dominio</b>	<b>Grupo</b>	<b>ID</b>	<b>Vulnerabilidad</b>	<b>Amenaza</b>
		SS.09	Ausencia de Presentación de Informes sobre las actividades	Incumplimiento Debida Diligencia
<b>Instalaciones</b>				
		L.01	Uso inadecuado o descuidado del control de acceso a las edificaciones y los recintos	Destrucción de equipos o medios
		L.02	Ubicación en un área susceptible de inundación	Inundación
		L.03	Red de energía inestable	Perdida del suministro de energía
		L.04	Ausencia de protección física en la edificación, puertas y ventanas	Hurto de Equipo
<b>Personal</b>				
		PE.01	Ausencia del Personal	Incumplimiento en la disponibilidad del Personal
		PE.02	Procedimientos inadecuados de contratación	Destrucción de equipos o Medios
		PE.03	Entrenamiento insuficiente en seguridad	Error en el uso
		PE.04	Uso incorrecto del Software o Hardware	Error en el uso
		PE.05	Falta de Conciencia acerca de la Seguridad	Error en el uso
		PE.06	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
		PE.07	Trabajo no supervisado del personal Interno o Temporal	Hurto de medios o documentos
		PE.08	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
<b>Total Vulnerabilidades</b>			<b>94</b>	

Fuente: Elaboración Propia, 2018.

**Anexo No. 18.** Valoración de las consecuencias (Impactos)

Nota: A manera de muestra

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
<b>Capa de Negocio</b>											
	Procesos		14	9	7	5	5	5	7	5	34
		BP.01	Ausencia Proc. Registro y retiro de Usuarios	Abuso de los derechos	2	3	3	5	3	5	21
		BP.03	Ausencia o insuficiencia de disposiciones en los contratos con clientes y/o terceras partes	Abuso de los derechos	2	1	2	5	5	3	18
		BP.05	Ausencia de auditorías regulares	Abuso de los derechos	1	3	3	5	5	3	20
		BP.06	Ausencia Proc. Identificación y valoración de Riesgos	Abuso de los derechos	3	5	3	5	3	3	22
		BP.10	Ausencia de Proc. Control de Cambios	Incumplimiento en el Mantenimiento del Sistema	3	5	1	5	3	3	20
		BP.14	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones	1	5	5	5	3	3	22
		BP.15	Ausencia de Planes de Continuidad	Falla del equipo	7	5	5	5	7	3	32
		BP.16	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso	1	3	1	2	3	3	13
		BP.20	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso	3	3	2	5	2	3	18
		BP.21	Ausencia o insuficiencia en las disposiciones (Seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos	3	1	1	3	5	5	18
		BP.23	Ausencia de Política sobre la utilización de computadoras portátiles	Hurto de Equipo	2	1	2	3	2	3	13
		BP.24	Ausencia de Control de los activos que se encuentran fuera de las instalaciones	Hurto de medios o documentos	3	2	3	3	3	3	17
		BP.25	Ausencia o insuficiencia de Política de escritorios limpios	Hurto de medios o documentos	2	1	1	2	5	1	12

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
		BP.29	Ausencia de Proc. Presentación de Informes sobre las debilidades en la seguridad	Uso no autorizado del Equipo	3	5	3	5	3	3	22
	Documentos		5	4	5	5	4	7	7	5	33
		D.02	Ausencia Proc. Revisión (supervisión) de los derechos de acceso	Abuso de los derechos	5	2	2	7	2	5	23
		D.04	Ausencia Proc. Monitoreo de los recursos de procesamiento de Información	Abuso de los derechos	5	5	3	5	2	3	23
		D.13	Ausencia de Proc. Autorización de la información disponible al publico	Datos provenientes de fuentes no confiables	2	1	4	3	3	3	16
		D.19	Ausencia Proc. Manejo de Información Clasificada	Error en el uso	4	5	3	7	7	3	29
		D.26	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos	3	5	3	5	3	3	22
<b>Servicios Internos</b>											
	Infraestructura de Colaboración				7	5	6	7	5	5	35
		SI.05	Ausencia de pistas de auditoria	Abuso de los Derechos	2	2	3	5	5	3	20
		SI.07	Software ampliamente distribuido	Corrupción de Datos	1	1	2	1	1	1	7
		SI.09	Interfaz de usuario compleja	Error en el Uso	1	3	3	1	2	1	11
		SI.10	Ausencia de Documentación del Sistema	Error en el Uso	3	5	3	3	4	3	21
		SI.11	Configuración incorrecta de parámetros	Error en el Uso	3	5	3	3	3	5	22
		SI.13	Ausencia de Mecanismos de Identificación y autenticación	Falsificación de Derechos	5	5	4	7	5	5	31
		SI.14	Tablas de Contraseñas sin protección	Falsificación de Derechos	7	3	5	5	3	5	28
		SI.15	Gestión deficiente de las contraseñas	Falsificación de Derechos	3	3	4	4	2	3	19
		SI.16	Habilitación de Servicios innecesarios	Procesamiento ilegal de datos	4	5	3	5	1	3	21
		SI.17	Software nuevo o inmaduro	Mal funcionamiento del Software	2	3	5	3	1	1	15
		SI.19	Ausencia de Control de Cambios	Mal funcionamiento del Software	3	3	4	5	2	3	20
		SI.21	Ausencia de Copias de Respaldo	Manipulación con Software	5	5	6	5	5	5	31

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
		SI.23	Falla en la producción de Informes de gestión	Uso no autorizado del equipos	2	3	3	5	3	3	19
		SI.27	<b>Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad</b>	Uso no autorizado del Equipo	3	5	5	5	3	5	26
<b>Equipamiento</b>											
	[SW] Aplicaciones		16	7	5	5	6	5	5	5	31
		SW.01	Ausencia o insuficiencia de Pruebas	Abuso de los Derechos	2	3	3	5	3	3	19
		SW.02	<b>Defectos bien conocidos en el software</b>	Abuso de los Derechos	3	4	5	5	3	5	25
		SW.03	Ausencia de "Terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los Derechos	2	1	1	3	1	3	11
		SW.05	<b>Ausencia de pistas de auditoria</b>	Abuso de los Derechos	3	3	2	5	5	3	21
		SW.06	Asignación errada de los derechos de acceso	Abuso de los Derechos	2	3	3	3	3	5	19
		SW.10	<b>Ausencia de Documentación del Sistema</b>	Error en el Uso	3	5	5	3	3	3	22
		SW.12	Fechas incorrectas	Error en el Uso	2	3	5	3	3	2	18
		SW.13	<b>Ausencia de Mecanismos de Identificación y autenticación</b>	Falsificación de Derechos	3	5	5	5	5	3	26
		SW.14	<b>Tablas de Contraseñas sin protección</b>	Falsificación de Derechos	5	5	5	5	5	5	30
		SW.15	Gestión deficiente de las contraseñas	Falsificación de Derechos	3	3	2	5	3	3	19
		SW.16	<b>Habilitación de Servicios innecesarios</b>	Procesamiento ilegal de datos	3	5	2	5	3	3	21
		SW.18	<b>Especificaciones incompletas o no claras para los desarrolladores</b>	Mal funcionamiento del Software	3	5	3	4	3	3	21
		SW.19	<b>Ausencia de Control de Cambios</b>	Mal funcionamiento del Software	5	4	5	5	4	3	26
		SW.20	<b>Descarga y Uso no controlado del Software</b>	Manipulación con Software	3	5	5	5	3	3	24
		SW.21	<b>Ausencia de Copias de Respaldo</b>	Manipulación con Software	5	5	6	5	5	5	31
		SW.23	<b>Falla en la producción de Informes de gestión</b>	Uso no autorizado del equipos	3	5	4	5	3	3	23
	[HW] Equipos		8	8	3	5	5	5	5	5	28
		HW.01	<b>Mantenimiento insuficiente</b>	Incumplimiento en el mantenimiento	3	5	3	5	3	3	22
		HW.02	Ausencia de esquemas de reemplazo	Destrucción de equipos o de medios	2	1	1	3	5	3	15

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
		HW.03	Susceptibilidad a la humedad, el Polvo	Polvo, Corrosión, Congelamiento	2	2	2	3	3	5	17
		HW.05	Ausencia de Control de Cambio	Error en el Uso	3	3	3	5	3	5	22
		HW.06	Susceptibilidad a las variaciones de Voltaje	Perdida de Suministro de Energía	3	5	4	3	3	3	21
		HW.07	Susceptibilidad a las variaciones de Temperatura	Fenómenos meteorológicos	3	5	4	3	3	3	21
		HW.08	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los Derechos	3	1	2	2	3	3	14
		HW.09	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	3	2	5	3	3	2	18
<b>[COM] Comunicaciones</b>					9	5	7	5	7	7	40
		COM.01	Ausencia de pruebas de envío o recepción de mensajes	Negación de Acciones	1	1	2	2	2	3	11
		COM.02	Líneas de comunicación sin Protección	Escucha encubierta	3	2	3	3	5	3	19
		COM.03	Trafico sensible sin protección	Escucha encubierta	3	3	4	3	5	5	23
		COM.04	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones	1	2	3	1	1	3	11
		COM.05	Punto único de fallas	Falla del equipo de telecomunicaciones	5	4	3	3	2	4	21
		COM.06	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de Derechos	1	1	2	2	2	3	11
		COM.07	Arquitectura insegura de la red	Espionaje remoto	9	5	7	5	7	5	38
		COM.08	Transferencias de contraseñas en texto claro	Espionaje remoto	3	3	4	3	5	7	25
		COM.09	Gestión inadecuada de la red (Fallas de enrutamiento)	Saturación del sistema de información	3	4	3	2	2	3	17
		COM.10	Conexiones de red pública sin protección	Uso no autorizado del equipos	3	3	3	3	3	4	19
<b>[AUX] Elementos Auxiliares</b>					3	3	5	5	5	5	26
		AUX.01	Mantenimiento insuficiente	Incumplimiento en el mantenimiento	3	3	3	5	3	3	20

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
		AUX.02	Susceptibilidad a la humedad, el Polvo	Polvo, Corrosión, Congelamiento	2	1	1	3	5	3	15
		AUX.03	Ausencia de Control de Cambio	Error en el Uso	2	3	1	3	2	2	13
		AUX.04	Susceptibilidad a las variaciones de Voltaje	Perdida de Suministro de Energía	3	3	5	3	3	5	22
		AUX.05	Susceptibilidad a las variaciones de Temperatura	Fenómenos meteorológicos	3	3	5	3	3	3	20
		AUX.06	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	3	2	5	3	3	2	18
<b>Servicios Subcontratados</b>			9	7	5	3	5	7	5	5	30
		SS.01	Ausencia del Personal	Incumplimiento en la disponibilidad del Personal	2	3	3	2	2	5	17
		SS.02	Uso incorrecto del Software o Hardware	Error en el uso	3	3	2	4	5	3	20
		SS.03	Falta de Conciencia acerca de la Seguridad	Error en el uso	3	3	5	5	4	3	23
		SS.04	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos	5	3	4	4	5	5	26
		SS.05	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos	3	3	1	5	5	3	20
		SS.06	Ausencia o insuficiencia de disposiciones (Seguridad de la información) en los contratos con Proveedores	Abuso de los derechos	2	2	2	4	5	3	18
		SS.07	Ausencia de auditorías regulares	Abuso de los derechos	2	3	3	7	3	5	23
		SS.08	Ausencia o insuficiencia en las disposiciones (Seguridad de la información) en los contratos del Personal Terciarizado	Procesamiento ilegal de datos	2	3	2	5	3	3	18
		SS.09	Ausencia de Presentación de Informes sobre las actividades	Incumplimiento Debida Diligencia	2	3	1	5	2	3	16
<b>Instalaciones</b>			4	4	5	5	5	5	5	3	28
		L.01	Uso inadecuado o descuidado del control de acceso a las edificaciones y los recintos	Destrucción de equipos o medios	3	5	3	5	5	3	24

