

**DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES (D.R.P) PARA LA
COMPAÑÍA AGENCIA DE ADUANAS PROFESIONAL SIAP NIVEL 1 SEDE
BOGOTÁ.**

LIGIA PATRICIA ARÉVALO CARRANZA

ÁNGELA PATRICIA ZAMBRANO RUIZ

EDWIN NEYID FERNÁNDEZ MAHECHA

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C – 2016

**DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES (D.R.P) PARA LA
COMPAÑÍA AGENCIA DE ADUANAS PROFESIONAL SIAP NIVEL 1 SEDE
BOGOTÁ.**

LIGIA PATRICIA ARÉVALO CARRANZA

ÁNGELA PATRICIA ZAMBRANO RUIZ

EDWIN NEYID FERNÁNDEZ MAHECHA

Trabajo de grado para obtener el título de especialista en Seguridad de la Información

ASESOR: HECTOR DARIO JAIMES

INGENIERO DE SISTEMAS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C – 2016

Atribución-No Comercial-Sin Derivadas 2.5 Colombia (CC BY-NC-ND 2.5 CO)

Usted es libre para:

- **Compartir** — copiar y redistribuir el material en cualquier medio o formato
- El licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

- **Atribución** — Usted debe darle crédito a esta obra de manera adecuada, proporcionando un enlace a la licencia, e indicando si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo del licenciante.
- **No Comercial** — Usted no puede hacer uso del material con fines comerciales.
- **Sin Derivar** — Si usted mezcla, transforma o crea nuevo material a partir de esta obra, usted no podrá distribuir el material modificado.
- **No hay restricciones adicionales** — Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.

Aviso:

- Usted no tiene que cumplir con la licencia para los materiales en el dominio público o cuando su uso esté permitido por una excepción o limitación aplicable.
- No se entregan garantías. La licencia podría no entregarle todos los permisos que necesita para el uso que tenga previsto. Por ejemplo, otros derechos como relativos a publicidad, privacidad, o derechos morales pueden limitar la forma en que utilice el material.

Nota de aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá D.C., Noviembre de 2016.

Dedicatoria

A DIOS, por darme vida, salud, perseverancia en cada momento.

A mi esposo por ser mi compañero de vida, por el optimismo Que siempre me impulso para culminar esta meta propuesta.

A mi hija, por su existencia, por su compañía, por ser mi Fuente de inspiración y motivación para seguir adelante.

A mi madre y hermana, por su ejemplo de Tenacidad, dedicación y su apoyo moral y espiritual.

Ligia Patricia Arévalo Carranza

A Dios por darme salud y fortaleza para cumplir esta meta.

A mi esposo por su comprensión y apoyo incondicional.

A mi abuelita y mi Madre por sus consejos, apoyo, amor y motivación.

Ángela Patricia Zambrano Ruiz

A mi hija, que este documento sea una pequeña muestra, de esfuerzo, dedicación y entrega para lograr

alcanzar las metas propuestas, a mi esposa por ser fuerza, inspiración, aliento y apoyo en la consecución de este objetivo y a mí madre por hacer todo esto posible.

Edwin Neyid Fernández Mahecha

Agradecimientos

Agradezco principalmente a DIOS, quien me ha guiado y otorgado la fortaleza necesaria para culminar este proyecto de vida.

A la Universidad Católica de Colombia, sus docentes, coordinadores y asesor de proyecto, quienes han sido participes activos en este proceso, brindado sus conocimientos, ideas, recomendaciones y experiencias para el desarrollo del proyecto y formación profesional; a mis compañeros de grupo que aportaron y contribuyeron con el desarrollo de actividades durante este periodo académico, dentro de un ambiente amigable, respeto y cordialidad.

A mi Esposo, hija, madre, hermana y en general a toda mi familia y amigos, por la confianza otorgada al saber que cada meta propuesta en mi vida se puede cumplir.

A mis compañeros de especialización, por su gran calidad humana, por contribuir con su conocimiento y por compartir momentos gratos.

Ligia Patricia Arévalo Carranza

Le agradezco a Dios por haberme dado la sabiduría y por darme fortaleza en los momentos de debilidad.

Le doy gracias a mi esposo Ludwig por ser mi compañero de vida, por apoyarme de manera incondicional y motivarme para culminar esta meta.

Le agradezco a mi Madre y Abuelita por impulsarme a seguir adelante.

Les agradezco a mis compañeros de la especialización por aportar sus conocimientos y experiencia.

Les Agradezco a los docentes que hicieron parte de esta formación y aportaron su conocimiento para el desarrollo de mi carrera profesional

Ángela Patricia Zambrano Ruiz

Agradezco a DIOS, por la salud y la oportunidad de alcanzar este objetivo de mi vida. A la Universidad Católica de Colombia, por las herramientas brindadas para el desarrollo del proyecto y la formación profesional; A mi hija, mi esposa y mi madre por ser apoyo, ejemplo, aliento y compromiso.

Edwin Neyid Fernández Mahecha

TABLA DE CONTENIDO

INTRODUCCIÓN	14
1. GENERALIDADES DEL TRABAJO DE GRADO	15
1.1. Línea de investigación.....	15
1.2. Planteamiento del problema	15
1.2.1. Antecedentes del problema	15
1.2.2. Pregunta de investigación.....	17
1.3. Justificación.....	17
1.4. Objetivos	18
1.4.1. Objetivo General	18
1.4.2. Objetivos Específicos	18
2. MARCOS DE REFERENCIA	19
2.1. Marco Conceptual	19
2.2. Marco Teórico	26
2.3. Marco Legal	34
3. ANALISIS DE IMPACTO AL NEGOCIO	39
4. EVALUACIÓN DE RIESGOS.....	40
5. ESCENARIOS DE DESASTRE.....	40
6. DOCUMENTO DRP AGENCIA SIAP NIVEL 1 BOGOTA	42
6.1. Propósito.....	43
6.2. Protección de datos e información confidencial	44
6.3. Prerrequisitos para la ejecución del DRP	44
7. DESCRIPCION DEL SISTEMA.....	45
7.1. Diagnostico situación actual.....	45
7.1.1. Centro de Cómputo y Comunicaciones principal	45
7.1.2. Copia de seguridad de los datos.	46
7.1.3. Infraestructura Básica – Oficinas SIAP Bogotá.....	48
7.2. Propuesta de infraestructura alterna:	50
7.2.1. Data Center Alterno.	51
8. ROLES Y RESPONSABILIDADES	53
8.1. Estructura del equipo de recuperación (organigrama general).....	53
8.2. Equipo de recuperación.....	53
8.2.1. Roles.....	53

8.2.2.	Asignación de roles	55
8.3.	Plan de comunicaciones	57
9.	FASES DE RECUPERACIÓN DE DESASTRES	61
9.1.	Prioridades de Recuperación	61
9.1.1.	Prioridad Alta	61
9.1.2.	Prioridad Media	62
9.2.	Procedimientos de Notificación	62
9.3.	Procedimientos de activación	64
9.3.1.	Orden de Inicio de Servicios de Computo en Ubicaciones Alternas	64
9.4.	Procedimientos en ejecución	67
9.4.1.	Actividades Contingencia Infraestructura	67
9.5.	Fase de Restauración (Plan de retorno a la normalidad)	84
9.5.1.	Decidir donde reiniciar operaciones	84
9.5.2.	Adquirir los recursos adicionales para restaurar por completo la operación.	84
9.6.	Regreso del personal a las instalaciones	85
9.6.1.	Restablecer las operaciones normales de la organización	85
9.6.2.	Reanudación de las operaciones en los niveles anteriores a la interrupción	85
	CONCLUSIONES	86
	REFERENCIAS	88
	APÉNDICE A	90
	APÉNDICE B	91

LISTA DE FIGURAS

Figura 1. Diagrama de Roles	55
Figura 2. Organigrama Roles y responsabilidades	57
Figura 3. Plan de comunicaciones código morado	58
Figura 4. Plan de comunicaciones código Amarillo	59
Figura 5. Plan de comunicaciones código Rojo	60

LISTA DE TABLAS

Tabla 1. Identificación del documento.....	42
Tabla 2. Control de versiones del documento.....	42
Tabla 3. Descripción de la infraestructura actual.....	45
Tabla 4. Políticas de ejecución de Backups de Base de datos	46
Tabla 5. Políticas de ejecución de Backups de Archivos.....	47
Tabla 6. Oficina Alterna	50
Tabla 7. Infraestructura Alterna Base Propuesta	51
Tabla 8. Plan de contingencia del escenario 1	68
Tabla 9. Plan de contingencia del escenario 2	70
Tabla 10. Plan de contingencia del escenario 3	71
Tabla 11. Plan de contingencia del escenario 4	78
Tabla 12. Plan de contingencia del escenario 5	80
Tabla 13. Plan de contingencia – Seguridad de la información.....	81

RESUMEN

En la actualidad uno de los activos más importantes para las compañías es la información, razón por la cual resulta prioritario analizar y diseñar planes de contingencia y de recuperación de desastres. Hoy en día, la compañía SIAP no cuenta con un plan de recuperación de desastres, solo atiende a través de un plan de contingencia, no documentado, sin actualizar y únicamente en caso de falla el canal dedicado de comunicaciones. Teniendo en cuenta lo anterior se realizó un análisis y evaluación de riesgos con el fin de plantear un plan de recuperación de desastres para la Agencia de Aduanas profesional nivel 1 Siap - Sede Bogotá.

La información suministrada en este documento es una sugerencia en la que se establecen normas y procedimientos a seguir en caso de una emergencia o desastre. El uso de dichos procedimientos orienta al personal de la agencia de aduanas a dar respuesta de manera asertiva en caso de ocurrir un evento que destruya todo o parte de los sistemas de información y recursos tecnológicos.

Palabras Clave:

Plan de recuperación de desastres

DRP

Backup

Desastres tecnológicos

Plan de contingencia

INTRODUCCIÓN

La información se ha convertido hoy en día en uno de los recursos más importantes y con gran valor para las empresas. Es vital contar con esta, de manera confiable, completa y oportuna, para que las organizaciones puedan tomar decisiones inteligentes y acertadas. También es evidente que dados los avances tecnológicos, se necesita invertir cada vez más en el recurso humano y económico para garantizar la protección eficiente la información.

Los planes de contingencia se convierten en un aliado significativo para las empresas, en los eventos en que se presenten interrupciones en la continuidad del negocio. En la actualidad las empresas están ajustándose a analizar, diseñar e implementar planes de recuperación de desastres (DRP), que es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que una empresa pueda comenzar de nuevo sus operaciones en caso de un desastre natural o un error humano.

Dado que cada vez más las empresas en Colombia necesitan acogerse de manera inmediata a estos planes de contingencia, se presenta la necesidad de diseñar un DRP para la compañía SIAP, que les permita proteger la información y recuperar su área de tecnología frente a cualquier eventualidad.

1. GENERALIDADES DEL TRABAJO DE GRADO

1.1. Línea de investigación

El ámbito dentro del cual se realiza este proyecto, teniendo en cuenta la poca preparación que tienen las empresas en Colombia, para continuar su operatividad frente a un desastre, lo ubica dentro de la línea de investigación “Software Inteligente y convergencia tecnológica”. La cual pretende, mediante la realización de acciones por parte de los investigadores con una comunidad, modificar un evento.

Toda vez que busca diseñar un plan de recuperación de desastres, dado que la compañía actualmente no cuenta con uno, permitiendo dotar a la entidad de una política de operación en escenarios de contingencia, el cual estará basado en las mejores prácticas y tecnología de vanguardia con el fin de cubrir las necesidades de la entidad y un ofreciendo un valor agregado de confianza para sus clientes.

1.2. Planteamiento del problema

El objetivo de la investigación fue generar el diseño de un plan de recuperación de desastres, para la compañía agencia de aduanas profesional nivel 1 SIAP, que permita la operación óptima de la entidad en escenarios de desastre, en ambientes de contingencia y así mismo la pronta restauración de la normalidad en infraestructura tecnológica y operaciones.

1.2.1. Antecedentes del problema

Hoy día, las organizaciones, buscan estar acordes con el contexto actual de las tecnologías de la información y esta búsqueda se enfoca en apalancar sus operaciones con ella. Normalmente se pretende sistematizar los procesos para hacer a la empresa altamente eficiente; pero no se

establece correctamente lo que puede pasar en caso de un desastre. Cuando se refiere a desastre, no se hace solamente orientado a aspectos de la naturaleza, sino además a la inexperiencia de un usuario que desconecta un cable de un servidor, la falla del fluido eléctrico en las instalaciones, la imposibilidad de acceder a las mismas o cualquier incapacidad para ejecutar las labores cotidianas en la empresa.