Dominio	Grupo	ID	Vulnerabilidad	Amenaza	[F]	[O]	[I]	[N]	[L]	[P]	[T]
		L.02	Ubicación en un área susceptible de inundación	Inundación	5	3	3	4	4	3	22
		L.03	Red de energía inestable	Perdida del suministro de energía	3	5	5	4	5	3	25
		L.04	Ausencia de protección física en la edificación, puertas y ventanas	Hurto de Equipo	3	2	2	3	3	2	15
<b>Personal</b>			9	7	3	5	3	5	5	5	26
		PE.01	Ausencia del Personal	Incumplimiento en la disponibilidad del Personal	1	2	1	3	3	3	13
		PE.02	Procedimientos inadecuados de contratación	Destrucción de equipos o Medios	2	2	1	3	5	3	16
		PE.03	Entrenamiento insuficiente en seguridad	Error en el uso	2	3	3	5	5	3	21
		PE.04	Uso incorrecto del Software o Hardware	Error en el uso	2	2	1	2	2	3	12
		PE.05	Falta de Conciencia acerca de la Seguridad	Error en el uso	2	3	2	4	3	3	17
		PE.06	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos	3	5	3	3	3	5	22
		PE.07	Trabajo no supervisado del personal Interno o Temporal	Hurto de medios o documentos	2	3	2	5	3	5	20
		PE.08	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	1	2	1	2	3	3	12
		PE.09	Ausencia o insuficiencia de disposiciones (Seguridad de la información) en los contratos de funcionarios internos	Abuso de los derechos	2	2	3	3	5	3	18
<b>Total</b>			<b>95</b>	<b>67</b>							

Fuente: Elaboración Propia, 2018.

**Anexo No. 19.** Subconjunto de Amenazas definido por MAGERIT

Dominio	Descripción	ID	Elemento	Estado
[N]	<b>Desastres Naturales</b>			
		N.01	Fuego	Aplica
		N.02	Daños por Agua	Aplica
		N.*	<b>Desastres Naturales</b>	
		N.*.01	Tormentas	Aplica
		N.*.02	Tormentas Eléctricas	Aplica
		N.*.03	Huracanes	Aplica
		N.*.04	Terremotos	Aplica
		N.*.07	Deslizamientos de Terreno	Aplica
		N.*.10	Frio Extremo	Aplica
		N.*.11	Calor Extremo	Aplica
[I]	<b>Origen Industrial</b>			
		I.01	Fuego	Aplica
		I.02	Daños por agua	Aplica
		I.*	Desastres Industriales	Aplica
		<b>I.05</b>	<b>Avería de origen físico o lógico</b>	
		I.05.1	<i>Software</i>	Aplica
		I.05.2	<i>Hardware</i>	Aplica
		I.05.3	Equipos de Comunicación	Aplica
		I.05.4	Equipamiento Auxiliar	Aplica
		<b>I.06</b>	<b>Corte del Suministro Eléctrico</b>	
		I.06.11	Interrupción Accidental	Aplica
		I.06.12	Interrupción deliberada por un agente externo	Aplica
		I.06.13	Interrupción deliberada por un agente interno	Aplica
		I.07	condiciones inadecuadas de temperatura/humedad	Aplica
		<b>I.08</b>	<b>Fallo en servicios de comunicaciones</b>	
		I.08.11	Interrupción Accidental	Aplica
		I.08.12	Interrupción deliberada por un agente externo	Aplica
		I.08.13	Interrupción deliberada por un agente interno	Aplica
		<b>I.09</b>	<b>Interrupción de otros servicios o suministros esenciales</b>	
		I.09.1	Papel	Aplica
		I.09.2	Refrigerante	Aplica
		I.09.3	Diésel	Aplica
		I.10	Degradación de los soportes de almacenamiento	
[E]	<b>Errores y Fallos no intencionados</b>			
		E.01	Errores y fallos de los usuarios	Aplica

Dominio	Descripción	ID	Elemento	Estado
		E.02	Errores del Administrador del Sistema	Aplica
		E.04	Errores de Configuración	Aplica
		<b>E.08</b>	<b>Discusión de Software Dañino</b>	
		E.08.0	Gusanos	Aplica
		E.08.1	Virus	Aplica
		E.08.2	Caballos de Troya	Aplica
		E.08.3	<i>Spyware</i>	Aplica
		<b>E.09</b>	<b>Errores de re-encaminamiento</b>	
		E.09.1	Queda en Casa	Aplica
		E.09.2	A terceros con acuerdo establecido	Aplica
		E.09.3	Al mundo entero	Aplica
		E.15	Alteración o Modificación de la Información <b>(Integridad)</b>	Aplica
		E.18	Destrucción de la Información	Aplica
		<b>E.19</b>	<b>Fuga de Información (Confidencialidad)</b>	
		E.19.1	A personal interno que no necesita conocerlo	Aplica
		E.19.2	A contratistas que no necesitan conocerlo	Aplica
		E.19.3	A personas externas que no necesitan conocerlo	Aplica
		E.19.4	Al público en general	Aplica
		E.19.5	A los medios de comunicación	Aplica
		E.19.11	Identificación de la localización	Aplica
		<b>E.20</b>	<b>Vulnerabilidad de los Programas</b>	
		E.20.dos	Denegación de Servicio	Aplica
		E.20.read	Acceso de LECTURA	Aplica
		E.20.write	Acceso de ESCRITURA	Aplica
		E.20.escalation	Escalada de privilegios	Aplica
		E.21	Errores de Mantenimiento / Actualización <i>(software)</i>	Aplica
		E.23	Errores de Mantenimiento / Actualización <i>(hardware)</i>	Aplica
		E.24	Caída del Sistema ( <b>Disponibilidad</b> )	Aplica
		E.25	Perdida de Equipos	Aplica
		<b>E.28</b>	<b>Indisponibilidad del Personal</b>	
		E.28.1	Enfermedad	Aplica
		E.28.2	Huelga	Aplica
		E.28.3	No hay personal	Aplica
		E.28.4	Personal insuficiente	Aplica
<b>[A]</b>	<b>Ataques Deliberados</b>			
		A.03	Manipulación de los Registros de Actividad ( <i>log</i> )	
		<b>A.05</b>	<b>Suplantación de Identidad del usuario</b>	
		A.05.1	Por personal interno	Aplica

Dominio	Descripción	ID	Elemento	Estado
		A.05.2	Por subcontratistas	Aplica
		A.05.3	Por personas externas	Aplica
		<b>A.06</b>	<b>Abuso de privilegios de acceso</b>	
		A.06.1	Por personal interno	Aplica
		A.06.2	Por subcontratistas	Aplica
		A.06.3	Por personas externas	Aplica
		<b>A.07</b>	<b>Uso no previsto</b>	
		A.07.1	Por personal interno	Aplica
		A.07.2	Por subcontratistas	Aplica
		A.07.3	Por personas externas	Aplica
		<b>A.08</b>	<b>Difusión de Software Dañino</b>	
		A.08.0	Gusanos	Aplica
		A.08.1	Virus	Aplica
		A.08.2	Caballos de Troya	Aplica
		A.08.3	Spyware	Aplica
		<b>A.09</b>	<b>Re-encaminamiento de mensajes</b>	
		A.09.1	Sin beneficio para nadie	Aplica
		A.09.2	A beneficio del atacante	Aplica
		A.09.3	Para dañar a la víctima	Aplica
		<b>A.10</b>	<b>Alteración de Secuencia</b>	
		A.10.1	Sin beneficio para nadie	Aplica
		A.10.2	A beneficio del atacante	Aplica
		A.10.3	Para dañar a la víctima	Aplica
		<b>A.11</b>	<b>Acceso no autorizado</b>	
		A.11.1	Por personal interno	Aplica
		A.11.2	Por subcontratistas	Aplica
		A.11.3	Por personas externas	Aplica
		<b>A.12</b>	<b>Análisis de Trafico</b>	
		A.12.1	Por personal interno	Aplica
		A.12.2	Por subcontratistas	Aplica
		A.12.3	Por personas externas	Aplica
		<b>A.14</b>	<b>Interceptación de la Información (Sniffers)</b>	
		A.14.1	Por personal interno	Aplica
		A.14.2	Por subcontratistas	Aplica
		A.14.3	Por personas externas	Aplica
		<b>A.15</b>	<b>Modificación de la Información (Defacement)</b>	
		A.15.1	Sin beneficio para nadie	Aplica
		A.15.2	A beneficio del atacante	Aplica
		A.15.3	Para dañar a la víctima	Aplica
		<b>A.18</b>	<b>Destrucción de la Información</b>	

<b>Dominio</b>	<b>Descripción</b>	<b>ID</b>	<b>Elemento</b>	<b>Estado</b>
		A.18.1	Sin beneficio para nadie	Aplica
		A.18.2	A beneficio del atacante	Aplica
		A.18.3	Para dañar a la víctima	Aplica
		<b>A.19</b>	<b>Revelación de la Información</b>	
		A.19.1	A personal interno que no necesita conocerlo	Aplica
		A.19.2	A contratistas que no necesitan conocerlo	Aplica
		A.19.3	A personas externas que no necesitan conocerlo	Aplica
		A.19.4	Al público en general	Aplica
		A.19.5	A los medios de comunicación	Aplica
		A.19.11	Identificación de la localización	Aplica
		<b>A.22</b>	<b>Manipulación del software</b>	
		A.22.1	Bombas lógicas	Aplica
		A.22.2	Caballos de Troya	Aplica
		A.22.3	<i>Keylogger (spyware)</i>	Aplica
		A.22.4	Puertas Traseras	Aplica
		A.22.5	Autenticación débil	Aplica
		A.22.6	Se elude la autenticación	Aplica
		<b>A.23</b>	<b>Manipulación del Hardware</b>	Aplica
		<b>A.24</b>	<b>Denegación de Servicio (DoS)</b>	
		A.24.1	Saturación de los canales de comunicaciones	Aplica
		A.24.2	Saturación de los recursos de software	Aplica
		A.24.3	Saturación de los recursos de hardware	Aplica
		<b>A.25</b>	<b>Robo de Equipos</b>	
		A.25.1	Por personal interno	Aplica
		A.25.2	Por subcontratistas	Aplica
		A.25.3	Por personas externas	Aplica
		<b>A.26</b>	<b>Ataque destructivo (Vandalismo/terrorismo)</b>	
		A.26.1	Vandalismo	Aplica
		A.26.2	Bombas	Aplica
		A.26.3	Terrorismo	Aplica
		<b>A.28</b>	<b>Indisponibilidad del Personal (E.28)</b>	
		A.28.1	Enfermedad	Aplica
		A.28.2	Huelga	Aplica
		A.28.3	Absentismo	Aplica
		<b>A.29</b>	<b>Extorsión</b>	
		A.29.1	Ataque desde el exterior	Aplica
		A.29.2	Ataque desde el interior	Aplica
		<b>A.30</b>	<b>Ingeniería Social</b>	
		A.30.1	Ataque desde el exterior	Aplica
		A.30.2	Ataque desde el interior	Aplica

**Anexo No. 20.** Evaluación de Controles Existentes

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
<b>Capa de Negocio</b>							
	Procesos						N1 - Inicial
		A.07	Uso no previsto	Plan de Contingencia	Preventivo	1 - Ineficaz	N1 - Inicial
	Documentos						N1 - Inicial
		E.02	Errores del Administrador del Sistema				N0 - Inexistente
		E.15	Alteración o Modificación de la Información (Integridad)	Gestión de cambios	Correctivo	3 - Insuficiente	N2 - Repetible
		E.18	Destrucción de la Información				N0 - Inexistente
		E.19	Fuga de Información (Confidencialidad)	Auditoria de Escritorios Limpios	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.05	Suplantación de Identidad del usuario (Phishing)	Campaña de Concientización	Preventivo	3 - Insuficiente	N1 - Inicial
		A.06	Abuso de privilegios de acceso	Control de Acceso basado en Roles	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.11	Acceso no autorizado	Controles de Acceso	Preventivo	3 - Insuficiente	N2 - Repetible
		A.15	Modificación de la Información				N0 - Inexistente
		A.18	Destrucción de la Información				N0 - Inexistente
		A.19	Revelación de la Información (Dataleaks)	Acuerdo de Confidencialidad	Compensatorio	3 - Insuficiente	N2 - Repetible
<b>Servicios Internos</b>							
	Infraestructura de Colaboración						N2 - Repetible
		I.05	Avería de origen físico o lógico				N0 - Inexistente
		E.01	Errores y fallos de los usuarios				N0 - Inexistente
		E.02	Errores del Administrador del Sistema	Gestión de Configuración	Correctivo	3 - Insuficiente	N2 - Repetible
		E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, Spyware)	Antivirus Corporativo	Detectivo	4 - Eficaz	N4 - Gestionado

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		E.09	Errores de re-encaminamiento	Default Gateway, VLANs	Preventivo	4 - Eficaz	N3 - Definido
		E.15	Alteración o Modificación de la Información (Integridad)				N0 - Inexistente
		E.18	Destrucción de la Información				N0 - Inexistente
		E.19	Fuga de Información (Confidencialidad)	Data Loss Prevention	Compensatorio	3 - Insuficiente	N1 - Inicial
		E.20	Vulnerabilidad de los Programas	Test de Vulnerabilidad	Compensatorio	3 - Insuficiente	N2 - Repetible
		E.21	Errores de Mantenimiento / Actualización (software)	Gestión de Cambios	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.05	Suplantación de Identidad del usuario (Phishing)	Campaña de Concientización	Disuasivo	3 - Insuficiente	N1 - Inicial
		A.06	Abuso de privilegios de acceso	Controlador de Dominio	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.07	Uso no previsto	AntiSpam	Detectivo	3 - Insuficiente	N2 - Repetible
		A.08	Difusión de Software Dañino	Antivirus Corporativo	Detectivo	4 - Eficaz	N4 - Gestionado
		A.09	Re-encaminamiento de mensajes	Default Gateway, VLANs	Compensatorio	4 - Eficaz	N3 - Definido
		A.11	Acceso no autorizado	Controlador de Dominio	Preventivo	3 - Insuficiente	N2 - Repetible
		A.15	Modificación de la Información (Defacement)				N0 - Inexistente
		A.18	Destrucción de la Información				N0 - Inexistente
		A.19	Revelación de la Información (Dataleaks)				N0 - Inexistente
		A.22	Manipulación del software				N0 - Inexistente
<b>Equipamiento</b>							
	[SW] Aplicaciones						N2 - Repetible
		I.05	Avería de origen físico o lógico	Backup de Aplicaciones	Correctivo	3 - Insuficiente	N1 - Inicial
		E.01	Errores y fallos de los usuarios	Validación de Entrada de datos	Compensatorio	3 - Insuficiente	N2 - Repetible
		E.02	Errores del Administrador del Sistema	Gestión de Configuración	Correctivo	3 - Insuficiente	N2 - Repetible

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		E.08	Difusión de Software Dañino (Virus, Gusanos, Troyanos, Spyware)	Antivirus Corporativo	Detectivo	4 - Eficaz	N4 - Gestionado
		E.09	Errores de re-encaminamiento	Default Gateway, VLANs	Preventivo	4 - Eficaz	N3 - Definido
		E.15	Alteración o Modificación de la Información (Integridad)				N0 - Inexistente
		E.18	Destrucción de la Información	Backup de Aplicaciones	Correctivo	3 - Insuficiente	N1 - Inicial
		E.19	Fuga de Información (Confidencialidad)	Data Loss Prevention	Compensatorio	3 - Insuficiente	N2 - Repetible
		E.20	Vulnerabilidad de los Programas	Test de Vulnerabilidad	Compensatorio	3 - Insuficiente	N2 - Repetible
		E.21	Errores de Mantenimiento / Actualización (software)	Gestión de Cambios	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.05	Suplantación de Identidad del usuario (Phishing)	Campaña de Concientización	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.06	Abuso de privilegios de acceso	Controlador de Dominio	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.07	Uso no previsto	AntiSpam	Detectivo	3 - Insuficiente	N2 - Repetible
		A.08	Difusión de Software Dañino	Antivirus Corporativo	Detectivo	4 - Eficaz	N4 - Gestionado
		A.09	Re-encaminamiento de mensajes	Default Gateway, VLANs	Compensatorio	4 - Eficaz	N3 - Definido
		A.11	Acceso no autorizado	Controlador de Dominio	Preventivo	3 - Insuficiente	N2 - Repetible
		A.15	Modificación de la Información	Pistas de Auditoria	Detectivo	3 - Insuficiente	N2 - Repetible
		A.18	Destrucción de la Información				N0 - Inexistente
		A.19	Revelación de la Información (Dataleaks)				N0 - Inexistente
		A.22	Manipulación del software				N0 - Inexistente
	[HW] Equipos						N1 - Inicial
		N.01	Fuego	Seguro de Incendio	Correctivo	3 - Insuficiente	N1 - Inicial
		N.02	Daños por Agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N1 - Inicial
		N.*	Desastres Naturales	Plan de Contingencia	Correctivo	1 - Ineficaz	N1 - Inicial
		I.01	Fuego	Extintor	Preventivo	3 - Insuficiente	N1 - Inicial
		I.02	Daños por agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N1 - Inicial

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		I.*	Desastres Industriales	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N1 - Inicial
		I.05	Avería de origen físico o lógico	Contrato con Proveedores	Compensatorio	3 - Insuficiente	N1 - Inicial
		I.06	Corte del Suministro Eléctrico	UPS	Correctivo	3 - Insuficiente	N3 - Definido
		I.07	Condiciones inadecuadas de temperatura/humedad	Aires Acondicionados	Preventivo	3 - Insuficiente	N2 - Repetible
		E.02	Errores del Administrador del Sistema	Gestión de Configuración	Correctivo	3 - Insuficiente	N2 - Repetible
		E.23	Errores de Mantenimiento / Actualización (hardware)	Gestión de Cambios	Disuasivo	3 - Insuficiente	N2 - Repetible
		E.24	Caída del Sistema por agotamiento de Recursos (Disponibilidad)	Planeamiento de Capacidad	Compensatorio	3 - Insuficiente	N1 - Inicial
		E.25	Perdida de Equipos	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N1 - Inicial
		A.06	Abuso de privilegios de acceso	Controlador de Dominio	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.07	Uso no previsto				N0 - Inexistente
		A.11	Acceso no autorizado	Controles de Acceso	Preventivo	3 - Insuficiente	N2 - Repetible
		A.23	Manipulación del Hardware				N0 - Inexistente
		A.24	Denegación de Servicio (DoS)				N0 - Inexistente
		A.25	Robo de Equipos	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N1 - Inicial
		A.26	Ataque destructivo (Vandalismo/terrorismo)				N0 - Inexistente
	[COM] Comunicaciones						N1 - Inicial
		I.08	Fallo en servicios de comunicaciones (Interrupción Accidental o Deliberada)	Enlaces Redundantes	Preventivo	3 - Insuficiente	N2 - Repetible
		E.02	Errores del Administrador del Sistema	Gestión de Configuración	Correctivo	3 - Insuficiente	N2 - Repetible
		E.09	Errores de re-encaminamiento				N0 - Inexistente
		E.15	Alteración o Modificación de la Información (Integridad)	Túneles VPN	Preventivo	3 - Insuficiente	N2 - Repetible

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		E.19	Fuga de Información (Confidencialidad)				N0 - Inexistente
		E.24	Caída del Sistema por agotamiento e Recursos (Disponibilidad)	Planeamiento de Capacidad	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.05	Suplantación de Identidad del usuario (Phishing)				N0 - Inexistente
		A.06	Abuso de privilegios de acceso	Gestión de Configuración	Compensatorio	3 - Insuficiente	N2 - Repetible
		A.07	Uso no previsto				N0 - Inexistente
		A.09	Re-encaminamiento de mensajes	Default Gateway, VLANs	Compensatorio	4 - Eficaz	N3 - Definido
		A.11	Acceso no autorizado				N0 - Inexistente
		A.12	Análisis de Trafico				N0 - Inexistente
		A.14	Interceptación de la Información (Sniffers)				N0 - Inexistente
		A.15	Modificación de la Información (Defacement)				N0 - Inexistente
		A.19	Revelación de la Información (Dataleaks)				N0 - Inexistente
		A.24	Denegación de Servicio (DoS)				N0 - Inexistente
		A.26	Ataque destructivo (Vandalismo/terrorismo)				N0 - Inexistente
	[AUX] Elementos Auxiliares						N2 - Repetible
		N.01	Fuego	Seguro de Incendio	Correctivo	3 - Insuficiente	N1 - Inicial
		N.02	Daños por Agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		N.*	Desastres Naturales	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		I.01	Fuego	Extintor	Preventivo	3 - Insuficiente	N1 - Inicial
		I.02	Daños por agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		I.*	Desastres Industriales	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		I.05	Avería de origen físico o lógico	Redundancia de Equipos	Compensatorio	3 - Insuficiente	N1 - Inicial
		I.06	Corte del Suministro Eléctrico	Generador/UPS	Correctivo	4 - Eficaz	N4 - Gestionado
		I.07	Condiciones inadecuadas de temperatura/humedad	Aires Acondicionados	Preventivo	3 - Insuficiente	N2 - Repetible