Según estudios realizados por Escuela Politécnica del Ejército, Sangolquí, Ecuador sobre las actitudes y prácticas que experimentaron algunas empresas en el momento de un desastre, y la preparación que han tenido para afrontar dichos eventos, se encontraron los siguientes resultados:

- El 46% de las empresas encuestadas en Latinoamérica dijo no considerar prioritario la preparación ante desastres, y ese mismo porcentaje manifestó que en caso de un desastre perdería al menos un 40% de su información.
- El 34% de los clientes de empresas como parte del estudio para Latinoamérica, afirmó que sus proveedores pymes habían suspendido sus servicios temporalmente a causa de un desastre. Esta interrupción les cuesta capital al día a los clientes.

En Colombia, más del 80% de las entidades, no cuentan con planes de predicción y/o contingencia de desastres y según IBM, de las empresas que han tenido una pérdida principal de registros automatizados, el 43% nunca vuelve a abrir, el 51% cierra en menos de 2 años y solo el 6% sobrevive a largo plazo. (<http://www.pymempresario.com/>, 2014)

Observando el contexto y ubicación de la organización, la operatividad del negocio y la tecnología dentro de la misma, en caso de suceder un desastre, este podría traer consigo, para la empresa consecuencias como: la pérdida de vidas, impacto a gran escala de infraestructura física

y tecnológica, afectación total y/o parcial de la cadena de suministro, pérdidas económicas y desventaja competitiva, lo cual podría ser determinante para la continuidad de la compañía.¹

1.2.2. Pregunta de investigación

¿Cuáles son los pasos que debe seguir la compañía Agencia de Aduanas Profesional Nivel 1, para la recuperación de sus procesos e infraestructura tecnológica, ante un desastre?

1.3. Justificación

El desarrollo de este proyecto, es viable, puesto que, un D.R.P. es una estrategia que incluye personas, procesos, políticas y tecnologías. Busca restaurar los sistemas de TI que son fundamentales para el funcionamiento de las entidades, permitiendo mitigar el impacto negativo de una situación adversa, brindando condiciones para continuar con la operación, haciendo más competitiva y eficiente a la organización y ubicándola como un socio estratégico para sus clientes.

Los resultados de esta actividad, contribuyen, con el sector empresarial en Colombia, a la sensibilización y actualización, sobre cómo garantizar la continuidad del negocio y por qué contar con estrategias de recuperación de desastres, debe ser visto como una inversión, más que un gasto, también con la academia quienes pueden utilizar dichos resultados para ilustrar su enseñanza, en el área de gestión de tecnología.

En el mismo contexto, de este proyecto se benefician los clientes, proveedores y accionistas de la empresa, al ver una ruta de acción que permite, retomar con el curso de actividades, al momento de materializarse un riesgo y también, las economías de las ciudades sedes de la misma,

¹ Danilo José Mannella Lemos, Francis Salazar Pico. (2012). Guía de recuperación ante desastres en Pymes usando computación en la nube. Sangolquí, Ecuador: Escuela Politécnica del Ejército.

por la inversión que se realizara en ellas, por mejoras y adecuaciones surgidas de hallazgos hechos en el desarrollo de esta tarea.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar el plan de recuperación de desastres (D.R.P.) para la compañía agencia de aduanas profesional SIAP Nivel 1 oficina Bogotá.

1.4.2. Objetivos Específicos

1. Identificar, analizar y clasificar los principales riesgos a los que se encuentra expuesta la compañía Agencia de Aduanas Profesional Nivel 1 S. I. A. P. sede Bogotá.
2. Establecer y formular, apoyados en los B. I. A, los procesos críticos que se apoyan en tecnología, que soportan la operatividad de la organización y plantear las estrategias de contingencia y fases del plan de recuperación de desastres.
3. Diseñar y entregar con base a las mejores prácticas, propuestas por Cisco y el National Institute of Standards and Technology, el documento con el plan de recuperación de desastres (D.R.P.) para la Agencia de Aduanas Profesional Nivel 1 SIAP sede Bogotá.

2. MARCOS DE REFERENCIA

2.1. Marco Conceptual

Plan de continuidad de negocio: Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.²

El BCP es el cómo una organización se prepara para afrontar futuros incidentes que puedan poner en peligro a ésta y a la consecución de los objetivos misionales del negocio. Las situaciones posibles incluyen desde incidentes locales (como incendios, terremotos, inundaciones, tsunamis etc.), incidentes de carácter regional, nacional o internacional hasta incidentes como pandemias y demás.

Plan de contingencia: Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño (Delivery and Support, véase ITIL).

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante.³

² www.wikipedia.org/Plan_de_continuidad_del_negocio

³ www.wikipedia.org/Plan_de_contingencias

El plan debe ser revisado periódicamente, generalmente, está la revisión será consecuencia de un nuevo análisis de riesgos. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.
- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.
- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista.

Plan de recuperación de desastres: Se enfoca en la recuperación de los servicios de TI (Tecnologías de información) y los recursos, dado un evento que ocasionara una interrupción mayor en su funcionamiento y tiene las siguientes etapas:

- Desarrollo de un reglamento de políticas de planificación de contingencias.
- Análisis del impacto en la empresa (BIA). El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA, (Business Impact Análisis) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un Plan de Continuidad del Negocio.
- Identificación de los controles preventivos. Las medidas tomadas para reducir los efectos de las interrupciones del sistema pueden ayudar a incrementar la disponibilidad del sistema y reducir los costos de los ciclos de vida de las contingencias

- Especificación de las Estrategias de desarrollo de la recuperación. A través de las estrategias de recuperación se asegura que el sistema pueda ser reconstituido de manera rápida y efectiva luego de una interrupción.⁴
- Desarrollo de un plan de contingencias en TI. El plan de contingencias debe contener de manera detallada guías y procedimientos para restaurar el sistema dañado.
- Evaluación del plan, entrenamiento y ejercicios. Con la evaluación del plan se identifican las fallas en la planificación, mientras que el entrenamiento prepara al personal que se ocupa de la recuperación para la activación del plan; ambas actividades mejoran la efectividad del mismo y la preparación de toda la agencia.
- Mantenimiento del Plan. El plan puede ser un documento vivo que sea actualizado regularmente para mantener el sistema acorde con los desafíos.

Un plan de recuperación puede ser de dos tipos: desastres naturales y desastres provocados por el hombre, y cualquiera de ellos puede tomar por sorpresa a las organizaciones, con poca o ninguna advertencia. Cuando algún desastre se presenta, aquellas empresas que se han preparado y efectuado sus Planes de Recuperación ante Desastres (DRP) sobreviven con una interrupción de su productividad o pérdida mínima de datos.

El objetivo principal de un plan de recuperación de desastres DRP es ayudar a que la organización mantenga la continuidad de su negocio, minimice los daños y prevenga pérdidas.

⁴ Jairo Romero, Jennifer Ramírez. (2013). Diseño e implementación de un prototipo que permita el despliegue de un plan de recuperación de desastres aplicable a empresas mipymes colombianas. Bogotá: Universidad Católica de Colombia.

Consecuentemente, y de acuerdo a lo mencionado anteriormente lo importante de un DRP es estar seguro de que cuando se lo ponga en práctica funcione, y para ello hay que ejecutarlo regularmente.

Proveedor: Persona o empresa que abastece a otras empresas o personas con productos, bienes o servicios, los cuales serán transformados para venderlos posteriormente y/o directamente se compran para su venta.

Data center: Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones. Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Virtualización: Es la creación a través de software, de una versión no física de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.⁵

Desastre: Es un evento calamitoso, repentino o previsible, que trastorna seriamente el funcionamiento de una comunidad, sociedad u organización y causa pérdidas humanas, materiales, económicas o ambientales que desbordan la capacidad de la comunidad o sociedad afectada para hacer frente a la situación a través de sus propios recursos. Aunque frecuentemente están causados por la naturaleza, los desastres pueden deberse a la actividad humana.⁶

⁵ www.wikipedia.org/Virtualización

⁶ www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/

Gestión de riesgo: El riesgo como “La exposición a la posibilidad de ocurrencia de ciertas cosas tales como pérdida o ganancia económica, daño físico, retrasos, daño a la salud pública, etc. que surgen como consecuencia de seguir un curso particular de acción” .El concepto de riesgo tiene dos elementos, la probabilidad de que algo ocurra y las consecuencias de si esto ocurre. Para efectuar una efectiva y eficiente gestión del riesgo, es necesario considerar cual es la probabilidad de que un siniestro ocurra y cuáles serían las consecuencias que se podrían generar si una o todas las cosas que podrían suceder en realidad sucedieran. Es importante considerar que los riesgos pueden surgir tanto de fuentes internas como externas”.

Administración del riesgo: Es un proceso lógico y metódico utilizado cuando se toman decisiones para mejorar la efectividad y eficiencia de las operaciones propias de una organización. La Administración de Riesgo se puede definir como “La aplicación sistemática de políticas, procedimientos y prácticas de gestión a la tarea de identificar, analizar, evaluar, tratar y controlar los riesgos.

Análisis de impacto del negocio (BIA): El objetivo fundamental es identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre. Además identifica los sistemas críticos y estima el tiempo que la compañía puede tolerar en caso de un desastre.

Un análisis de Impacto de negocio permite abordar un plan de acción con sólidos elementos de criterio basados no sólo en necesidades de capacidad, sino también de seguridad. Para poder definir las contingencias deseadas es necesario conocer los servicios de IT que el departamento de

informática ofrece a la compañía, sus vulnerabilidades, así como las amenazas y posibles impactos; además de identificar qué servicios de IT soportan los procesos de negocio de la compañía.⁷

RPO (Recovery Point Objective): Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. ¿Las transacciones de cuánto tiempo está dispuesta a perder, o a tener que reintroducir al sistema? El RPO determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

RTO (Recovery Time Objective): Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

Pasos a seguir para recuperar las aplicaciones y los datos en caso de contingencia:

- Restaurar el ordenador (dependiendo del tipo de problema pueden ser minutos, horas o días).
- Restaurar las copias de seguridad
- Reanudar la operación

A partir de este punto se deberán repetir las transacciones que faltan, desde el momento de la caída hasta el momento de la recuperación, que serán más cuanto mayor sean RPO y RTO.⁸

⁷ Jairo Romero, Jennifer Ramírez. (2013). Diseño e implementación de un prototipo que permita el despliegue de un plan de recuperación de desastres aplicable a empresas mipymes colombianas. Bogotá: Universidad Católica de Colombia.

⁸ www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

Costes de recuperación de desastres: Definir los valores de RPO y RTO, pueden proporcionar resultados sorprendentes que podrían no ser aceptables para la gestión. Una vez fijados, podrá establecer una estrategia de recuperación, que llevará asociados unos costes que varían en función precisamente del RPO y del RTO.⁸

Operación normal para contingencia: En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para mantener preparada la solución de recuperación, compuesta por la infraestructura contratada (Centro de cómputo de Contingencia, enlaces de comunicaciones, aplicaciones) y el Plan de Recuperación de Desastres (DRP).⁹

Manejo de incidentes: En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para evaluar un problema que potencialmente lleve a la declaración de contingencia, la toma de la decisión de dicha declaración y la notificación de la misma, tanto a las áreas internas como a entes externos (clientes, proveedores, entidades reguladoras y otros).

Cubre el período desde el momento cero de la contingencia, es decir aquel en el cual se presenta el evento, hasta que se activen los equipos de trabajo y sus respectivos planes.⁹

Movilización: En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para trasladar la operación afectada al Centro de Computo de Contingencia - CCC y en caso de ser requerido al – Centro de Operaciones de Contingencia COC; desde el momento en que se declara, notifica y activan los planes, hasta la puesta en operación de dichos servicios al segundo data center.⁹

⁹ Jairo Romero, Jennifer Ramírez. (2013). Diseño e implementación de un prototipo que permita el despliegue de un plan de recuperación de desastres aplicable a empresas mipymes colombianas. Bogotá: Universidad Católica de Colombia.

Operación durante la contingencia: En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar durante la operación en el Centro de Cómputo de Contingencia, después de concluida la movilización, con el fin de mantener activas las aplicaciones movilizadas, hasta el momento en que se inicia el retorno a la normalidad, prestando el servicio con las restricciones propias de la contingencia.⁹

Retorno a la normalidad: En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar desde el momento en que se inicia la movilización del CCC hacia el CCP, hasta que el servicio sea recuperado totalmente en el CCP.⁹

Agente aduanero: Persona jurídica autorizada por la DIAN para actuar ante los órganos competentes del servicio aduanero en nombre y por cuenta de aquel que contrata sus servicios, en el trámite de una operación, régimen o actividad aduanera.

NIST: El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), la misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.¹⁰

2.2. Marco Teórico

NIST 800 – 34: Guía de planificación de contingencia para los Sistemas de Información, proporciona instrucciones, recomendaciones y consideraciones para la planificación de la información.