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		I.09	Interrupción de otros servicios o suministros esenciales				N0 - Inexistente
		E.23	Errores de Mantenimiento / Actualización (hardware)	Gestión de Cambios	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.07	Uso no previsto				N0 - Inexistente
		A.23	Manipulación del Hardware				N0 - Inexistente
		A.25	Robo de Equipos	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		A.26	Ataque destructivo (Vandalismo/terrorismo)				N0 - Inexistente
<b>Servicios Subcontratados</b>							N2 - Repetible
		E.28	Indisponibilidad del Personal (Enfermedad, Huelga)	Persona de Backup Terciarizacion	Preventivo	3 - Insuficiente	N3 - Definido
		A.19	Revelación de la Información	Acuerdo de Confidencialidad	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.25	Robo de Equipos	Seguro Todo Riesgo	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.29	Extorsión				N0 - Inexistente
		A.30	Ingeniería Social	Campaña de Concientización	Disuasivo	3 - Insuficiente	N1 - Inicial
<b>Instalaciones</b>							N2 - Repetible
		N.01	Fuego	Seguro de Incendio	Correctivo	3 - Insuficiente	N1 - Inicial
		N.02	Daños por Agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		N.*	Desastres Naturales	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		I.01	Fuego	Extintor	Preventivo	3 - Insuficiente	N1 - Inicial
		I.02	Daños por agua	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		I.*	Desastres Industriales	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		E.18	Destrucción de la Información		Correctivo	4 - Eficaz	N4 - Gestionado
		E.19	Fuga de Información (Confidencialidad)				N0 - Inexistente
		A.07	Uso no previsto				N0 - Inexistente
		A.11	Acceso no autorizado	Controles de Acceso	Preventivo	3 - Insuficiente	N2 - Repetible

Dominio	Grupo	ID	Amenazas	Control Existente	Tipo de Control	Evaluación	Nivel de Madurez
		A.26	Ataque destructivo (Vandalismo/terrorismo)				N0 - Inexistente
<b>Personal</b>							<b>N1 - Inicial</b>
		Usuarios de Sistemas					
		E.19	Fuga de Información (Confidencialidad)	Campaña de Concientización	Compensatorio	3 - Insuficiente	N1 - Inicial
		E.28	Indisponibilidad del Personal (Enfermedad, Huelga)				N0 - Inexistente
		A.19	Revelación de la Información	Acuerdo de Confidencialidad	Disuasivo	3 - Insuficiente	N2 - Repetible
		A.25	Robo de Equipos	Seguro Todo Riesgo	Correctivo	3 - Insuficiente	N3 - Definido
		A.29	Extorsión				N0 - Inexistente
		A.30	Ingeniería Social	Campaña de Concientización	Disuasivo	3 - Insuficiente	N1 - Inicial
<b>Total</b>			<b>125</b>	<b>Evaluación General</b>			N2 - Repetible

Fuente: Elaboración Propia, 2019.

**Anexo No. 21.** Matriz de Determinación de Riesgos Cualitativos

Nota: A manera de muestra

Fuente de Riesgo	ID	Amenazas	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Afecta a:	Impacto	Probabilidad	Nivel de Riesgo
[N] Desastres Naturales	N.01	Fuego	Incendio	Posibilidad de que el fuego acabe con recursos del sistema	Interrupción de Actividades (Disponibilidad)	(HW) Equipos Informáticos	5	C	E
	N.02	Daños por Agua	Inundaciones	Posibilidad de que el agua acabe con recursos del sistema		(P) Personas			
	N.*	Desastres Naturales	Tormentas Eléctricas, Huracanes, Terremotos, Deslizamientos de Terreno, Frio Extremo, Calor Extremo	Posibilidad de que algún fenómeno natural cause daño a los recursos del sistema		(Medios) Soportes de Información			
[I] Origen Industrial	I.*	Desastres Industriales	Explosiones, derrumbes, contaminación, sobrecarga, accidentes de tráfico	Posibilidad de algún desastre industrial debido a la actividad humana	Interrupción de Actividades (Disponibilidad)	(L) Instalaciones		B	E
	I.03	Contaminación Mecánica	Vibraciones, Polvo, Suciedad	Posibilidad de que la contaminación Mecánica dañe los recursos del sistema		(HW) Equipos Informáticos	4	C	H

Fuente de Riesgo	ID	Amenazas	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Afecta a:	Impacto	Proba_bilidad	Nivel de Riesgo
						(AUX) Equipamiento Auxiliar			
I.04	Contaminación Electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta	Posibilidad de que la contaminación electromagnética dañe los recursos del sistema	Interrupción de Actividades (Disponibilidad)	(HW) Equipos Informáticos (COM) Comunicaciones (Medios) Soportes de Información (AUX) Equipamiento Auxiliar	2	D	M	
I.05	Avería de origen físico o lógico	Fallo en Programas, Equipos y Equipamiento Auxiliar	Defecto de origen o de funcionamiento	Interrupción de Actividades (Disponibilidad)	(HW) Equipos Informáticos (COM) Comunicaciones (Medios) Soportes de Información (AUX) Equipamiento Auxiliar	2	C	M	
I.06	Corte del Suministro Eléctrico	Interrupción Accidental, deliberada (agente externo/interno)	Posibilidad de Pérdida del Suministro de Energía	Interrupción de Actividades (Disponibilidad)	(HW) Equipos Informáticos (COM) Comunicaciones (Medios) Soportes de Información (AUX) Equipamiento Auxiliar	3	C	H	
I.07	Condiciones inadecuadas de temperatura/humedad	Exceso de Temperatura, humedad	Mala aclimatación, excediendo los márgenes de trabajo	Interrupción de Actividades (Disponibilidad)	(HW) Equipos Informáticos (COM) Comunicaciones	3	C	H	

Fuente de Riesgo	ID	Amenazas	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Afecta a:	Impacto	Proba_bilidad	Nivel de Riesgo
[E] Errores y Fallos no intencionados						(Medios) Soportes de Información (AUX) Equipamiento Auxiliar			
	L.08	Fallo en servicios de comunicaciones	Destrucción física o Interrupción Accidental, deliberada (agente externo/interno)	Incapacidad para atender al tráfico presente	Cese de la capacidad de transmitir datos (Disponibilidad)	(COM) Comunicaciones	2	B	H
	I.09	Interrupción de otros servicios o suministros esenciales	Falta de suministros papel, tóner, refrigerante, combustible	Otros servicios o recursos de los que depende la operación de los equipos	Interrupción de Actividades (Disponibilidad)	(AUX) Equipamiento Auxiliar	2	C	M
	I.10	Degradación de soportes de Almacenamiento	destrucción física o daño de medios de almacenamientos	Destrucción de medios como consecuencia del paso del tiempo	Degrado del medio (Integridad)	(Medios) Soportes de Información	1	D	L
	E.01	Errores de Usuario	Equivocaciones, descuidos, falta de capacitación	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Daños de integridad y (Disponibilidad)	(SI) Servicios Infraestructura Datos / Información (SW) Aplicaciones	2	C	M
	E.02	Errores del Administrador	Equivocaciones, descuidos, falta de capacitación	Equivocaciones de personas con responsabilidades de instalación y operación	Daños de integridad, Disponibilidad, Confidencialidad, Autenticidad	(SI) Servicios Infraestructura Datos / Información (SW) Aplicaciones (HW) Equipos Informáticos (COM) Comunicaciones	3	D	M
	E.04	Errores de Configuración	datos o registros de configuración erróneos	Prácticamente todos los activos dependen de su	Privilegios de Acceso, Registros	(SI) Servicios Infraestructura	4	E	M

Fuente de Riesgo	ID	Amenazas	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Afecta a:	Impacto	Proba_bilidad	Nivel de Riesgo
				configuración y ésta de la diligencia del administrador:	incompletos, Monitoreo, encaminamiento	Datos / Información (SW) Aplicaciones (HW) Equipos Informáticos (P) Personas			
E.08	Difusión de Software Dañino		Fallo en Programas, Equipos de Computación	Fallas de equipos, mal funcionamiento del Software, saturación del S.O (Virus, Gusanos, Caballos de Troya, Spyware)	Daños de integridad, Disponibilidad por Infección de Malware	Datos / Información (SI) Servicios Infraestructura (SW) Aplicaciones (COM) Comunicaciones (P) Personas	4	C	H
E.09	Errores de re-encaminamiento		Demora en la entrega por error de enrutamiento	Incapacidad para enrutar el tráfico de información	Cese de la capacidad de transmitir datos (Disponibilidad)	(SI) Servicios Infraestructura (SW) Aplicaciones (COM) Comunicaciones	2	C	M
E.19	Fuga de Información		Revelación de información crítica y/o sensible	Difusión de información a personal interno, contratistas, público en general o medios de comunicación que no necesitan conocerlo	Privilegios de Lectura, Escritura (Confidencialidad)	Datos / Información (SI) Servicios Infraestructura (SW) Aplicaciones (P) Personas	3	C	H
E.20	Vulnerabilidad de los Programas		Interrupción o daño de la aplicación o Servicio de información	Defectos de software que permiten a un atacante aprovechar una debilidad	Daños de Integridad y Disponibilidad	Datos / Información (SI) Servicios Infraestructura (SW) Aplicaciones (L) Instalaciones	3	C	H

**Anexo No. 22.** Formulario de Registro de Riesgos

**Nota:** A manera de muestra

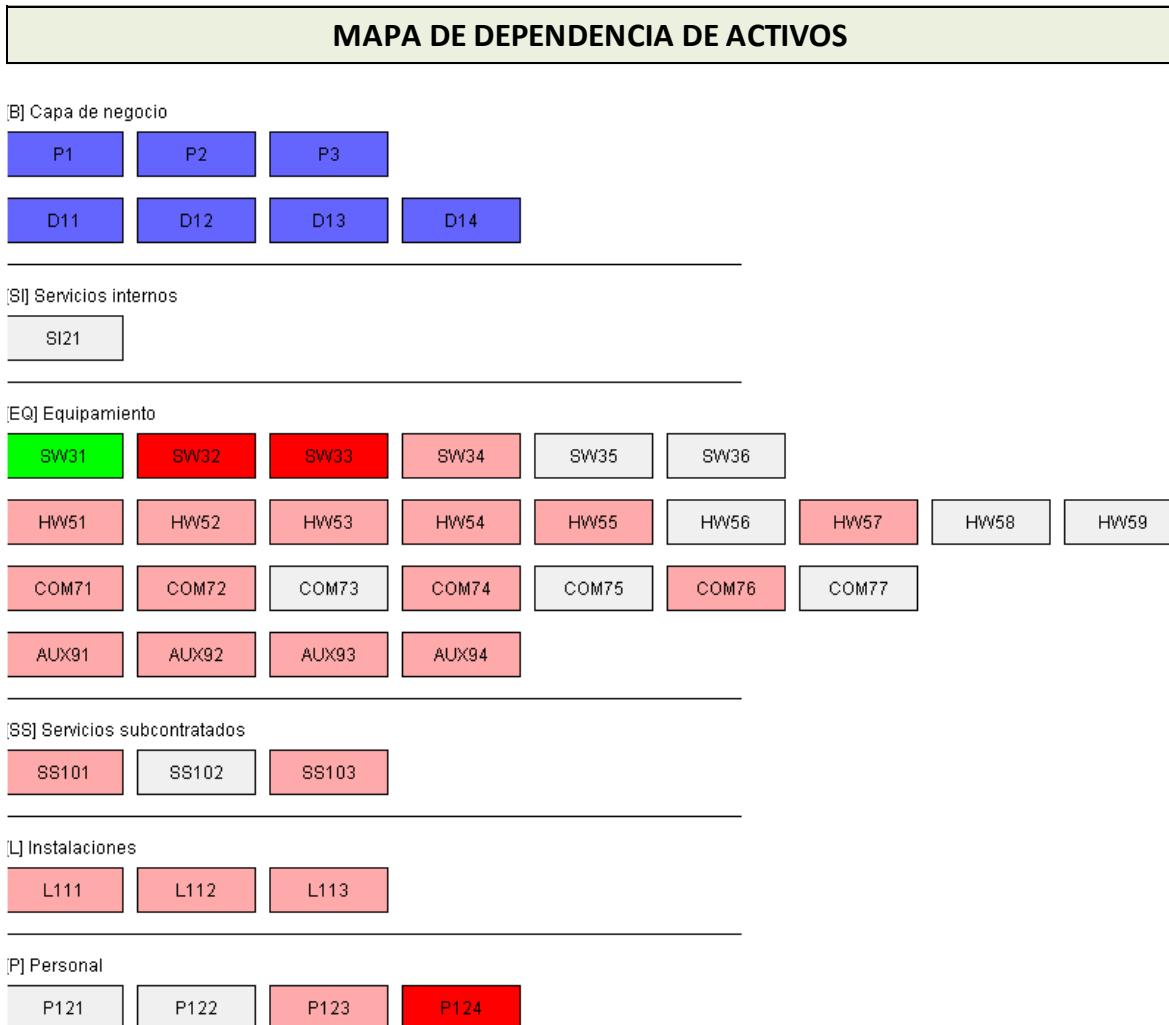
 <b>NACIONAL SEGUROS</b> <small>PATRIMONIALES Y FIANZAS S.A.</small>	<b>Formulario de Análisis de Riesgos</b>	F-785 Revisión 5 Agosto, 2018
--	--	-------------------------------------