¹⁰ www.wikipedia.org/Instituto_Nacional_de_Estandares_y_Tecnología

Esta guía se dirige a las recomendaciones específicas de planificación de contingencia para tres tipos de plataforma y proporciona estrategias y técnicas comunes a todos los sistemas.

- Sistemas cliente / servidor;
- Los sistemas de telecomunicaciones;
- Sistemas mainframe.

Esta guía define el siguiente proceso de planificación de contingencia de siete pasos que una organización puede aplicar para desarrollar y mantener un programa de planificación de contingencia viable para sus sistemas de información. Estos siete pasos progresivos están diseñados para ser integrados en cada etapa del ciclo de vida de desarrollo del sistema.

1. Desarrollar la declaración de política de planificación de contingencia. Una política formal proporciona la autoridad y la orientación necesaria para desarrollar un plan de contingencia efectivo.
2. Llevar a cabo el análisis de impacto en el negocio (BIA). El BIA ayuda a identificar y dar prioridad a los sistemas de información y los componentes críticos para apoyar los procesos de misión / negocio de la organización. Se proporciona una plantilla para el desarrollo de la BIA para ayudar al usuario.
3. Identificar los medios de prevención. Las medidas adoptadas para reducir los efectos de las interrupciones del sistema pueden aumentar la disponibilidad del sistema y reducir los costes del ciclo de vida de contingencia.
4. Crear estrategias de contingencia. Estrategias de recuperación exhaustivas asegurar que el sistema se puede recuperar rápidamente y con eficacia después de una interrupción.

5. Desarrollar un plan de información del sistema de contingencia. El plan de contingencia debe contener orientaciones y procedimientos detallados para la restauración de un sistema dañado única para requisitos de nivel de impacto en la seguridad y recuperación del sistema.
6. Asegurar que se analiza el plan, el entrenamiento y ejercicios. Las pruebas validan las capacidades de recuperación, mientras que el entrenamiento prepara al personal de recuperación para la activación del plan y ejercer el plan identifica las carencias de planificación; combinado, las actividades mejoran la efectividad del plan y la preparación general de la organización.
7. Asegurar el mantenimiento del plan. El plan debe ser un documento vivo que se actualiza regularmente para mantenerse al día con las mejoras del sistema y los cambios en la organización.¹¹

SANS institute - disaster recovery plan strategies and processes: está diseñada para asegurar la continuidad de los procesos de negocio vitales en el caso de que se produzca un desastre. Este plan proporciona una solución eficaz que puede ser utilizada para recuperar todos los procesos de negocio vitales dentro del marco de tiempo requerido usando registros vitales que son almacenados fuera del sitio.

Este Plan es sólo uno de los diversos planes que proporcionan procedimientos para manejar situaciones de emergencia. Pueden ser utilizados individualmente, pero están diseñados para soportar uno otro.

• ¹¹ Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. (2010). Contingency Planning Guide for Information Technology Systems. Estados Unidos: National Institute of Standards and Technology.

Por lo tanto, la prevención de riesgos es un elemento crítico en el proceso de recuperación de desastres. Un Sistema de Gestión de recuperación de desastres se puede definir como el proceso en curso de la planificación, desarrollo, prueba e implementación de los procedimientos y procesos de gestión de recuperación de desastres para asegurar la reanudación eficiente y eficaz de las funciones vitales del negocio en caso de una interrupción no programada.¹²

Con la creciente dependencia de E / S y el Business Process y el apoyo y crecimiento del negocio y los cambios asociados con sus complejidades, agravada con la complejidades de la evolución de la tecnología, los siguientes elementos son clave para implementar un programa integral de recuperación de desastres:

- Evaluación de aplicaciones críticas
- Procedimientos de respaldo
- Procedimientos de recuperación
- Procedimientos de Ejecución
- Procedimientos de prueba
- Plan de Mantenimiento

Cisco disaster recovery: best practices: Los desastres son inevitables, pero sobre todo impredecibles y varían en tipo y magnitud. La mejor estrategia es contar con un plan de recuperación de desastres en su lugar, para volver a la normalidad, después de que un escenario de riesgo se ha materializado. Para una empresa, un desastre significa la interrupción brusca de la

● ¹² SANS Institute Disaster Recovery Plan. Cycle The Plan, Plan the Cycle. Febrero 2002

totalidad o parte de sus operaciones comerciales, que pueden resultar directamente en la pérdida de ingresos.

Para reducir al mínimo las pérdidas por desastres, es muy importante tener un buen plan de recuperación, para cada subsistema y operación del negocio dentro de una empresa. En el área de tecnologías de la información, la recuperación de desastres (D.R.), no quiere decir lo mismo que, alta disponibilidad.

Aunque ambos conceptos están relacionados con la continuidad del negocio, la alta disponibilidad se trata prestar el servicio de forma interrumpida, mientras que las operaciones de recuperación de desastres implica una cierta cantidad de tiempo de inactividad, por lo general estos tiempos son medidos en días.

Cada desastre en el negocio tiene una o más causas y efectos. Las causas pueden ser naturales, humanas o de origen mecánico, que van desde eventos tales como un pequeño componente de hardware o software de mal funcionamiento, a situaciones universalmente conocidas tales como terremotos, incendios e inundaciones.

Los resultados finales son una evaluación formal de riesgos, un plan de recuperación de desastres, incluye todos los mecanismos disponibles de recuperación y un Comité de recuperación de desastres, de carácter oficial, que tiene la responsabilidad de planear, ejecutar, probar y mejorar el plan diseñado para una entidad.¹³

La recuperación de desastres que ocurre en las siguientes fases secuenciales:

¹³ CISCO Systems. White_paper_c11-453495 Disaster Recovery: Best Practices. Agosto 2008.

1. Fase de activación: en esta fase, los efectos de los desastres se evalúan y anuncian.

2. Fase de ejecución: En esta fase, los procedimientos reales, para recuperar cada una de las entidades y/o frentes afectados se ejecutan. Las operaciones de negocios se restauran en el sistema de recuperación.

3. Fase de reconstitución: En esta fase el sistema original se restaura y de nuevo es puesto en marcha, los procedimientos activados en la fase de ejecución se detienen y las operaciones son retornadas a la normalidad.

Marco de recomendaciones norma ISO 17799: Lo que pretende esta norma es ofrecer un conjunto de reglas a un sector donde anteriormente no existían teniendo en cuenta las necesidades actuales:

- Los usuarios necesitan políticas de seguridades claras y disponibles.
- Los administradores necesitan técnicas de seguridad y control.
- Los administradores de seguridad necesitan un entorno flexible para mantener y comunicar las políticas de seguridad.
- Los recursos tecnológicos deben estar disponibles para todos los usuarios.
- Debe contarse con métodos para garantizar la integridad, seguridad, validez y disponibilidad de la información.

La norma técnica ISO 17799, proporciona una serie de estándares reconocidos mundialmente sobre las áreas que se muestran. Los fundamentos de un buen sistema de gestión de seguridad de la información son las 10 áreas de control de seguridad, que se mencionan a continuación.

- Política de Seguridad. La política documentada ayuda a proyectar las metas de seguridad de la información de una organización.
- Organización de la Seguridad. Relacionada con el diseño de una estructura de administración dentro de la organización que establezca la responsabilidad de los grupos en áreas de seguridad y un proceso para el manejo de respuesta a incidentes.
- Clasificación y Control de Activos. Relacionado con la necesidad de inventariar y clasificar los activos de la organización en cuanto a su criticidad, grado de exposición al riesgo y nivel de protección necesario, y la designación de responsables por la custodia de los mismos.
- Seguridad del Personal. Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad, integrándolos de esta forma en la cadena de detección y respuesta a incidentes.
- Seguridad Física y Ambiental. Responde a la necesidad de proteger las áreas de procesamiento e instalaciones de la organización.
- Gestión de Comunicaciones y Operaciones: Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información
- Minimizar el riesgo de falla de los sistemas
- Proteger la integridad del software y la información
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.

- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.
- Control de Accesos. Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos y externos.
- Desarrollo y mantenimiento de Sistemas. En toda labor de tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso de desarrollo e implantación de software.
- Administración de la Continuidad de los Negocios. La organización debe estar preparada para contrarrestar las interrupciones en las actividades y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.
- Cumplimiento. Establece la necesidad de que las organizaciones verifiquen si el cumplimiento con la Norma Técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la Privacidad, la Ley de Responsabilidad y Transferibilidad del Seguro Médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Bliley (GLBA por su sigla en inglés).¹⁴

Técnica Delphi: Una Delphi consiste en la selección de un grupo de expertos a los que se les pregunta su opinión sobre cuestiones referidas a acontecimientos del futuro. Las estimaciones

¹⁴ www.wikipedia.org/ISO/IEC_27002

de los expertos se realizan en sucesivas rondas, anónimas, al objeto de tratar de conseguir consenso, pero con la máxima autonomía por parte de los participantes.

Se puede decir también que el método Delphi es una técnica de comunicación estructurada, desarrollada como un método de predicción sistemático interactivo, que se basa en un panel de expertos. Es una técnica prospectiva para obtener información esencialmente cualitativa, pero relativamente precisa, acerca del futuro. Por lo tanto, la capacidad de predicción de la Delphi se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos.

Aunque, la formulación teórica del método Delphi propiamente dicho comprende varias etapas sucesivas de envíos de cuestionarios, de vaciado y de explotación, en buena parte de los casos puede limitarse a dos etapas, lo que sin embargo no afecta a la calidad de los resultados tal y como lo demuestra la experiencia acumulada en estudios similares.

Delphi se basa en:

- Anonimato de los intervinientes.
- Repetitividad y retroalimentación controlada.
- Respuesta del grupo en forma estadística.

2.3. Marco Legal

Régimen Administrativo Aduanero: La actividad aduanera en Colombia se encuentra regulada al detalle en el Decreto 2685 de 1999, expedido por el Ministerio de Hacienda y Crédito Público, y en la Resolución 4240 de 2000, por medio del cual el gobierno nacional reguló la legislación aduanera. Sin embargo, existen disposiciones de orden constitucional y legal que le

sirven de fundamento normativo, y que son de obligatoria referencia a efectos de analizar debidamente el fenómeno de la importación ordinaria.

Decreto 2685 de 1999

ARTICULO 5. SISTEMATIZACIÓN DE LOS PROCEDIMIENTOS ADUANEROS.

Los procedimientos para la aplicación de los diferentes regímenes aduaneros de que trata el presente Decreto, deberán realizarse mediante el uso del sistema de transmisión y procesamiento electrónico de datos, adoptado por la autoridad aduanera. En casos de contingencia, la autoridad aduanera podrá autorizar el trámite manual mediante la presentación física de la documentación.

De acuerdo con lo previsto en el inciso anterior y en los términos y con los controles que para el efecto establezca la Dirección de Impuestos y Aduanas Nacionales se podrán efectuar por medios electrónicos, entre otras, las siguientes operaciones: ingreso y salida de mercancías al o desde el territorio aduanero nacional, presentación de las declaraciones, aceptación o rechazo de las mismas, determinación de la inspección, liquidación de tributos aduaneros y sanciones, levante de mercancías y, en general, todos los procesos de importación, exportación y tránsito de mercancías, incluido el pago a través de transferencia electrónica de fondos o cualquier sistema que otorgue garantías similares.

Para el desarrollo y facilitación de dichas operaciones a través del sistema informático aduanero, la Dirección de Impuestos y Aduanas Nacionales expedirá normas y establecerá los parámetros técnicos y procedimientos que regulen la emisión, transferencia, uso y control de la información relacionados con tales operaciones. La información del sistema informático aduanero deberá estar soportada por medios documentales, magnéticos o electrónicos, y se reputará legítima,

salvo prueba en contrario. PARAGRAFO. La autoridad aduanera podrá fijar los costos de utilización del sistema informático aduanero y los procedimientos de recaudo de los mismos.

ARTICULO 6. MEDIDAS Y PROCEDIMIENTOS DE CONTINGENCIA.

La Dirección de Impuestos y Aduanas Nacionales dispondrá de los procedimientos y desarrollos informáticos y de comunicaciones que garanticen la prestación continua e ininterrumpida del servicio aduanero y de los mecanismos de control previstos en este Decreto, a través de los procesos automatizados establecidos en el mismo.

Cuando se presenten fallas en el sistema informático aduanero, podrá aceptarse la realización de trámites, actuaciones y procesos aduaneros mediante la utilización de medios documentales, físicos o magnéticos, según lo disponga la autoridad aduanera.

ARTICULO 7. FORMULARIOS OFICIALES PARA DECLARAR LOS REGÍMENES ADUANEROS.

Las declaraciones de importación, exportación y tránsito aduanero deberán presentarse en los formularios oficiales que para el efecto determine la Dirección de Impuestos y Aduanas Nacionales, a través de medios electrónicos, o magnéticos, o excepcionalmente por medios documentales cuando ésta así lo autorice. En circunstancias especiales, la Dirección de Impuestos y Aduanas Nacionales podrá autorizar la presentación de declaraciones utilizando formularios habilitados para el efecto.

ARTICULO 8. UTILIZACIÓN DE LA CLAVE ELECTRÓNICA CONFIDENCIAL.

Para la presentación de información y documentos ante las autoridades aduaneras a través de medios electrónicos de transmisión de datos, los usuarios utilizarán el sistema de identificación

que determine la Dirección de Impuestos y Aduanas Nacionales, mediante la asignación de una clave electrónica confidencial.¹⁵

Decreto 2883 de 2008:

Artículo 12. Agencias de aduanas. Las agencias de aduanas son las personas jurídicas autorizadas por la Dirección de Impuestos y Aduanas Nacionales para ejercer el agenciamiento aduanero, actividad auxiliar de la función pública aduanera de naturaleza mercantil y de servicio, orientada a garantizar que los usuarios de comercio exterior que utilicen sus servicios cumplan con las normas legales existentes en materia de importación, exportación y tránsito aduanero y cualquier operación o procedimiento aduanero inherente a dichas actividades.

Las agencias de aduanas tienen como fin esencial colaborar con las autoridades aduaneras en la estricta aplicación de las normas legales relacionadas con el comercio exterior para el adecuado desarrollo de los regímenes aduaneros y demás actividades y procedimientos derivados de los mismos.

Conforme con los parámetros establecidos en este decreto, las agencias de aduanas se clasifican en los siguientes niveles:

1. Agencias de aduanas nivel 1.
2. Agencias de aduanas nivel 2.
3. Agencias de aduanas nivel 3.
4. Agencias de aduanas nivel 4.

¹⁵ www.dian.gov.co/descargas/normatividad/Proy_Normatividad/Proyecto_Estatuto_SIN_PV_Dic_01_2011.pdf

Artículo 14. Requisitos generales de las agencias de aduanas. Para ejercer la actividad de agenciamiento aduanero se deberá cumplir con los siguientes requisitos generales:

8. Contar con una infraestructura financiera, física, técnica, administrativa y, con el recurso humano que permita ejercer de manera adecuada la actividad de agenciamiento aduanero.

Artículo 15. Requisitos especiales para las agencias de aduanas nivel 1. Además de los requisitos generales establecidos en el artículo anterior, las agencias de aduanas nivel 1, deberán cumplir con los siguientes requisitos:

3. Mantener a disposición del público una página Web donde se garantice el acceso a la siguiente información:

- a) Estados financieros.
- b) Identificación de los representantes legales, gerentes, administradores, agentes de aduanas y auxiliares autorizados para actuar ante la Dirección de Impuestos y Aduanas Nacionales, junto con un extracto de las hojas de vida destacando su experiencia o conocimiento en comercio exterior.
- c) Relación de los servicios ofrecidos al público.

Artículo 27-2. Obligaciones de las agencias de aduanas. Las agencias de aduanas en ejercicio de su actividad, a través de sus representantes legales, administradores, agentes de aduanas o auxiliares tendrán las siguientes obligaciones:

18. Contar con la infraestructura de computación, informática y comunicaciones, debidamente actualizada, conforme a la tecnología requerida por la Dirección de impuestos y

Aduanas Nacionales, a efectos de garantizar la debida transmisión electrónica en los regímenes aduaneros y los documentos e información que la entidad determine.¹⁶

3. ANALISIS DE IMPACTO AL NEGOCIO

El análisis de impacto al negocio (BIA), permite identificar la prioridad de recuperación de cada área, determinando el impacto en caso de interrupción. Esta actividad implica identificar los procesos críticos, los recursos utilizados para soportar la operación, así mismo los proveedores, también determinar los sistemas críticos y evaluar el tiempo que SIAP puede tolera en caso de un incidente o desastre. EL BIA es la guía que determina que necesita ser recuperado y el tiempo que se requiere para dicha recuperación.

A través del desarrollo del BIA se obtiene la siguiente información:

- Evaluación de los procedimientos, donde se establece cuáles son primordiales para la continuidad de la Entidad.
- Priorización y establecimiento del período de tiempo en el que los sistemas, aplicaciones y funciones deben ser recuperados después de una interrupción (RTO).
- Establecimiento del tiempo máximo tolerable permitido de pérdida de información ante una Interrupción en los sistemas de información (RPO).
- Definición de los recursos necesarios para el buen desarrollo de los procedimientos a nivel De: Tecnología, personal, infraestructura y soporte proveedores.

(Ver Apéndice A)

¹⁶ www.dian.gov.co/descargas/normatividad/dec288306082008.pdf

4. EVALUACIÓN DE RIESGOS

La capacidad para reestablecer las operaciones de tecnología y cada uno de los procesos del negocio, ante algún evento que pueda interrumpir las actividades que le impidan cumplir con sus objetivos estratégicos, es un elemento esencial para la compañía. Los riesgos asociados son altos y la dependencia de las tecnologías de información ha motivado a SIAP a establecer medidas preventivas y un plan de recuperación para reanudar sus actividades en un tiempo adecuado.

En esta etapa se identificaron y analizaron las posibles amenazas de personas, infraestructura y procesos que podrían generar riesgos de continuidad del negocio. La gestión de riesgos tiene como objetivo reducir el impacto que puede provocar un evento de desastre o una interrupción significativa en los servicios. (Ver Apéndice B).

5. ESCENARIOS DE DESASTRE

El Plan DRP está diseñado para crear un estado de preparación y respuesta oportuna y adecuada a cualquiera de los siguientes escenarios:

- **Escenario 1:** Limitación parcial o pérdida total de Servicios de Telecomunicaciones en la Head Office SIAP Bogotá: el incidente ocasionó daños importantes en cualquiera de los equipos críticos de los servicios de Telecomunicaciones de la compañía y como resultado éste se encuentra inoperable, total o parcialmente. El personal técnico y operativo de SIAP, Head Office Bogotá, si tiene acceso a las instalaciones y sus puestos de trabajo habituales.
- **Escenario 2:** Incidentes con Contratistas críticos de Servicios, el altercado puede causar fallas o interrupciones de los servicios entregados por terceros. (ejemplo: telefonía, internet, Data Center, Almacenamiento de datos), afectando directamente los servicios proporcionados por SIAP.

- **Escenario 3:** Limitación en el funcionamiento de los servicios dispuestos por la Dirección de Informática y Tecnología y/o Centro de Computo inoperable: en este escenario se considera que el incidente ocasionó una pérdida parcial de la Head Office Bogotá, inhabilitando la operatividad del Centro de Cómputo.

- **Escenario 4:** Acceso Nulo a las instalaciones Head Office SIAP Bogotá/Limitación de Personal o evacuación del edificio (Con funcionamiento del centro de datos): el incidente ocasionó que el personal no tenga acceso a la Head Office Bogotá o las instalaciones fueron evacuadas, pero los Centros de Cómputo no han sufrido daños y continúan operando de manera normal.

- **Escenario 5:** Acceso limitado a las instalaciones Head Office SIAP Bogotá/Limitación de Personal o evacuación del edificio (Sin funcionamiento del centro de datos): el incidente ocasionó que el personal tenga acceso limitado a los puestos disponibles en la Head Office Bogotá o que las instalaciones fueron evacuadas, y la disponibilidad de los Centros de Cómputo no están operando normalmente.

En escenarios mencionados, la activación de los equipos de recuperación, será indicada cuando el Comité Directivo de Manejo de Incidentes, en su evaluación, declare el desastre y la activación del Plan DRP a través del Coordinador Ejecutivo IMP con la notificación al Gerente y/o Coordinador DRP.

6. DOCUMENTO DRP AGENCIA SIAP NIVEL 1 BOGOTA

Tabla 1. Identificación del documento

IDENTIFICACIÓN DEL DOCUMENTO		
Propietario del documento:	Agencia de Aduanas Profesional Nivel 1 SIAP	
País:	Bogotá, Colombia	
Edificio:	Head Office SIAP BOGOTA	
Nombre del Documento:	Plan de Recuperación de Desastre (DRP SIAP V 1.0)	Código: DRP SIAP –BGT - DIT-001
		Área Responsable: Dirección de Informática y Telecomunicaciones
Status del documento:	Versión 0	

Tabla 2. Control de versiones del documento

CONTROL DE VERSIONES DEL DOCUMENTO					
Versión	Descripción	Autor	Acción	Fecha	Firma
0	Plan de Recuperación de Desastres (DRP)	PATRICIA AREVALO ANGELA ZAMBRANO EDWIN FERNANDEZ	ELABORACION	NOVIEMBRE 2016	

6.1. Propósito

El Plan de Recuperación de Desastres (DRP) está diseñado como lista de comprobación o instructivo de trabajo en caso de la materialización de un escenario de desastre a nivel de infraestructura. En él, se describen las estrategias, los recursos, los procesos y los procedimientos que los equipos de recuperación de desastres que la Dirección de Informática y Tecnología, utilizará para cualquier incidente o acontecimiento imprevisto que substancialmente interrumpa o deteriore la Head Office SIAP Bogotá.

Este **DRP** busca dar los lineamientos para conseguir las siguientes metas:

- A. Disponer de un plan de acción organizado, para atender una interrupción inesperada en los servicios críticos ofrecidos por la Dirección de Informática y Tecnología.
- B. Prestar una oportuna continuidad en los servicios tecnológicos de la Dirección de Informática y Tecnología de la Agencia de adunas profesional nivel 1 SIAP sede Bogotá, en caso de presentarse una situación de contingencia mayor o catastrófica.
- C. Establecer la coordinación de actividades y comunicación interna y externa, adecuada, entre los líderes de la Dirección de Informática y Tecnología y los usuarios de servicios de tecnología finales.
- D. Recuperar las aplicaciones críticas del negocio de una manera oportuna, incrementando la habilidad de la compañía para recuperarse de una pérdida o daños a las instalaciones y servicios.
- E. Administrar exitosamente los eventos de desastre, minimizando el impacto al negocio.

6.2. Protección de datos e información confidencial

Cuando sea necesario entregar este **Desaster Recovery Plan**, (en adelante **DRP**) a terceras partes no pertenecientes al grupo **SIAP**, se entregara una copia del mismo en la que no se incluyan datos de carácter personal de los miembros de los equipos de recuperación ni de ningún otro participante en el **DRP**. Si se requiere comprobar que los miembros están definidos se puede invitar a la tercera empresa a visualizar una copia del **DRP** desde un computador de **SIAP** sin permitir ningún tratamiento sobre los datos personales ni el contenido del mismo. De igual manera se trataran los datos confidenciales de sistemas, configuraciones, contraseñas y redes dirección IP, etc.

6.3. Prerrequisitos para la ejecución del **DRP**

La ejecución satisfactoria del plan de recuperación de desastres describe los siguientes requerimientos para su adecuado funcionamiento:

- Los recursos mínimos para la ejecución de los procedimientos de recuperación y/o contingencia se han adquirido y están disponibles.
- Los funcionarios se encuentran disponibles y tienen el perfil para ejecutar las diferentes actividades asignadas.
- Se cuenta con unos sitios alternos y operativos; dispuestos para la recuperación de las operaciones, procesos y procesamiento de información.
- El respaldo de la información crítica (registros vitales), se está realizando de forma adecuada en un lugar fuera de las instalaciones de la compañía y con las prácticas de seguridad adecuadas en el transporte de los mismos.
- El suministro del servicio de energía es normal en los sitios alternos.

- Las organizaciones externas tales como aseguradores, proveedores, agencias gubernamentales, no han sufrido el desastre, cooperarán en la recuperación de la compañía y estarán disponibles en cualquier momento de la recuperación.

7. DESCRIPCION DEL SISTEMA

7.1. Diagnostico situación actual

7.1.1. Centro de Cómputo y Comunicaciones principal

Se encuentra contratado a modo de “Colocation”, está ubicado en la Calle 170 con Av. Boyacá, en la bodega DATACENTER COLOMBIA XV, que pertenece al proveedor LEVEL TREE, en Bogotá, D.C., Colombia. Su ubicación permite un fácil acceso y cuenta con respaldo a fallos eléctricos, y redundancia en canales de telecomunicaciones.

La infraestructura tecnología dispuesta en este lugar se describe a continuación.