<b>[SW] Aplicaciones (software)</b>	
<b>Código:</b>	SW31
<b>Nombre:</b>	Sistema de Aplicacion (ERP)
<b>Descripción:</b>	Sistemas esenciales de Planificación de Recursos Empresariales (ERP), tales como: Propio (eProperty, UponSoft, SSP Personal, UIF)
<b>Propietario:</b>	Nacional Seguros Patrimoniales y Fianzas S.A.
<b>Responsable:</b>	/ Gerente de Desarrollo de Software / TECorp

<b>Tipo (marque todos los adjetivos que procedan):</b>									
<b>[SW] Aplicaciones (Software)</b>									
<input checked="" type="checkbox"/> [prp] Desarrollo propio (in house) <input checked="" type="checkbox"/> [sub] Desarrollo a medida (subcontratado)									
<b>[std] estandar (Comercial)</b>									
<input type="checkbox"/> [browser] navegador web <input type="checkbox"/> [www] servidor de presentacion <input type="checkbox"/> [app] Servidor de aplicaciones <input type="checkbox"/> [email_client] cliente de Correo electronico <input type="checkbox"/> [email_server] Servidor de correo electronico <input type="checkbox"/> [directory] servidor de directorio <input type="checkbox"/> [file] servidor de archivos <input type="checkbox"/> [dbms] Sistema de gestion de Base de Datos <input type="checkbox"/> [tm] monitor transaccional <input type="checkbox"/> [office] Ofimatica <input type="checkbox"/> [av] Antivirus <input type="checkbox"/> [os] Sistema operativo <input type="checkbox"/> [ts] Servidor Terminal Server <input type="checkbox"/> [backup] Servicio de Backup <input checked="" type="checkbox"/> [other] Otros									
	<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="background-color: #c6e2ff;">Valor</th> <th style="background-color: #c6e2ff;">Dimensión</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">10</td> <td>Disponibilidad</td> </tr> <tr> <td style="text-align: center;">10</td> <td>Integridad</td> </tr> <tr> <td style="text-align: center;">5</td> <td>Confidencialidad</td> </tr> </tbody> </table>	Valor	Dimensión	10	Disponibilidad	10	Integridad	5	Confidencialidad
Valor	Dimensión								
10	Disponibilidad								
10	Integridad								
5	Confidencialidad								
<b>Coeficiente de Riesgo Calculado</b> <span style="font-size: 2em; font-weight: bold;">8.3</span>									

<b>Valoración</b>		
Dimensión	Valor	Justificación
[D] Disponibilidad	10	Asegurar que la información estará disponible cuando se requiera acceder a ella.
[I] Integridad	10	Garantía de la exactitud y completitud de la información
[C] Confidencialidad	5	Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso
[A] Autenticidad	0	Garantizar la autenticidad de los usuarios y de la información
[T] Trazabilidad	0	Garantizar el seguimiento y trazabilidad de los servicios y de los datos de una operación hasta el punto de partida

<b>Dependencias de activos inferiores (hijos)</b>			
<b>Activo:</b>	SW32 Motor de base de datos	<b>Grado:</b>	100%
<b>¿Por qué?:</b>	Es el sistema de gestión de base de Datos basado en SQL Server, necesario para acceder y manipular los datos		
<b>Activo:</b>	SW33 Servidor de Aplicaciones	<b>Grado:</b>	100%
<b>¿Por qué?:</b>	Es el entorno de publicación de aplicaciones basado en IIServer, necesario para acceder a las aplicaciones empresariales		
<b>Activo:</b>	P124 Soporte L2 (Administradores de infraestructura)	<b>Grado:</b>	10%
<b>¿Por qué?:</b>	Disponibilidad del personal de infraestructura		
<b>Activo:</b>		<b>Grado:</b>	
<b>¿Por qué?:</b>			



**Anexo No. 23.** Matriz de Riesgos con prioridad

**Nota:** A manera de muestra

Prioridad	ID Riesgo	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Impacto	Probabilidad	Evaluación	Riesgo Medido
1	③	Tormentas Eléctricas, Huracanes, Terremotos, Deslizamientos de Terreno, Frio Extremo, Calor Extremo	Posibilidad de que algún fenómeno natural cause daño a los recursos del sistema	Interrupción de Actividades (Disponibilidad)	4	4	16	Alto
2	①	Incendio	Posibilidad de que el fuego acabe con recursos del sistema	Interrupción de Actividades (Disponibilidad)	5	3	15	Alto
2	④	Explosiones, derrumbes, contaminación, sobrecarga, accidentes de trafico	Posibilidad de algún desastre industrial debido a la actividad humana	Interrupción de Actividades (Disponibilidad)	5	3	15	Alto
3	②	Inundaciones	Posibilidad de que el agua acabe con recursos del sistema	Interrupción de Actividades (Disponibilidad)	4	3	12	Medio
3	⑯	Fallo en Programas, Equipos de Computación	Fallas de equipos, mal funcionamiento del Software, saturación del S.O (Virus, Gusanos, Caballos de Troya, Spyware)	Daños de integridad, Disponibilidad por Infección de Malware	4	3	12	Medio
4	⑧	Interrupción Accidental, deliberada (agente externo/interno)	Posibilidad de Pérdida del Suministro de Energía	Interrupción de Actividades (Disponibilidad)	3	3	9	Medio
4	⑨	Exceso de Temperatura, humedad	Mala aclimatación, excediendo los márgenes de trabajo	Interrupción de Actividades (Disponibilidad)	3	3	9	Medio

Prioridad	ID Riesgo	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Impacto	Probabilidad	Evaluación	Riesgo Medido
4	⑯	Revelación de información crítica y/o sensible	Difusión de información a personal interno, contratistas, público en general o medios de comunicación que no necesitan conocerlo	Privilegios de Lectura, Escritura (Confidencialidad)	3	3	9	Medio
4	⑯	Interrupción o daño de la aplicación o Servicio de información	Defectos de software que permiten a un atacante aprovechar una debilidad	Daños de Integridad y Disponibilidad	3	3	9	Medio
5	⑩	Destrucción física o Interrupción Accidental, deliberada (agente externo/interno)	Incapacidad para atender al tráfico presente	Cese de la capacidad de transmitir datos (Disponibilidad)	2	4	8	Medio
6	⑤	Vibraciones, Polvo, Suciedad	Posibilidad de que la contaminación Mecánica dañe los recursos del sistema	Interrupción de Actividades (Disponibilidad)	2	3	6	Bajo
6	⑦	Fallo en Programas, Equipos y Equipamiento Auxiliar	Defecto de origen o de funcionamiento	Interrupción de Actividades (Disponibilidad)	2	3	6	Bajo
6	⑪	Falta de suministros papel, tóner, refrigerante, combustible	Otros servicios o recursos de los que depende la operación de los equipos	Interrupción de Actividades (Disponibilidad)	2	3	6	Bajo
6	⑬	Equivocaciones, descuidos, falta de capacitación	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Daños de integridad y (Disponibilidad)	2	3	6	Bajo
6	⑭	Equivocaciones, descuidos, falta de capacitación	Equivocaciones de personas con responsabilidades de instalación y operación	Daños de integridad, Disponibilidad, Confidencialidad, Autenticidad	3	2	6	Bajo

Prioridad	ID Riesgo	Riesgo del Negocio	Descripción del Riesgo	Riesgo Tecnológico	Impacto	Probabilidad	Evaluación	Riesgo Medido
6	⑯	Demora en la entrega por error de enrutamiento	Incapacidad para enrutar el tráfico de información	Cese de la capacidad de transmitir datos (Disponibilidad)	2	3	6	Bajo
7	⑯	Interferencias de radio, campos magnéticos, luz ultravioleta	Posibilidad de que la contaminación electromagnética dañe los recursos del sistema	Interrupción de Actividades (Disponibilidad)	2	2	4	Bajo
7	⑯	datos o registros de configuración erróneos	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador:	Privilegios de Acceso, Registros incompletos, Monitoreo, encaminamiento	4	1	4	Bajo
7	⑯	Interrupción o demora del Servicio	Ausencia accidental del puesto de trabajo por enfermedad, alteraciones del orden público, guerra bacteriológica	Cese de la capacidad de atender los procesos (Disponibilidad)	2	2	4	Bajo
8	⑯	Destrucción física o daño de medios de almacenamientos	Destrucción de medios como consecuencia del paso del tiempo	Degradación del medio (Integridad)	1	2	2	Bajo

Fuente: Elaboración Propia, 2019.