Tabla 3. Descripción de la infraestructura actual

DESCRIPCIÓN	HOSTNAME	RAM (GB)	STORAGE GB	SISTEMA OPERATIVO	PROCESADORES	Modelo
Servidor web SGO	SIAPWEB	21	281,46	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	BLADE FOR RACK
Servidor Reportes	SIAPTABLEAU	9	118,54	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	
Servidor Documentos	SIAPDOCS	4	738,41	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	

DESCRIPCIÓN	HOSTNAME	RAM (GB)	STORAGE GB	SISTEMA OPERATIVO	PROCESADORES	Modelo
Servidor RDP	SIAPADMIN	14	244,12	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	
Servidor Base de Datos	SIAPBD	32	731,86	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	
Servidor Soporte (JQ - DIFERBAO)	SRVSOPORTE	8	236,51	Windows Server 2012	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	
Servidor Intercomex	INTERCOMEX - SIAP	8	120,51	Linux Centos 7	Intel Xeon CPU ES- 2680 2,7 Ghz (4 Procesadores)	

En la actualidad No se cuenta con centro de cómputo alterno.

7.1.2. Copia de seguridad de los datos.

Las copias de seguridad completa e incremental preservan los activos de información corporativa y se realizan de forma regular para registros de auditoría y archivos que sean insustituibles, tienen un alto costo de reposición, o se consideran críticos.

Descripción de frecuencia, tipo de backup y sistema resguardado:

Tabla 4. Políticas de ejecución de Backups de Base de datos


POLITICAS DE BACKUP						
SERVIDOR	PERIODICIDAD	PERIODO DE RETENCION	POOL	TIPO DE BACKUP	INSTANCIA	FRANJA HORARIA PARA BACKUP
SIAPBD	Diario	1 Semana	Netbackup	FULL	ADM	Domingo a Viernes 02:00 am
	Semanal	1 Mes	Netbackup-Mensual			Sabado 02:00
	Mensual	1 Año	SIAP-Anual			Primer martes del mes 02:00
	Diario	1 Semana	Netbackup	FULL	OPE	Domingos a Viernes 18:00
	Semanal	1 Mes	Netbackup-Mensual			Sabado 18:00
	Mensual	1 Año	SIAP-Anual			Primer martes del mes 18:00

Tabla 5. Políticas de ejecución de Backups de Archivos

POLITICAS DE BACKUP					Level(3) CORPORATE AND PRODUCTION THE BACKUP AND RECOVERY
MAQUINA	PERIODICIDAD	PERIODO DE RETENCION	POOL	TIPO DE BACKUP	FRANJA HORARIA PARA BACKUP
SIAPADMIN	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 01:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 01:00
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 01:00
	Anual	Infinito	Net Backup-Trianual		Primer día del año a partir de la 01:00 am
SIAPBD	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 01:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 01:00 am
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 01:00 am
	Anual	Infinito	Net Backup-Trianual		Primer día del año a partir de la 01:00 am
SIAPDOCS	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 04:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 04:00 am
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 04:00 am
INTERCOMEX-SIAP	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 05:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 05:00 am
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 05:00 am
	Anual	Infinito	Net Backup-Trianual		Primer día del año a partir de la 05:00 am
SIAPTABLEAU	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 02:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 02:00 am
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 02:00 am
	Anual	Infinito	Net Backup-Trianual		Primer día del año a partir de la 02:00 am
SIAPWEB	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Lunes a Sabado 20:30
	Semanal	1 Mes	Netbackup-Mensual		Domingo 14:00
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 04:00 am
SRVSOPORTE	Diaria	1 Semana	Netbackup	ALL_LOCAL_DRIVES	Domingo a Viernes 03:00 am
	Semanal	1 Mes	Netbackup-Mensual		Sabado 03:00
	Mensual	1 Año	SIAP-Anual		Ultimo sabado del mes 03:00
	Anual	Infinito	Net Backup-Trianual		Primer día del año a partir de la 04:00 am

Las instalaciones de seguridad de la empresa de Custodia de los BackUp de la información Externa contratada por SIAP para este servicio, están bajo responsabilidad del proveedor LEVEL 3, el cual garantiza, se encuentran suficientemente alejadas de la sede del Centro de Proceso de Datos, en una infraestructura industrial específicamente seleccionada para este propósito, ubicadas en una zona empresarial cerrada, con vigilancia nocturna e inmejorables accesos a las principales zonas de negocios de Bogotá.

Esta empresa cuenta con los más avanzados sistemas para garantizar la seguridad y conservación de los soportes magnéticos.

No se cuenta con un plan establecido para la restauración de la información, en caso de ser necesario.

7.1.3. Infraestructura Básica – Oficinas SIAP Bogotá

Actualmente las oficinas de SIAP, se encuentran ubicadas en la Calle 25 G No 100 – 26 en Bogotá Colombia, en un edificio de 5 plantas, con puertas de seguridad exteriores, operadas de forma electrónica, con acompañamiento de personal de celaduría, vigilado en modelo 7* 24, con personal profesional para dicha actividad, circuito cerrado de televisión, alarma conectada a la policía del sector, servicios públicos completos y rutas de fácil acceso.

Sistema de detección de humo y alarma para incendios, con conexiones de agua para bomberos, 12 extintores categoría 123 (todo incendio), de capacidad media, distribuidos de la siguiente manera, dos en el primer piso, para recepción y parqueadero, tres en el segundo piso para el area, tres en el tercer piso, dos en el cuarto piso y dos en el quinto piso.

130 Escritorios de madera con cajoneras de metal, 130 sillas ergonómicas de material acolchado y malla, iluminación natural y acondicionada con cajones de lámparas fluorescentes sobre cada puesto.

En cuento a infraestructura tecnológica, está dotado con:

- 150 puntos de red de datos distribuidos de la siguiente manera :

12 En el primer piso.

35 En el segundo piso.

44 en el tercer piso.

40 En el cuarto piso.

25 en el quinto piso

- 100 puntos de red de telefonía.

- 6 impresoras distribuidas de la siguiente manera:
 - 1 en la primera planta, junto a recepción.
 - 2 en la segunda planta, compartidas por los operarios de la dirección Operativa y Comercial.
 - 2 en la tercera planta, compartida por los operarios de la dirección administrativa y de informática y telecomunicaciones.
 - 1 En el 5 piso compartida por las oficinas de los directores de área.

100 teléfonos y 200 Celulares.

RACK CENTRAL ubicado en área de Data Center del 4 Piso, junto a las oficinas de tecnología en zona aislada de acceso restringido, dotada de aire acondicionado, alimentación de energía eléctrica con corriente regulada y acondicionada con UPS de 20 KVA, sistema detector de humo y control de temperatura.

Gabinete de comunicaciones, con ocho switches, cuatro de 48 puertos, administrables capa 2 – 3 Marca CISCO Small Bussines SGE2000P y cuatro de 24 puntos capa 2, X510 Series Allied Telesis, conectados en apilamiento, que garantizan la cobertura en puntos de red para la oficina.

Entrada de canal principal de comunicaciones, LEVEL 3, con router CISCO Small Bussines RV25, y canal alternativo con router del proveedor CLARO.

En la actualidad no se cuenta con oficinas alternas en la ciudad de Bogotá, se tiene sede de operaciones ubicada en la ciudad de Medellín.

7.2. Propuesta de infraestructura alterna:

Tabla 6. Oficina Alterna

SITIO ALTERNO				
RECURSO HUMANO MINIMO	DIR. OPERATIVA	DIR.COMERCIAL	DIR.ADTVA	DIR. T.I.
PERSONAS	8	1	2	2
AUXILIARES	2	1	2	1
DISPOSICION DE PUESTOS DE TRABAJO	25			
UBICACIÓN	Oficina en ubicación Central, de Facil acceso, Sector Propuesto Chapinero, Provista de servicios publicos Energia, Agua, Telefono, Y Telecomunicaciones			
EQUIPOS EN OFICINA ALTERNA				
PC	10	2	3	3
IMPRESORAS	1	1	1	1
ESCRITORIO	10	2	3	2
PLANTA ELECTRICA	1			
TELEFONOS	4	1	1	1
INFRAESTRUCTURA				
Red LAN	25 Puntos de datos			
	10 Puntos de Voz			
red Wi Fi	Acces Point para Clientes Wi Fi			
Switches	1 de 48 Puntos Capa 2 - 3 Administrable con Capacidad de apilamiento			
Centro de cableado	1			
Firewall	1			
Red WAN				
Router	2 Principal y redundante que garantice conectividad			
Enlaces	2 Principal y redundante que garantice conectividad			
Materiales y herramientas para cableado estructurado				
Gabinete de comunicaciones				

SITIO ALTERNO				
RECURSO HUMANO MINIMO	DIR. OPERATIVA	DIR.COMERCIAL	DIR.ADTVA	DIR. T.I.
Aire Acondicionado	1			
Sistema Electrico	1	1	1	1
UPS	1			
Sistema de Incendio	1			
OTROS				
Red de energía eléctrica alternativa	1			
Ubicación geográfica a más de 25 km de la ubicación de las oficinas principales de SIAP	1			
Facilidad de vías de acceso principales y secundarias	1			
Disponibilidad de Servicios públicos	1			
Proveedor de Canal de Telecomunicaciones en sede alterna	2 (1 Principal - Level 3 y 1 Alterno ETB)			

7.2.1. Data Center Alterno.

Tabla 7. Infraestructura Alterna Base Propuesta

SERVIDOR	MODELO	POCESADORES	RAM	DISCO DURO	INTERFACES DE RED	ALIMENTACION	SERVICIO
ALTERTPR	RACK - BladeCenter	Intel Xeon - 4 Core - 2,4 Ghz - 2M cache HT	8 GB	SATA - 500 Gb	2 - 1GB	Fuentes de alimentación de alta eficiencia hot-swap de 2980 W CA con funciones de equilibrio de carga y failover. Funcionamiento a 200 - 240 V	PROXY
ALTERP1	RACK - BladeCenter	Intel Xeon - 4 Core - 2,4 Ghz - 2M cache HT	8 GB	SATA - 500 Gb	2 - 1GB	Fuentes de alimentación de alta eficiencia hot-swap de 2980 W CA con funciones de equilibrio de carga y failover.	DNS – DHCP

SERVIDOR	MODELO	POCESADORES	RAM	DISCO DURO	INTERFACES DE RED	ALIMENTACION	SERVICIO
						Funcionamiento a 200 - 240 V	
ALTERP2	RACK - ThinkServer	Intel Xeon E5 - 4 Core - 3,2 GHZ, 12Mb Cache	16 GB	SATA - 1 TB	2 - 1GB	Fuente 550w, certificación 80 PLUS Platinum	LDAP - SQL 2008
ALTERP3	RACK - ThinkServer	Intel Xeon E5 - 4 Core - 3,2 GHZ, 12Mb Cache	32 GB	SATA - 1 TB	2 - 1GB	Fuente 550w, certificación 80 PLUS Platinum	FILE SERVER
ALTERP4	TORRE - Power Edge	Intel Xeon E3 - 4 Core - 3,5 GHZ, 8Mb Cache	8 Gb	SATA - 500 Gb	2 - 1GB	Fuente de alimentación de CA de 750 W	JQ WEB SERVER
ALTERP5	RACK - BladeCenter	Intel Xeon - 4 Core - 2,4 Ghz - 2M cache HT	16 GB	SATA - 500 Gb	2 - 1GB	Fuentes de alimentación de alta eficiencia hot-swap de 2980 W CA con funciones de equilibrio de carga y failover. Funcionamiento a 200 - 240 V	SGO, SIGLO XXI
ALTERP6	RACK - BladeCenter	Intel Xeon - 4 Core - 2,4 Ghz - 2M cache HT	16 GB	SATA - 500 Gb	2 - 1GB	Fuentes de alimentación de alta eficiencia hot-swap de 2980 W CA con funciones de equilibrio de carga y failover. Funcionamiento a 200 - 240 V	SEOS, COLSIN

La propuesta recomendada para este centro de procesamiento de datos alternos (Data Center Alterno) tiene como base la tecnología Cloud Data Center, en modalidad D&R (Dissaster and Recovery), que permite a la empresa implementar e integrar la protección automática a un

precio asequible. Es una alternativa que, además de ser económica, es eficiente y escalable a cualquier requisito, incluso permite ampliar su complejidad inicial.

Este servicio permite administración en tiempo real, bajos RTOs, bajos RPO, uso eficiente del ancho de banda, disminuye limitaciones geográficas y minimiza el riesgo de pérdida de datos.

8. ROLES Y RESPONSABILIDADES

8.1. Estructura del equipo de recuperación (organigrama general)

Las principales funciones de este equipo serán restablecer los servicios de cómputo mediante la restauración de la infraestructura, software operativo, los sistemas, las telecomunicaciones y los datos. Proveerá un enlace entre los esfuerzos de recuperación de la Dirección de Informática y Tecnología y las áreas de negocio. El personal de la DIT también apoyará con el reporte de evaluación de daños en la infraestructura de tecnología.

8.2. Equipo de recuperación

La conformación de equipo de recuperación de desastres tiene como objetivo establecer las distintas responsabilidades para conseguir recuperación exitosa ante una emergencia, teniendo en cuenta el DRP establecido.

8.2.1. Roles

El equipo de DRP tiene las siguientes responsabilidades:

- Definir controles preventivos necesarios y viables, con el fin de disminuir la probabilidad de ocurrencia.
- Establecer, probar, ajustar y actualizar el DRP.
- Recuperar los servicios en el menor tiempo posible y dentro de los tiempos establecidos.

- Realizar un informe acerca de las causas del desastre y en caso de ser necesario modificar los controles y el DRP si así se requiere.

Teniendo en cuenta las responsabilidades, se conformaron los siguientes equipos de trabajo y se establecieron sus funciones:

a. Dirección Estratégica y Coordinación(DEC):

- Dirigir y coordinar las actividades de los demás equipos que conforman la brigada de DRP.
- Manifestar la situación de emergencia, contingencia y restablecimiento.
- Determinar el nivel de desastre producido por una contingencia: total o mayor, parcial, menor.
- Realizar y probar los planes de recuperación.
- Controlar la ejecución del DRP y realizar los respectivos ajustes teniendo en cuenta los problemas y errores detectados durante la ejecución del mismo

b. Recuperación de hardware (RH):

- Identificar el hardware que ha sido afectado por el plan de contingencia.
- Coordinar con los proveedores de hardware el cumplimiento de los contratos de mantenimiento, garantías y niveles de soporte.
- Participar en las instalaciones de sistemas operativos que realizan los proveedores Comprobar el funcionamiento del hardware que han sido restaurados o remplazados por proveedores.
- Identificar los elementos de comunicaciones y centros de cómputo que han sido afectados por el plan de contingencia.
- Suministrar los backups necesarios para la restauración de la información.
- Suministrar el software necesario para la restauración

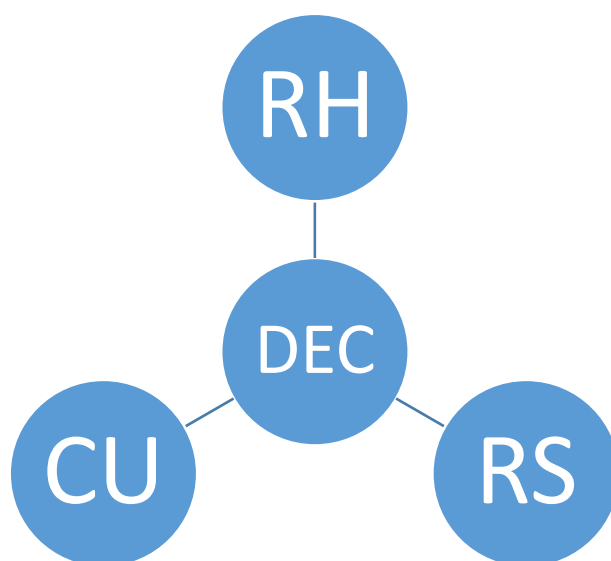
c. Recuperación de software (RS):

- Identificar servicios, procesos, bases de datos y aplicaciones que han sido afectados por el plan de contingencia.
- Instalar, configurar y adecuar el software que ha sido afectado por la contingencia.

d. Equipo de comunicación a usuarios (CU):

- Comunicar oficialmente a los usuarios, el plan de contingencia que será llevado a cabo, el tiempo del restablecimiento de las condiciones normales.
- Realizar comunicados a los usuarios internos.

Figura 1. Diagrama de Roles



8.2.2. Asignación de roles

D E C (Dirección Estratégica y coordinación)

- Coordinador General del Plan

R H (Recuperación de Hardware)

- Líder de infraestructura
- Proveedores Principales y alternos

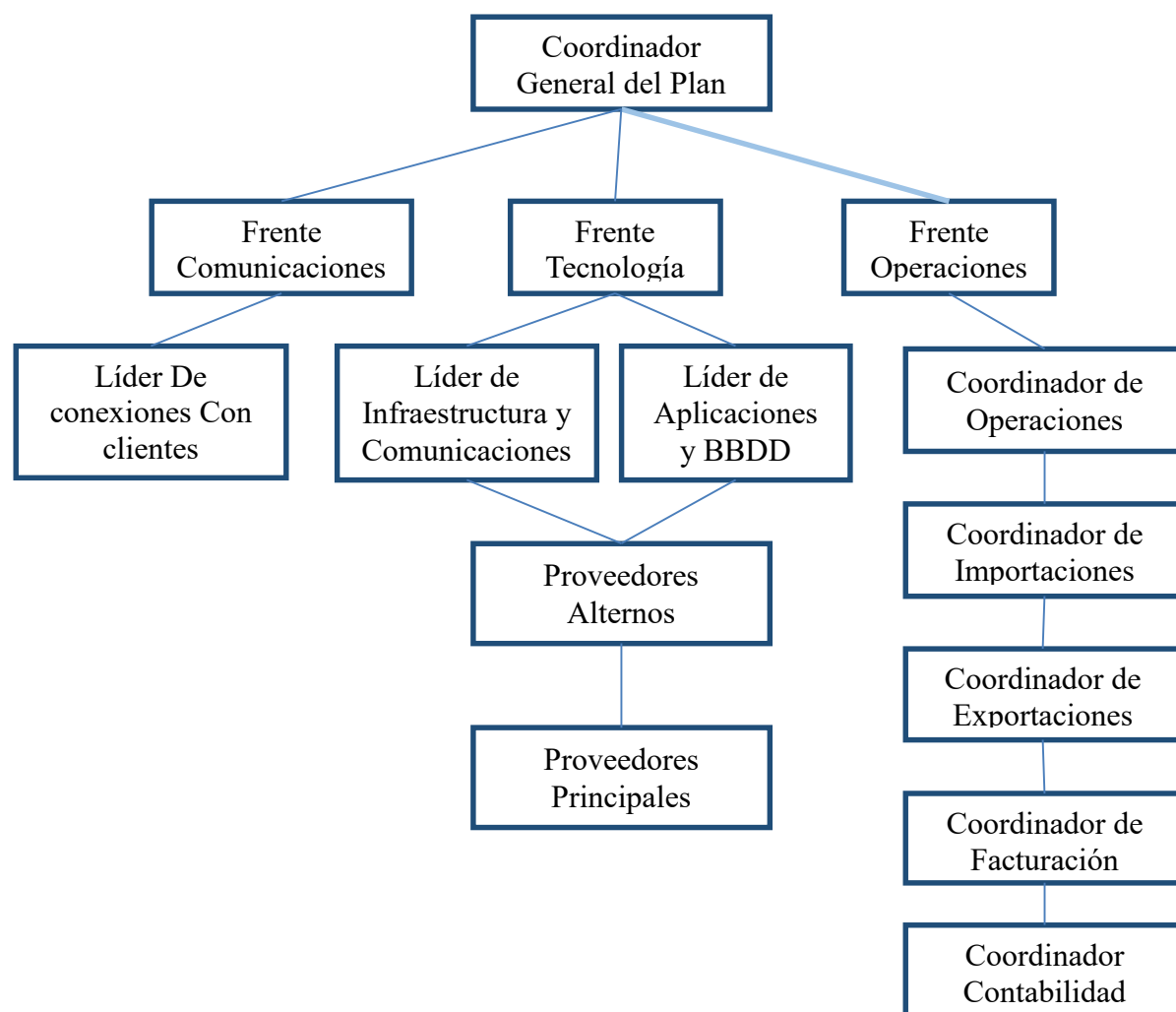
R S (Recuperación Software)

- Líder de aplicaciones y Base de datos

C U (Comunicación Usuarios)

- Coordinador de operaciones

Figura 2. Organigrama Roles y responsabilidades

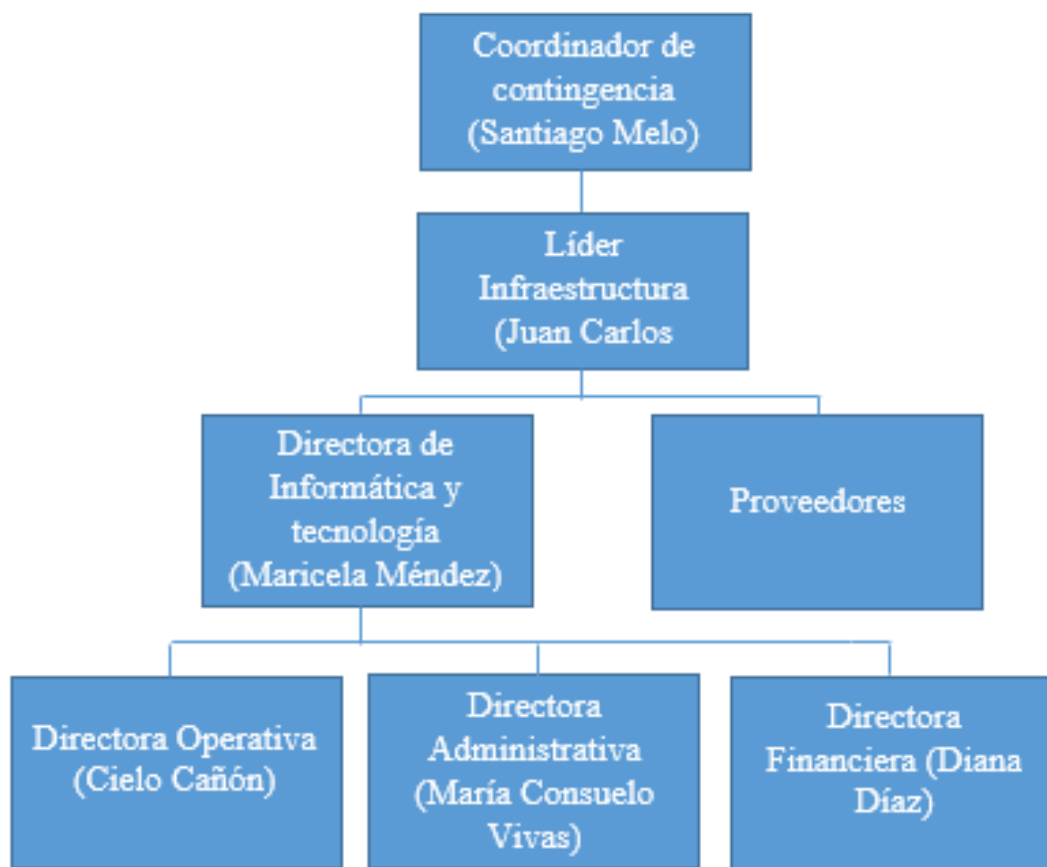


8.3. Plan de comunicaciones

En el plan de comunicaciones, se establece el orden jerárquico en el cual serán informados los usuarios acerca del plan de contingencia que se llevará a cabo y los tiempos establecidos para regresar la operación a la normalidad.