**Anexo No. 24.** Plan de Tratamiento de Riesgos

**Nota:** A manera de muestra

Prioridad	ID Riesgo	Amenazas	Riesgo del Negocio	Riesgo Medido	Estado	Responsable	Evento Disparador	Opción de Tratamiento	Tipo de Control	Estrategia de Respuesta
1	③	Desastres Naturales	Tormentas Eléctricas, Huracanes, Terremotos, Deslizamientos de Terreno, Frio Extremo, Calor Extremo	Alto	Activo	Alta Dirección	Falla en la Continuidad de las operaciones	Compartir el Riesgo (Transferir)	4. Correctivo	Seguro Todo Riesgo
2	①	Fuego	Incendio	Alto	Activo	Alta Dirección	Falla en la Continuidad de las operaciones	Compartir el Riesgo (Transferir)	4. Correctivo	Seguro Todo Riesgo
2	④	Desastres Industriales	Explosiones, derrumbes, contaminación, sobrecarga, accidentes de tráfico	Alto	Activo	Alta Dirección	Falla en la Continuidad de las operaciones	Compartir el Riesgo (Transferir)	4. Correctivo	Seguro Todo Riesgo
3	②	Daños por Agua	Inundaciones	Medio	Activo	Servicios Generales	Falla en la Continuidad de las operaciones	Compartir el Riesgo (Transferir)	4. Correctivo	Seguro Todo Riesgo
3	⑯	Difusión de Software Dañino	Fallo en Programas, Equipos de Computación	Medio	Activo	Gerente de TI y Seguridad	Incidente de Seguridad	Modificar Riesgo (Reducir)	3. Detectivo	Antivirus Corporativo
4	⑧	Corte del Suministro Eléctrico	Interrupción Accidental, deliberada (agente externo/interno)	Medio	Activo	Servicios Generales	Caída de Servidores y/o Equipamiento	Modificar Riesgo (Reducir)	4. Correctivo	Sistema de Transferencia de energía (UPS, Generador)

Prioridad	ID Riesgo	Amenazas	Riesgo del Negocio	Riesgo Medido	Estado	Responsable	Evento Disparador	Opción de Tratamiento	Tipo de Control	Estrategia de Respuesta
4	⑨	Condiciones inadecuadas de temperatura/humedad	Exceso de Temperatura, humedad	Medio	Activo	Jefe de IT	Reinicio de Servidores y/o Equipamiento	Modificar Riesgo (Reducir)	3. Detectivo	Sistema de Monitoreo de temperatura y Humedad
4	⑯	Fuga de Información	Revelación de información crítica y/o sensible	Medio	Activo	Gerente de TI y Seguridad	Exposición de información crítica o sensible	Modificar Riesgo (Reducir)	5. Compensatorio	Herramientas Visibilidad del Tráfico de Datos (DLP, SIEM)
4	⑯	Vulnerabilidad de los Programas	Interrupción o daño de la aplicación o Servicio de información	Medio	Activo	Gerente de Desarrollo	Incidente de Seguridad	Modificar Riesgo (Reducir)	5. Compensatorio	Registros de eventos de la sesión
5	⑩	Fallo en servicios de comunicaciones	Destrucción física o Interrupción Accidental, deliberada (agente externo/interno)	Medio	Activo	Adm. de Telecom	Perdida de Servicios con agencias Locales, Nacionales	Modificar Riesgo (Reducir)	5. Compensatorio	Balanceador ADC (App delivery Controller)
6	⑤	Contaminación Mecánica	Vibraciones, Polvo, Suciedad	Bajo	Inactivo	Servicios Generales	Falla en la Continuidad de las operaciones	Aceptar el Riesgo	2. Preventivo	Ninguna, el nivel de riesgo es bajo
6	⑦	Avería de origen físico o lógico	Fallo en Programas, Equipos y Equipamiento Auxiliar	Bajo	Activo	Jefe de IT	Falla en la ejecución del Plan de Contingencia	Aceptar el Riesgo	2. Preventivo	Ninguna, el nivel de riesgo es bajo

Prioridad	ID Riesgo	Amenazas	Riesgo del Negocio	Riesgo Medido	Estado	Responsable	Evento Disparador	Opción de Tratamiento	Tipo de Control	Estrategia de Respuesta
6	⑪	Interrupción de otros servicios o suministros esenciales	Falta de suministros papel, tóner, refrigerante, combustible	Bajo	Inactivo	Gerente de Operaciones	Falla en la Continuidad de las operaciones	Aceptar el Riesgo	5. Compensatorio	Ninguna, el nivel de riesgo es bajo
6	⑬	Errores de Usuario	Equivocaciones, descuidos, falta de capacitación	Bajo	Activo	Usuario	Errores de entrada de datos	Aceptar el Riesgo	5. Compensatorio	Ninguna, el nivel de riesgo es bajo
6	⑭	Errores del Administrador	Equivocaciones, descuidos, falta de capacitación	Bajo	Activo	Gerente de TI y Seguridad	Violación de PNPs	Aceptar el Riesgo	4. Correctivo	Ninguna, el nivel de riesgo es bajo
6	⑯	Errores de re-encaminamiento	Demora en la entrega por error de enrutamiento	Bajo	Activo	Adm. de Telecom	Errores de entrega de Datos	Aceptar el Riesgo	2. Preventivo	Ninguna, el nivel de riesgo es bajo
7	⑯	Contaminación Electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta	Bajo	Inactivo	Gerente General	Fuente de contaminación cercana a las instalaciones	Aceptar el Riesgo	3. Detectivo	Ninguna, el nivel de riesgo es bajo
7	⑮	Errores de Configuración	datos o registros de configuración erróneos	Bajo	Activo	Adm. de Bases de Datos	Falla en cálculos del sistema	Aceptar el Riesgo	4. Correctivo	Ninguna, el nivel de riesgo es bajo

Prioridad	ID Riesgo	Amenazas	Riesgo del Negocio	Riesgo Medido	Estado	Responsable	Evento Disparador	Opción de Tratamiento	Tipo de Control	Estrategia de Respuesta
7	②0	Indisponibilidad del Personal	Interrupción o demora del Servicio	Bajo	Activo	Sub Gerente Corporativo de RRHH	Bajo rendimiento del Proceso o Servicio	Aceptar el Riesgo	2. Preventivo	Ninguna, el nivel de riesgo es bajo
8	⑫	Degradación de soportes de Almacenamiento	destrucción física o daño de medios de almacenamientos	Bajo	Activo	Gerente de TI y Seguridad	Falla en recuperación de información	Aceptar el Riesgo	4. Correctivo	Ninguna, el nivel de riesgo es bajo

**Fuente:** Elaboración Propia, 2019.

**Anexo No. 25. FRM de Análisis de Elementos de Servicios Críticos para el BIA**

**Nota:** A manera de muestra

<b>FRM de Análisis de Elementos de Servicios Críticos para el Análisis de Impacto al negocio (BIA)</b>		<b>F-553 Revisión x Valido desde xxx, xxxx</b>																														
<b>ANALISIS DE IMPACTO AL NEGOCIO (BIA)</b>																																
<b>1</b>	<b>1. INFORMACIÓN GENERAL DEL ELEMENTO DE CONFIGURACION DE SERVICIO</b>																															
1.1	<b>DENOMINACIÓN DEL ELEMENTO DE SERVICIO:</b>	SI21 - Infraestructura de Colaboracion																														
		Nuevo Servicio Crítico: <input checked="" type="checkbox"/> No																														
1.2	<b>Principales aplicaciones soportadas por el servicio</b>	Controlador de Dominio, Servicio DNS, DHCP, Certificate Server, FileServer, Servidor de correos Exchange, Servidor de Mensajes Lync Server, Servidor proxy/Firewall TMG, Antivirus, AntiSpam, WSUS, Tserver.																														
1.3	<b>Descripción, Comentarios y Observaciones acerca del Elemento de Servicio Crítico:</b>	Los usuarios de Nacional Seguros Vida y Salud requieren acceso permanente a los Servicios de colaboración de la infraestructura tecnológica para compartir información, enviar y recibir correo electrónicos y mensajes internos. Es importante planear periódicamente la capacidad de crecimiento y el monitoreo continuo de la disponibilidad de los servicios, además de garantizar si se respaldó la Maquina Virtual del Servicio.																														
1.4	<b>Fecha de la última actualización</b>	Actualizado a: Enero 2019																														
1.5	<b>Costo Comercial \$us.</b>	24,000.00																														
		Criticidad actual <input checked="" type="checkbox"/> Muy Alta																														
1.6	<b>Unidad de Negocio</b>	Tecnología Corporativa																														
1.7	<b>Responsable en la Cuenta</b>	Gerente de TI y Seguridad Informática - TECorp																														
1.8	<b>Gestor del Servicio</b>	Jefe de IT / Adm. de Servidores TECorp																														
1.9	<b>Responsable Usuario</b>	Gerente Nacional de Operaciones NSVS																														
1.10	<b>¿Existen mecanismos para realizar la actividad de negocio o soportar el procesamiento con sistemas reducidos o alternos?</b>	PARCIAL																														
Si la respuesta anterior es afirmativa.																																
1.11	<b>¿Cuánto tiempo se puede trabajar utilizando los procedimientos alternativos o sistemas reducidos?</b>	Tiempo Estimado: (MTD) <input checked="" type="checkbox"/> 8 Horas																														
1.12	<b>Relación de ubicaciones (Sucursales o Agencias de trabajo) donde se encuentran las personas que realizan la función de negocio</b>	<table border="1"> <thead> <tr> <th>Clientes o Sucursales</th> <th>Nº de Usuarios dependientes del Servicio</th> <th>Nº de Usuarios Críticos</th> </tr> </thead> <tbody> <tr> <td>SCZ - Sitio Principal (Paraguá)</td> <td>&gt; 100</td> <td>25 a 50</td> </tr> <tr> <td>SCZ - Regional (Bahiti)</td> <td>&gt; 100</td> <td>25 a 50</td> </tr> <tr> <td>SCZ - Agencia Regional (Montero)</td> <td>1 a 10</td> <td>1 a 10</td> </tr> <tr> <td>SCZ - Sitio Alterno (Parque Industrial)</td> <td>25 a 50</td> <td>10 a 25</td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	Clientes o Sucursales	Nº de Usuarios dependientes del Servicio	Nº de Usuarios Críticos	SCZ - Sitio Principal (Paraguá)	> 100	25 a 50	SCZ - Regional (Bahiti)	> 100	25 a 50	SCZ - Agencia Regional (Montero)	1 a 10	1 a 10	SCZ - Sitio Alterno (Parque Industrial)	25 a 50	10 a 25															
Clientes o Sucursales	Nº de Usuarios dependientes del Servicio	Nº de Usuarios Críticos																														
SCZ - Sitio Principal (Paraguá)	> 100	25 a 50																														
SCZ - Regional (Bahiti)	> 100	25 a 50																														
SCZ - Agencia Regional (Montero)	1 a 10	1 a 10																														
SCZ - Sitio Alterno (Parque Industrial)	25 a 50	10 a 25																														