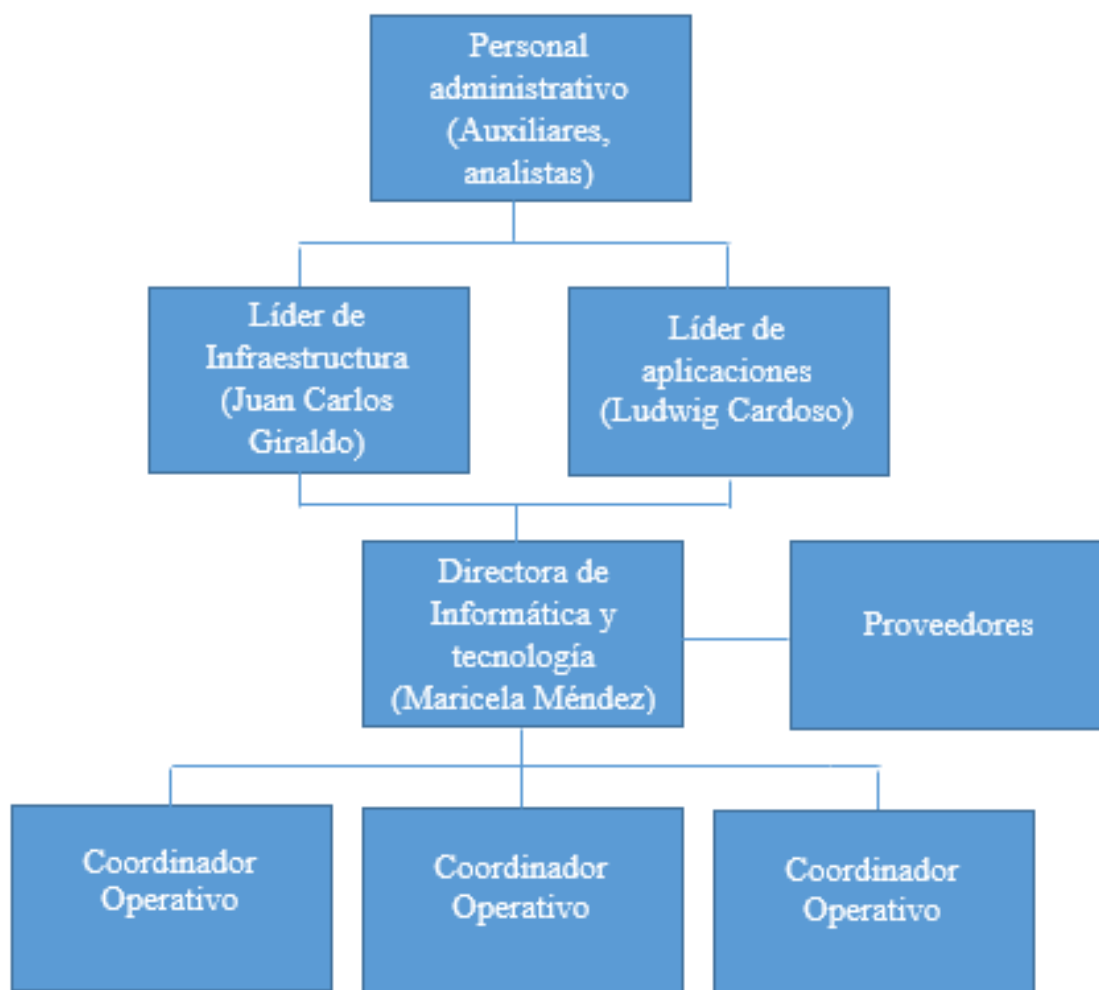
- **Código Morado:**

Figura 3. Plan de comunicaciones código morado



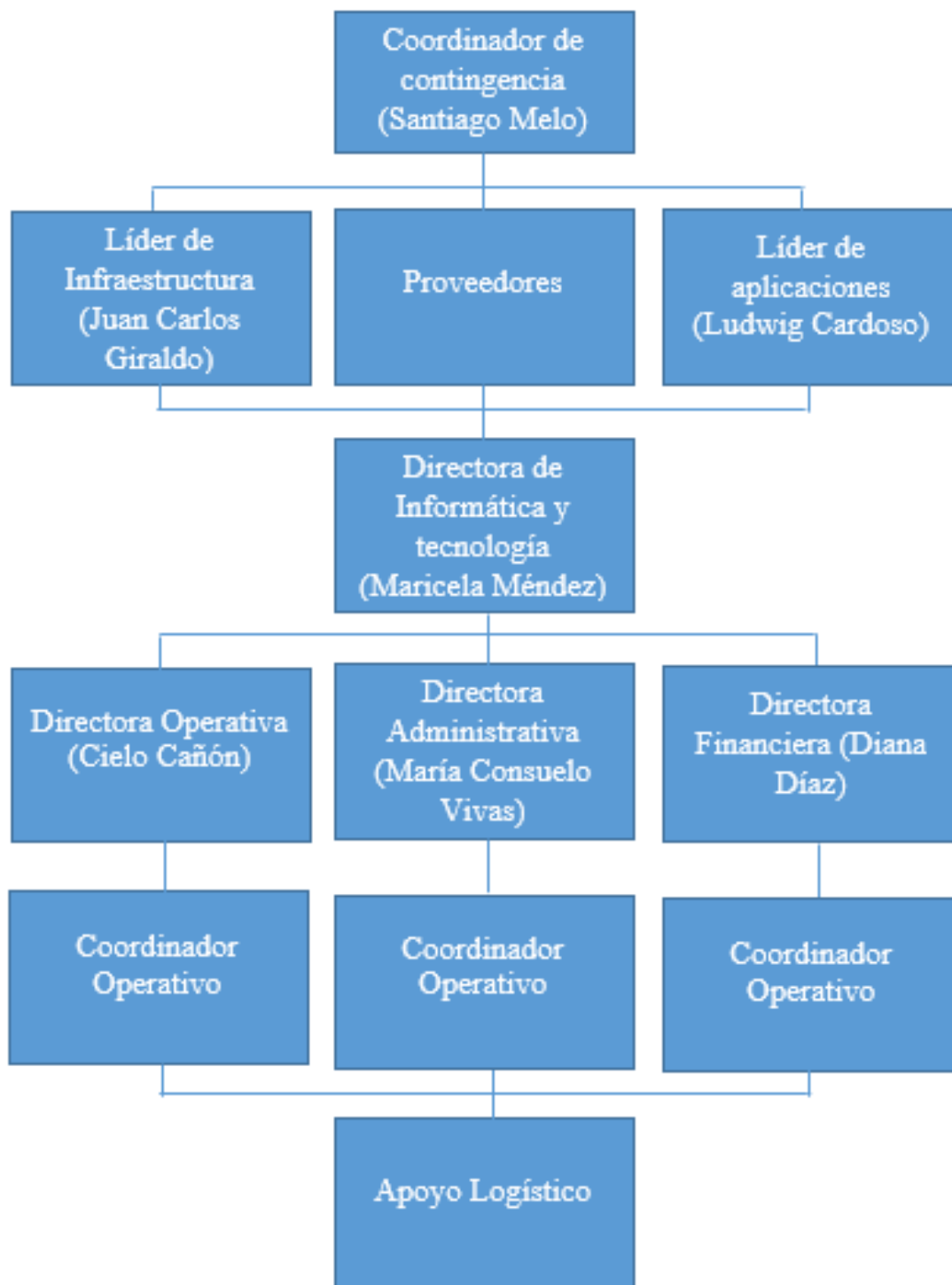
- **Código Amarillo**

Figura 4. Plan de comunicaciones código Amarillo



- **Código Rojo:**

Figura 5. Plan de comunicaciones código Rojo



9. FASES DE RECUPERACIÓN DE DESASTRES

Se recogen en este apartado las principales estrategias alternativas de recuperación y los tiempos estimados de restauración de los servicios.

La restauración de copias de seguridad de datos conforme a la política y procedimientos aprobados por la Dirección, las alianzas y acuerdos de colaboración

Con proveedores alternativos para la sustitución urgente de componentes o elementos de hardware fallidos, la utilización y mantenimiento de grupos electrógenos y sistemas de alimentación ininterrumpidos (UPS) que cubran eventuales cortes en el suministro de energía eléctrica y la flexibilidad para utilizar la sede alternativa de SIAP, ubicada geográficamente con capacidad para la recuperación de procesos críticos.

9.1. Prioridades de Recuperación

De acuerdo a la clasificación de funciones de la agencia de adunas profesional nivel 1 SIAP, sede Bogotá y los puntos máximos, las prioridades de recuperación durante el plan de contingencia son:

9.1.1. Prioridad Alta

- Canales de comunicación - WAN
- Canal de Internet Local
- Infraestructura de Red Local
- Herramientas de Gestión de Servicios y su infraestructura de apoyo (Servidores y Bases de Datos)
- Infraestructura de apoyo (Telefonía/telecomunicaciones y aplicaciones)
- Aplicaciones de negocio

9.1.2. Prioridad Media

- Correo electrónico
- Servidor PROXY.

9.2. Procedimientos de Notificación

Los criterios de activación se basan en la evaluación de los siguientes parámetros:

- Seguridad del personal y/o magnitud de los daños de las instalaciones
- Magnitud del daño de la infraestructura (Física, Operacional, otra)
- Estimativo del tiempo de interrupción

Si la notificación inicial es clara y evidente, se puede activar el plan de continuidad asignando un código de color:

- **Morado:** Pérdida total del centro de operación espacio de trabajo para colaboradores e infraestructura de la empresa
- **Rojo:** Incidentes graves en curso que afectan los procesos críticos de la Compañía.
- **Amarillo:** Incidentes graves en progreso pero bajo control.
- **Verde:** El incidente ya no está en progreso o el incidente se realiza bajo procedimientos operativos normales.

En los demás casos, la notificación se iniciará como código de color amarillo. Así mismo, después de la evaluación de los daños, el código se puede cambiar a rojo o verde, dependiendo del resultado.

Criterio para código Morado

La integridad de los recursos y equipos de la oficina Head Office SIAP Bogotá, debido a causas de desastre natural, evento de fuerza mayor o pérdida de canales de comunicaciones; así mismo se considera la ausencia masiva de personal que impida la operación normal.

Instrucciones:

- a. Activar Plan de comunicaciones para dicho código.
- b. Activar Lugar Alterno de Operación.
- c. Activar Canales Alternos de Comunicación.
- d. Activar Data Center Alterno (si es necesario).
- e. Activar Plan de Continuidad de Recursos Humanos, solo si es necesario.

Criterio para código Rojo

Un incidente que tiene efectos severos o catastróficos para las operaciones, activos o personas la compañía SIAP Bogotá. Se considera un evento que afecte a más de 65 usuarios finales, en la calidad de prestación y entrega de los servicios de apoyo a los procesos misionales, algunos escenarios contemplados son:

- Incidentes en las facilidades del Centro de cómputo de la oficina principal. (Falla de Suministro Eléctrico, Falla en el canal de comunicación principal, latencia en las comunicaciones, alarma de detección de incendios)
- Pérdida de infraestructura crítica: Enlaces de Red, Telefonía, directorio activo, servidor de archivos.

Instrucciones:

- a. Activar Plan de Contingencia Infraestructura de acuerdo al Escenario.

- b. Activar Plan de Continuidad solo si es necesario.

Criterio para código Amarillo

Progreso de un riesgo o incidente grave pero bajo control:

- Pérdida de aplicaciones críticas.
- Ataque de virus informáticos.

Instrucciones:

- a. Solicitar al Administrador del Centro de cómputo, ejecutar los procedimientos de restauración de servicios de acuerdo al Incidente.

9.3. Procedimientos de activación

9.3.1. Orden de Inicio de Servicios de Computo en Ubicaciones Alternas

En el evento que sea necesario hacer uso de las ubicaciones alternas, dispuestas para superar los escenarios de desastre, se debe hacer el control, para el orden de activación de los servicios de cómputo, el cual garantizara el funcionamiento adecuado de la infraestructura alterna, el orden propuesto es el siguiente:

1. Inicio de servicios eléctricos en ubicación alterna.
2. Inicio de servicios de telecomunicaciones principales (canal de internet), en ubicación alterna. Si estos no están disponibles, pasar a punto 2.1.

2.1 Inicio de Servicios de Telecomunicaciones de respaldo (alternos). No usar estos servicios si la conexión principal está activa.
3. Activar gabinete de comunicaciones de la oficina alterna.
4. Activar equipos de cómputo de gestión de TI, en oficina alterna.
5. Verificar acceso a la red desde los equipos de gestión de TI, en la oficina alterna.

6. Verificación de conectividad a internet en ubicación alterna por canal principal o alterno.
7. Validación de Conexión, desde ubicación alterna a Data Center Colombia XV, si dicha conexión es nula o no se presenta, pasar al punto 7.1.

7.1 Activar estrategia DRP, de servidores con el proveedor GIGAS. Pasar a punto 20.1
8. Verificación de disponibilidad de File Server.
9. Verificar perdida de información en File Server. Si hay pérdidas de información pasar a punto 21.1.
10. Verificación de disponibilidad de aplicativo SEOS.
11. Verificar perdida de información en aplicativo SEOS. Si hay pérdidas de información pasar a punto 21.2
12. Verificación de disponibilidad de aplicativo SGO.
13. Verificar perdida de información en aplicativo SGO. Si hay pérdidas de información pasar a punto 21.3
14. Verificación de disponibilidad de aplicativo Siglo XXI.
15. Verificar perdida de información en aplicativo Siglo XXI. Si hay pérdidas de información pasar a punto 21.4
16. Verificación de disponibilidad de aplicativo JQ.
17. Verificar perdida de información en aplicativo JQ. Si hay pérdidas de información pasar a punto 21.5
18. Verificación de disponibilidad de aplicativo Diferbao.
19. Verificar perdida de información en aplicativo Diferbao. Si hay pérdidas de información pasar a punto 21.6

20. Activación estrategia DRP con proveedor GIGAS.

20.1 Conectarse por consola WEB, a la herramienta de administración de servidores de GIGAS.

20.2 Verificar que la plataforma e imágenes de los servidores virtuales estén accesibles.

20.3 Iniciar el servidor alternativo DNS - DHCP.

20.4 Iniciar el servidor alternativo AD – LDAP.

20.5 Verificar en el servidor alternativo AD – LDAP inicio de servicio de Motor de Base de Datos SQL 2008.

20.6 Iniciar servidor Alterno FILE SERVER.

20.7 Verificar conexión a carpetas compartidas del file server desde una de las estaciones de trabajo de la sede alterna.