2. DISPONIBILIDAD DEL ELEMENTO DE SERVICIO																																																	
2.1 Acuerdo de Nivel de Servicio existente	SI																																																
	<table border="1"> <thead> <tr> <th colspan="2">Acuerdo Vigente</th> </tr> </thead> <tbody> <tr> <td>Calendario</td> <td>24x7 (365)</td> </tr> <tr> <td>Disponibilidad (%)</td> <td>0.99 (8 hr/mes, 2 hr/sem, 0.5 hr/día)</td> </tr> <tr> <td>Tiempo de Respuesta</td> <td>Critica 4 Hr, Alta 8 Hr, Media 24 Hr, Baja 48 Hr</td> </tr> </tbody> </table>	Acuerdo Vigente		Calendario	24x7 (365)	Disponibilidad (%)	0.99 (8 hr/mes, 2 hr/sem, 0.5 hr/día)	Tiempo de Respuesta	Critica 4 Hr, Alta 8 Hr, Media 24 Hr, Baja 48 Hr																																								
Acuerdo Vigente																																																	
Calendario	24x7 (365)																																																
Disponibilidad (%)	0.99 (8 hr/mes, 2 hr/sem, 0.5 hr/día)																																																
Tiempo de Respuesta	Critica 4 Hr, Alta 8 Hr, Media 24 Hr, Baja 48 Hr																																																
3. PARÁMETROS DE RECUPERACIÓN																																																	
3.1 ¿En cuánto tiempo se debe disponer de un nivel mínimo de prestación del ELEMENTO DE SERVICIO? (WR)	Tiempo estimado: (WR) 4 Horas																																																
3.2 ¿En cuánto tiempo deben estar recuperadas totalmente las prestaciones del ELEMENTO DE SERVICIO? (RTO)	Tiempo estimado: (RTO) 8 Horas																																																
3.3 ¿Cuánta es la pérdida de información puede soportar el negocio? (RPO)	Tiempo estimado: (RPO) > de 24 Horas																																																
3.4 Indicar el número mínimo imprescindible de usuarios conectados al mismo tiempo al Elemento de Servicio en situación de servicio degradado	85																																																
3.5 ¿Qué porcentaje sobre el total de usuarios son los anteriores?	45%																																																
4. NIVELES DE IMPACTO																																																	
<a href="#">Visualizar Tabla de Impactos</a> <a href="#">Visualizar Tabla de Crítica</a>																																																	
4.1 Impacto de parada de actividad de negocio	<table border="1"> <thead> <tr> <th></th> <th>1 HORA</th> <th>1 DIA</th> <th>1 SEMANA</th> <th>1 MES</th> <th>TOTAL (S)</th> </tr> </thead> <tbody> <tr> <td>Impacto Financiero (1-5)</td> <td>1</td> <td>3</td> <td>4</td> <td>5</td> <td><b>13</b></td> </tr> <tr> <td>Impacto Operativo (1-5)</td> <td>1</td> <td>3</td> <td>4</td> <td>5</td> <td><b>13</b></td> </tr> <tr> <td>Impacto Imagen, Reputación, Marca (1-5)</td> <td>1</td> <td>3</td> <td>4</td> <td>5</td> <td><b>13</b></td> </tr> <tr> <td>Impacto Normativo, Legal (1-5)</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td><b>10</b></td> </tr> <tr> <td>Impacto Laboral, Talentos Humanos (1-5)</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td><b>10</b></td> </tr> <tr> <td><b>TOTAL (Σ)</b></td> <td><b>5</b></td> <td><b>13</b></td> <td><b>18</b></td> <td><b>23</b></td> <td></td> </tr> <tr> <td></td> <td>Muy Bajo</td> <td>Medio</td> <td>Grave</td> <td>Muy Grave</td> <td></td> </tr> </tbody> </table>		1 HORA	1 DIA	1 SEMANA	1 MES	TOTAL (S)	Impacto Financiero (1-5)	1	3	4	5	<b>13</b>	Impacto Operativo (1-5)	1	3	4	5	<b>13</b>	Impacto Imagen, Reputación, Marca (1-5)	1	3	4	5	<b>13</b>	Impacto Normativo, Legal (1-5)	1	2	3	4	<b>10</b>	Impacto Laboral, Talentos Humanos (1-5)	1	2	3	4	<b>10</b>	<b>TOTAL (Σ)</b>	<b>5</b>	<b>13</b>	<b>18</b>	<b>23</b>			Muy Bajo	Medio	Grave	Muy Grave	
	1 HORA	1 DIA	1 SEMANA	1 MES	TOTAL (S)																																												
Impacto Financiero (1-5)	1	3	4	5	<b>13</b>																																												
Impacto Operativo (1-5)	1	3	4	5	<b>13</b>																																												
Impacto Imagen, Reputación, Marca (1-5)	1	3	4	5	<b>13</b>																																												
Impacto Normativo, Legal (1-5)	1	2	3	4	<b>10</b>																																												
Impacto Laboral, Talentos Humanos (1-5)	1	2	3	4	<b>10</b>																																												
<b>TOTAL (Σ)</b>	<b>5</b>	<b>13</b>	<b>18</b>	<b>23</b>																																													
	Muy Bajo	Medio	Grave	Muy Grave																																													
<p>Resumen x Período de Impacto</p> <table border="1"> <thead> <tr> <th>Período</th> <th>Impacto</th> </tr> </thead> <tbody> <tr> <td>1 Hora</td> <td>5</td> </tr> <tr> <td>1 Dia</td> <td>13</td> </tr> <tr> <td>1 Semana</td> <td>18</td> </tr> <tr> <td>1 Mes</td> <td>23</td> </tr> </tbody> </table>		Período	Impacto	1 Hora	5	1 Dia	13	1 Semana	18	1 Mes	23																																						
Período	Impacto																																																
1 Hora	5																																																
1 Dia	13																																																
1 Semana	18																																																
1 Mes	23																																																
<p>Resumen x Tipo de Actividad de Negocio</p> <table border="1"> <thead> <tr> <th>Actividad</th> <th>Impacto</th> </tr> </thead> <tbody> <tr> <td>FIN</td> <td>13</td> </tr> <tr> <td>OPE</td> <td>13</td> </tr> <tr> <td>IMA</td> <td>13</td> </tr> <tr> <td>NOR</td> <td>10</td> </tr> <tr> <td>HUM</td> <td>10</td> </tr> </tbody> </table>		Actividad	Impacto	FIN	13	OPE	13	IMA	13	NOR	10	HUM	10																																				
Actividad	Impacto																																																
FIN	13																																																
OPE	13																																																
IMA	13																																																
NOR	10																																																
HUM	10																																																

5	5. INTERRUPCIÓN DEL SERVICIO			
	<a href="#">Visualizar Tabla de Impactos</a>			
5.1	<b>Legislación:</b> ¿Existe alguna legislación que no sería cumplida por falta de servicio? ¿Cuál?	Acuerdos de niveles de servicio y Contratos, ISO 9001		
5.2	Relación de otros Elementos de Servicio imprescindibles para la realización de la actividad de negocio (Interfaces y necesidades de información de otros sistemas)	Sistemas operativos de Red, Suite Ofimática en el usuario		
5.3	<b>Proveedores:</b> ¿Existe algún contrato y/o acuerdo con proveedores de servicio? Indicar las dependencias de proveedores externos para brindar el servicio	TECorp L1, Dima L2		
5.4	¿Existe alguna posibilidad, de recuperar los datos previamente introducidos en el sistema informático?	PARCIAL		
5.5	En caso de respuesta afirmativa a la pregunta anterior ¿qué mecanismo se utilizaría para recuperarlos ? (Breve descripción)	Cache del Usuario		
5.6	Si existe mecanismo alternativo de recuperación (RPO) ¿hasta dónde se podrían recuperar los datos introducidos antes de un incidente? (todos los datos / hasta las últimas X)	1 semana		
5.7	¿Hay algún periodo de tiempo en el que la criticidad del Elemento de Servicio sea mayor? (Períodos de tiempo, y/o fechas)	del 1-5 y del 25-30 de cada mes		
6	6. LINEA DE TENDENCIA EN LOS SIGUIENTES 12 MESES			
6.1	La carga de trabajo del Elemento de Servicio	<input checked="" type="radio"/> Aumentará	<input type="radio"/> Se mantendrá	<input type="radio"/> Disminuirá
6.2	El número de usuarios	<input checked="" type="radio"/> Aumentará	<input type="radio"/> Se mantendrá	<input type="radio"/> Disminuirá
6.3	El número de transacciones diarias	<input checked="" type="radio"/> Aumentará	<input type="radio"/> Se mantendrá	<input type="radio"/> Disminuirá

**Anexo No. 26. Cotización Enlace Inter-Sitio con Fibra Oscura 40Gbps/80Gbps**

Señor:

Ing. Alexis Garcia Sandoval  
Gerente de Proyectos y Seguridad  
TECNOLOGIA CORPORTAIVA

Presente:

Ref.: Propuesta de servicio de Fibra óptica oscura  
(Hilos ópticos).

De mi consideración:

Por medio de la presente nos es grato presentar a usted nuestra propuesta de servicio Fibra oscura.

Lugar de Enlace: Ciudad de Santa Cruz

**Alquiler 2 hilos ópticos**

Nº	Descripción del Enlace	Tipo de Enlace	Cantidad	Costo Instalación	Precio Unitario en Bs	Costo Total Mensual En Bs
1	<b>Desde:</b> Oficina Tecorp, Paragua Avenida Segundo Anillo casi Paragua, UV19, Distrito 3, Manzana P01 Sección 6 Barrio Gualberto Villarroel. <b>Hasta:</b> Oficina Tecorp, Z. Parque Industrial, Manzana 17	Fibra oscura (Hilos ópticos)	2	2000,00	1500,00	3000,00

**Alquiler 4 Hilos ópticos**

Nº	Descripción del Enlace	Tipo de Enlace	Cantidad	Costo Instalación	Precio Unitario en Bs	Costo Total Mensual En Bs
1	<b>Desde:</b> Oficina Tecorp, Paragua Avenida Segundo Anillo casi Paragua, UV19, Distrito 3, Manzana P01 Sección 6 Barrio Gualberto Villarroel. <b>Hasta:</b> Oficina Tecorp, Z. Parque Industrial, Manzana 17	Fibra oscura (Hilos ópticos)	4	2000,00	1400,00	5600,00

**Especificaciones técnicas:**

1. El Enlace tendrá las características de conexión fibra oscura.
2. **Instalación cableado:** La instalación del cableado es Aéreo, murales y ductos.
3. **Ancho de Banda:** Para esta conexión se tendrá un canal con capacidad de trasportar un ancho de banda que alcance hasta 40G.
4. **El tipo de conector final en ambos extremos** será de tipo LC/PC

## Anexo No. 27. Acta de entrega y aceptación del Proyecto BCM



NACIONAL  
SEGUROS

**PLAN DE DIRECCION DEL PROYECTO  
DE GESTION DE CONTINUIDAD DEL NEGOCIO  
(BCM)  
PL-404**

**RESUMEN DE VERSIONES**

Nº de Versión	Fecha de emisión:	Motivo de la revisión	Descripción de las modificaciones
1	Noviembre - 2015	Emitido inicial.	Versión original

Página 1 de 75

Elaborado por:  Alexis Garcia Gerente de TI y Seguridad Fecha: 17-II-2015	Validado por:  Marco Antonio Lopez Gerente Nacional de Operaciones NSVS Fecha: 17-II-2015	Validado por:  Julio Cesar Basa Gerente Nacional de Operaciones NSPI Fecha: 17-II-2015
Aprobado por:  Javier Camacho Gerente General de TECORP Fecha: 17-II-2015	Aprobado por:  Jorge Hugo Parada Gerente General de NSPF Fecha: 17-II-2015	Aprobado por:  Alvaro Toledo Gerente General de NSVS Fecha: 17-II-2015

Este documento es controlado por el departamento de Calidad, su modificación se encuentra regulada según procedimientos internos y su vigencia es válida al momento de su aprobación.

	NACIONAL SEGUROS	PL - 404 PLAN DE DIRECCION DEL PROYECTO DE GESTION DE CONTINUIDAD DEL NEGOCIO (BCM)	V: 01/ Noviembre - 2016 Uso Confidencial
			Página 2 de 75

**Acta de Entrega y Aceptación**  
**“Plan de Dirección del Proyecto de Gestión de Continuidad**  
**Del Negocio”**

A través del presente documento, se da conformidad al contenido y para su cumplimiento en cuanto a los procesos esenciales evaluados para la gestión de la continuidad del negocio, considerando el análisis de riesgo, análisis de impacto al negocio y la selección de las estrategias adecuadas de recuperación para la continuidad del negocio.

Lic. Alvaro Toledo Peñaranda  
 Gerente General  
*Nacional Seguros Vida y Salud S.A.*

Lic. Marco Antonio Lopez  
 Gerente Nacional de Operaciones  
*Nacional Seguros Vida y Salud S.A.*

Lic. Jorge Hugo Parada  
 Gerente General  
*Nacional Seguros Patrimoniales y  
 Fianzas S.A.*

Lic. Julio Cesar Saa  
 Gerente Nacional de Operaciones  
*Nacional Seguros Patrimoniales y  
 Fianzas S.A.*

Ing. Javier Camacho Miserendino  
 Gerente General  
*Tecnología Corporativa S.A.*

Ing. Alexis García Sandoval  
 Gerente TI y Seguridad  
*Tecnología Corporativa S.A.*

**Anexo No. 28.** Resultados de la Prueba del Plan de Continuidad del Negocio

PRUEBA DEL PLAN DE CONTINUIDAD (SITIO ALTERNO)												
Hora de Inicio:	09:38											
Hora de Finalización:	11:36						01:58					
<b>1. Configuración Networking:</b>												
SW-A	Port	Servi	6 VLAN	24 Acceso		09:42	09:49					
SW-A	Port	usuario	8 VLAN	1 Trunk								
SW-B	Port		6 VLAN	24 Acceso								
SW-B	Port		8 VLAN	1 Trunk								
<b>Equipos Compatibles</b>		PC GESPENHAIN			PC EAYALA							
configuracion ip	172.16.24.201	P E	172.16.24.150	DNS 192.168.2.25								
<b>2. Prueba de Conexión de PC al Blade:</b>												
Test PC a vCenter	Resultado	172.16.24.133	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
Test PC al Blade1	Resultado	172.16.24.134	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
Test PC al Blade2	Resultado	172.16.24.135	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
Test PC al Blade3	Resultado	172.16.24.136	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
Test PC al Blade4	Resultado	172.16.24.142	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
Test PC al Blade5	Resultado	172.16.24.143	VLAN	24 Resultado Esperado	<input checked="" type="checkbox"/>							
<b>3. Ingreso al vCenter:</b>					Inicio	Fin						
Ingresar al vCenter	HTML5	<a href="https://vcenter02">https://vcenter02</a>			09:57	11:26	01:29					
		Usuario	<a href="https://172.16.24.133">https://172.16.24.133</a>									
		Admi	Usuario Permitido Administrator@vsphere.local N@cion@l2016*+									
Para acceder a vSphere, Inicie sesión en:		VR VM Ware Replication No trae la opción VR										
<a href="#">vSphere Web Client (Flash)</a>												
<a href="#">vSphere Client (HTML5): funcionalidad parcial</a>												
<a href="https://vcenter02/vsphere-client/?locale=en_US">https://vcenter02/vsphere-client/?locale=en_US</a>												

**Levantar la Replica**

Servidor	IP	Orden	BL	Activar Red	revisar servicios
1 ARES	192.168.2.3	2	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 EP01	172.16.14.111	3	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3 EP02	172.16.14.119	4	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4 EVEREST	192.168.2.4	5	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5 FILESERVER	192.168.3.131	6	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6 GSUITE-NSP	172.16.14.140	7	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7 RADIUS	192.168.2.228	8	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8 SC01SR3PAR	192.168.2.170	9	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9 sc01srac01	192.168.3.70	10	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10 sc01srac02	172.16.14.106	11	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11 SC01SRAPP2	172.16.14.107	12	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12 SC01SRAPP3	172.16.14.72	13	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13 SC01SRAPP4	172.16.14.112	14	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14 SC01SRAPP5	192.168.122.1	15	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15 SC01SRAPP6	172.16.14.132	16	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16 SC01SRAPP7		17	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17 SC01SRAPPGNV02	10.192.168.11	18	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18 SC01SRAPPGNV03	10.192.168.20	19	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19 SC01SRAPPGNV05	10.192.168.23	20	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20 SC01SRAPPGNV07	10.192.168.25	21	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21 SC01SRAPPGNV08		22	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22 SC01SRAPPLT01	172.16.14.104	23	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23 SC01SRAPPNV01	192.168.2.175	24	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24 SC01SRAPPNV02	192.168.2.184	25	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25 SC01SRAPPNV03	192.168.3.2	26	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26 SC01SRAPPNV04	192.168.2.112	27	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
27 SC01SRAPPNV05	172.16.14.116	28	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
28 SC01SRAPPNV06	172.16.14.127	29	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
29 SC01SRAPPNV07	172.16.14.128	30	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
30 SC01SRAV01	172.16.14.101	31	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
31 SC01SRAV02	172.16.14.102	32	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
32 SC01SRAV04	172.16.14.100	33	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
33 SC01SRB05	172.16.14.71	34	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
34 SC01SRB06	172.16.14.81	35	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
35 SC01SRBDODISTNV1	192.168.2.108	36	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
36 SC01SRBDODISTNV2	192.168.2.169	37	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
37 SC01SRBOLT01	192.168.2.2	38	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
38 SC01SRBOLT02	172.16.14.124	39	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
39 SC01SRBNV01	10.192.168.21	40	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
40 SC01SRBNV02	10.192.168.15	41	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
41 SC01SRBNV03	172.16.14.153	42	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

42 SC01SRBDNV04	10.192.168.28	43	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
43 SC01SRBDNV05	10.192.168.26	44	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
44 SC01SRBDOR0LT1	172.16.14.65	45	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
45 SC01SRBDOR0LT2	172.16.14.67	46	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
46 SC01SRBDOR0NV01	172.16.14.63	47	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
47 SC01SRB01	172.16.14.118	48	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
48 SC01SRB02	172.16.14.114	49	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
49 SC01SRB03	172.16.14.115	50	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
50 SC01SRBK01	192.168.3.7	51	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
51 SC01SRDSD	192.168.3.65	52	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
52 SC01SRDV01	192.168.2.250	53	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
53 sc01srdrsync	192.168.2.24	54	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
54 SC01SREG	192.168.2.21	55	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
55 SC01SREL01	172.16.14.21	56	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
56 SC01SREL02	172.16.14.22	57	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
57 SC01SREL03	172.16.14.29	58	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
58 SC01SREL1	172.16.14.54	59	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
59 SC01SREL2	172.16.14.56	60	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
60 SC01SREL3	172.16.14.57	61	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
61 SC01SRE501	172.16.14.31	62	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
62 SC01SRE502	172.16.14.32	63	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
63 SC01SRE503	172.16.14.33	64	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
64 SC01SRESPIA	172.16.14.68	65	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
65 SC01SREXHY2	192.168.3.9	66	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
66 SC01SREFE02	172.16.14.13	67	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
67 SC01SRFS02	192.168.2.1	68	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
68 SC01SRIS501\vtm-b]	192.168.3.38	69	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
69 SC01SRIB0S01	192.168.3.120	70	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
70 SC01SRIB0S02	192.168.2.138	71	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
71 SC01SRIB0S03	172.16.14.55	72	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
72 SC01SRMBX01	172.16.14.24	73	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
73 SC01SRMBX02	172.16.14.25	74	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
74 SC01SRMNT01	192.168.2.140	75	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
75 SC01SRMNTD2	172.16.14.109	76	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
76 SC01SRNLB01		77	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
77 SC01SRNNVAPP02	192.168.2.121	78	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
78 SC01SR00002	172.16.14.64	79	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
79 SC01SRPDC	192.168.2.14	80	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
80 SC01SRPHIP03	172.16.14.123				

81	SC01SRPX02	172.16.14.16	81	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
82	SC01SRPX03	172.16.14.15	82	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
83	SC01SRSP01	192.168.2.71	83	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
84	SC01SRSP02	192.168.2.72	84	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
85	SC01SRTB01	172.16.14.99	85	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
86	SC01SRTK01	172.16.14.117	86	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
87	SC01SRTMG	192.168.2.20	87	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
88	SC01SRSTS1	192.168.2.70	88	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
89	SC01SRUPON	192.168.2.141	89	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
90	SC01SRVR01	172.16.24.250	90	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
91	SC01SRWEB	192.168.3.8	91	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
92	SC01SRWEB2	172.16.14.133	92	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
93	SC01SRPHP01	172.16.14.59	93	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
94	SR5TS01		94	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
95	SR5TS02		95	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
96	SOLARWINDS BD	172.16.14.82	96	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
97	SOLARWINDSORION	172.16.14.69	97	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
98	THOR	192.168.2.11	98	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
99	TITAN	172.16.14.53	99	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
100	VERITAS	172.16.14.122	100	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
101	VCENTER01	172.16.24.39	101	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Nombre Ejecutor

German Espenhain

Firma



Fecha

21/12/18

**TECORP**  
TECNOLOGIA CORPORATIVA  
German Espenhain Chávez  
JEFE DE IT

Nombre Ejecutor

Eduar Sosa

Firma



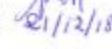
Fecha

21/12/18

Nombre Veedor

Freddy Aparicio

Firma



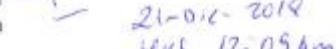
Fecha

21/12/18

Nombre Aprobador

Alexis Gómez

Firma

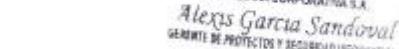


Fecha

21-01-2019  
Hrs 12:09 pm

**TECORP**  
TECNOLOGIA CORPORATIVA S.A.

Alexis García Sandoval  
GERENTE DE PROTECCION Y SEGURIDAD INFORMATICA



**Anexo No. 29.** Procesamiento estadístico con la corrección de Yates

GUIA DE OBSERVACIÓN		entrada ( <i>pre-test</i> )				Salida ( <i>post-test</i> )				$\alpha$	0.01	99.0%
CRITERIOS DE OBSERVACIÓN		S	GM	AM	N	S	GM	AM	N	GL	1	6.63
		80-	60-	10-		60-	10-					
		100%	79	59	<10%	80-100%	79	59	<10%			
<b>DIMENSIÓN - Evaluación</b>												
I	Interrupciones o incidentes mayores en lo últimos 5 años que han afectado los procesos críticos del negocio	1.5.1			50		70			= 34.81	0.97	Si
J	Tiempo Objetivo de Recuperación como meta Corporativa	2.1.1			30		60			= 66.11	0.99	Si
K	Resultados de la última Prueba realizada al BCM	2.1.2			25		50			= 82.51	0.99	Si
<b>DIMENSIÓN - Política</b>												
L	La dirección está comprometida con los Objetivos de TI y Seguridad y apoya las estrategias con los recursos necesarios	2.2.1			40		70			= 45.91	0.98	Si
M	% del Presupuesto de Anual Operativo de TI y Seguridad con respecto a la facturación Total del Grupo empresarial	2.2.2			30		80			= 53.91	0.98	Si
<b>DIMENSIÓN - Compromiso y Apoyo de la Dirección</b>												
N	Grado de conocimiento del Plan Estratégico de TI, Seguridad y Continuidad para la implementación de Controles y Salvaguardas	2.3.1			55		75			= 27.21	0.97	Si
<b>DIMENSIÓN - Estrategia de Tecnología, Seguridad y Continuidad</b>												

Fuente: Elaboración Propia, 2019.

(Hoja intencionalmente dejada en blanco)

- Fin de la Tesis-