20.8 Iniciar servidor Alterno WEB SERVER – JQ

20.9 Verificar que los servicios del Internet Information Server estén activos y disponibles.

20.10 Validar que el servicio MsFoxPro este activo y disponible.

20.11 Iniciar servidor Alterno SGO

20.12 Validar que el sitio web de la compañía SGO esté disponible a nivel de la red Interna de la Organización.

20.13 Validar que el aplicativo Web Siglo XXI responda a peticiones a nivel de la red Interna de la organización.

20.14 Iniciar servidor Alterno COLSIN – SEOS

20.15 Validar que se presente disponibilidad del servicio del aplicativo COLSIN.

20.16 Validar que el aplicativo SEOS responda a peticiones a nivel de la red Interna de la organización.

20.17 Verificar desde una de las maquinas cliente acceso a los diferentes servidores y o servicios ofrecidos por cada uno de estos.

21. Validación de Perdida de Información.

21.1 Si se presenta Perdida de Información en File Server.

21.2 Validar la fecha y hora del backup replicado con la información de servidor de archivos. Si es el más actualizado, se inicia el proceso de liberación del servidor y reingreso de información no disponible al momento.

21.3 Verificar y solicitar con el proveedor LEVEL3 la disponibilidad del backup de dicha carpeta de información, con una fecha más actualizada.

21.4 Restaurar la imagen de la información entregada por LEVEL3.

21.5 Validar acceso al recurso desde los equipos cliente.

21.6 Liberar recurso para iniciar el proceso reingreso de información no disponible al momento.

9.4. Procedimientos en ejecución

9.4.1. Actividades Contingencia Infraestructura

- **Escenario 1:** Limitación parcial o pérdida total de Servicios de Telecomunicaciones en la Head Office SIAP Bogotá: el incidente ocasionó daños importantes en cualquiera de los equipos críticos de los servicios de Telecomunicaciones de la compañía y como resultado éste se encuentra inoperable, total o parcialmente. El personal técnico y operativo de SIAP, Head Office Bogotá, si tiene acceso a las instalaciones y sus puestos de trabajo habituales.

Tabla 8. Plan de contingencia del escenario 1

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
<ul style="list-style-type: none"> Ausencia prolongada en el servicio de comunicación por voz, ya sea por desastres naturales, error humano, fallas en los componentes del sistema de telecomunicaciones, fallas eléctricas, vandalismo, etc. Ausencia prolongada en el servicio de Conectividad, ya sea por desastres naturales, error humano, fallas en los componentes del sistema de telecomunicaciones, fallas eléctricas, vandalismo, etc. Caída del servicio de internet., ya sea por desastres naturales, error humano, fallas en los componentes del sistema de telecomunicaciones, 	<ul style="list-style-type: none"> Telefonía fija, telefonía IP, servicio de larga distancia nacional e internacional, etc. Canal de comunicación LAN y WAN, Gabinete de comunicaciones, switches, routers, firewalls, modem, etc. Conexión VPN 	<ul style="list-style-type: none"> La oficina no cuenta con equipos suficientes que garanticen el óptimo desarrollo de las actividades críticas. Soporta la infraestructura de comunicaciones del Head Office Bogotá 	<ul style="list-style-type: none"> El personal técnico y operativo de SIAP que si tiene acceso a las instalaciones, valida la magnitud del daño ocasionado, revisa si se cuenta en servicio otros medios de comunicación alternos tales como correo electrónico, telefonía celular, etc. En caso de no contar con estas alternativas se debe llamar al Proveedor de soporte, con el fin de reestablecer el servicio de manera oportuna de acuerdo a lo contratado. Si se encuentra daño en algún equipo de comunicación, los técnicos deben validar si es posible la recuperación o reemplazo del equipo afectado en un tiempo mínimo. Validar si dentro del inventario de equipamiento se tienen existencias del equipo afectado para su reemplazo. Si la contingencia implementada no soporta la falta de disponibilidad de servicio de telecomunicaciones se activa 	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
fallas eléctricas, vandalismo, etc.	<ul style="list-style-type: none"> Fibra óptica Banda ancha 		<p>el data Center y Oficina alterna.</p> <ul style="list-style-type: none"> La compañía tiene enlace a Internet con el proveedor CLARO en la Of principal. SIAP cuenta con alta disponibilidad de sus canales con redundancia para Bogotá – DATA CENTER Colombia VX, en caso de caída subirá automáticamente el otro, sin que se vea afectado el servicio. Si la contingencia implementada no soporta la falta de disponibilidad de servicio de internet se activa el data Center y Oficina alterna. 	

- Escenario 2:** Incidentes con Contratistas críticos de Servicios, el altercado puede causar fallas o interrupciones de los servicios entregados por terceros. (ejemplo: telefonía, internet, Data Center, Almacenamiento de datos), afectando directamente los servicios proporcionados por SIAP.

Tabla 9. Plan de contingencia del escenario 2

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
<ul style="list-style-type: none"> cortes de servicios por suspensión de productos contratados sin Importar su causa, ya sean ocasionados por huelgas, daños en la infraestructura propia o de los proveedores. Finalización unilateral de contratos causados por cambios en las condiciones pactadas, precios etc. Deficiencias en el Servicio por demoras o mala calidad en los servicios contratados. 	<ul style="list-style-type: none"> Sistema de comunicación para funcionarios SIAP Bogotá 	<ul style="list-style-type: none"> Soporta la infraestructura de comunicaciones del Head Office Bogotá. 	<ul style="list-style-type: none"> Notificar o reportar el incidente brindando la mayor cantidad de información posible acerca del incidente al coordinador del plan, constatar la veracidad del incidente presentado Identificar el tipo de incidente, evaluando si está relacionado con seguridad de la información o con requerimientos de infraestructura de TI, determinado a la vez el impacto de la situación de desastre en la infraestructura de los sistemas de información y/o comunicación y poder decidir sobre las acciones a ejecutar. Verificar la disponibilidad de recursos para la contingencia como: existencia de oficinas o áreas de la sede que no estén afectadas por la interrupción del servicio entregados por terceros, donde se pueda continuar con la operación normal de ciertas labores, manuales técnicos de instalación de sistemas de comunicación, restauración de backups etc. 	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
			<ul style="list-style-type: none"> Comunicar a los usuarios del incidente presentado indicando el tiempo estimado de restablecimiento del servicio, si la contingencia no es suficiente, se habilita el sitio alternativo donde se garantiza la disponibilidad de equipos de comunicación y la disponibilidad de la información. 	

● **Escenario 3:** Limitación en el funcionamiento de los servicios dispuestos por la Dirección de Informática y Tecnología y/o Centro de Computo inoperable: en este escenario se considera que el incidente ocasionó una pérdida parcial de la Head Office Bogotá, inhabilitando la operatividad del Centro de Cómputo.

Tabla 10. Plan de contingencia del escenario 3

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Falla en el suministro eléctrico	Sistema Eléctrico en el espacio de trabajo para operarios funcionales e infraestructura tecnología SIAP Bogotá	Soporta la infraestructura de comunicaciones, redes y seguridad del Head Office Bogotá.	Validar la activación automática de la UPS de 20 KVAs, la cual está respaldada por la planta eléctrica en el Piso 1 Head Office Bogotá. En caso negativo, llamar inmediatamente al Proveedor de soporte.	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
			Si la contingencia implementada no soporta la falta de disponibilidad del servicio de energía, se valida la activación de data Center y Oficina alterna.	
Presencia de fuego y/o humo en las áreas protegidas	Sistema de detección y extinción de Incendios. Centro de cómputo	El sistema cubre el área del centro de cómputo y de la UPS	<p>El centro de cómputo cuenta con su sistema de extinción de incendios propio, adicional al sistema administrado por la administración de la torre Head Office SIAP Bogotá (los aspersores de agua están deshabilitados del Datacenter y del Cuarto UPS, los sensores de humo están activos.). Se debe validar la activación automática de los sistemas de extinción, en caso negativo activar procedimiento manual de acuerdo a las instrucciones publicadas dentro del centro de cómputo.</p> <p>Si el fuego se extiende en la instalaciones validar plan de acción de activación de Data Center alternativo y Oficina Alterna</p>	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Caída del canal de Internet Level 3	Conexión VPN, Data Center Bogotá Internet	Soporta los servicios emisionales de enlace a Internet con el SIAP(SEOS, SGO, E-MAIL, COLSIN, SIGLO XXI, JQ, MUISCANET) y la salida a Internet	La compañía cuenta con otro proveedor CLARO en la Oficina principal. La Compañía cuenta con alta disponibilidad de sus canales con redundancia para Bogotá – DATA CENTER Colombia VX, en caso de caída subirá automáticamente el otro, sin que se vea afectado el servicio.	
Falla enlace principal Falta de disponibilidad de los recursos tecnológicos o de información	Conectividad Centro de cómputo oficina principal	Permite conectar el centro de cómputo en Bogotá y oficina principal	En caso de falla de los canales principales y alternos desde la Head Office Bogotá, La contingencia a desarrollar es Activación de Oficina Alterna.	
Falla enlace principal de internet “Level 3”, afectación de usuarios Head office SIAP.	No acceso y/o disponibilidad de aplicativos corporativos y información, servidor de archivos.	Permite la operatividad de estos elementos o sistemas	La compañía cuenta con un enlace a Internet con el proveedor CLARO en la Oficina principal. Que en caso de caída del canal principal y el	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Perdida de Sistema de Comunicaciones Unificadas los recursos tecnológicos o de información			redundante, se activara manualmente, permitiendo acceso a los servicios sin que se vea afectados los mismos.	
Falla fibra principal (Rompimiento o perdida física de cable) Perdida de disponibilidad de los recursos tecnológicos o de información	Conectividad Centro de cómputo oficina principal	Permite conectar el centro de cómputo en Bogotá y oficina principal	Se cuenta con una fibra alterna para re direccionar todo el tráfico hacia y desde el Data Center. Se cuenta con 2 enlaces en Bogotá (Level 3 y CLARO).	
Falla en Servicio DHCP Controlador de Dominio Equipos no reciben direcciones IP		Caída del servicio DHCP o apagado del servidor	Está configurado el servidor DHCP en modo Failover con el controlador alterno del proveedor LEVEL 3, Si se cae el DHCP de Bogotá, el Alternativo de Level 3 toma el rol principal de forma automática mientras el principal vuelve a subir. Se tiene backup mensual de la configuración del servicio DHCP.	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Caída del Controlador de Dominio Usuarios no pueden autenticarse a la red Wifi	Servicio Wifi acceso de dispositivos móviles a Intranet e Internet	Caída del servicio NPS o apagado del servidor	El servicio NPS no permite manejar Failover, esta implementado sobre el servidor de controlador de dominio. Se tiene backup semanal de la configuración. En caso de caída o apagado del servidor, se debe importar la configuración al servidor alternativo y cambiar la configuración de las controladoras WIFI para que apunte al nuevo servidor.	
Caída del Controlador de Dominio Usuarios no pueden autenticarse al dominio de SIAP Bogotá, salir a Internet o compartir información.	Servicio DNS	Caída del servicio DNS o apagado del servidor	El servicio DHCP está brindando de forma automática dos DNS a los equipos, en caso no se resuelva por el primero lo hace por el segundo. Se cuenta con dos servidores DNS, uno en Bogotá. Los servidores tienen configurados dos DNS de forma estática. El servicio DNS está integrado con el directorio activo.	
Caída del Controlador de Dominio Usuarios no reciben las	Servicios de políticas de GPO	Apagado del servidor o daño Sistema Operativo	Se cuenta con dos controladores de Dominio, uno en Bogotá y otro alternativo por el proveedor Level 3. Las políticas son replicadas entre los controladores de dominio internos y externos. Se tiene	Gerente de Datacenter

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
políticas de usuario, equipos no aplican directivas de SIAP Bogotá.			un backup mensual de todas las políticas de Grupo, en caso que una política esta corrupta se hace un restore, a la última operativa correctamente.	
Falla del Directorio Activo Controlador de Dominio Usuarios no pueden iniciar sesión en el dominio SIAP Bogotá, dispositivos de seguridad y red integrados con LDAP no brindan los servicios requeridos.		Apagado del servidor o daño Sistema Operativo	Se cuenta con dos controladores de Dominio, uno en Bogotá y otro alterno por el proveedor Level 3. Las políticas son replicadas entre los controladores de dominio internos y externos. Cada controlador maneja la base de datos de objetos del directorio activo, en caso que uno falle, el otro puede brindar las mismas funciones y servicios de usuarios y grupos. Los dispositivos de red y seguridad tienen configurados las IPs de los dos controladores, en caso no encuentre el primero, puede autenticarse con el segundo. Se tiene un backup mensual del System State que incluye toda la base del directorio activo y sus configuraciones.	
Falla en Herramienta de Gestión (SGO)	Servidor o Base de datos	Prestación de servicio para registro, gestión y seguimiento de	Restauración de backup con tiempos de indisponibilidad	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Perdida de disponibilidad de los recursos tecnológicos o de información		servicios en los clientes.	mientras se hace la restauración	
Falla en Herramienta de Gestión (SIGLO XXI)	Servidor o Base de datos	Prestación de servicio para registro, gestión y seguimiento de compras, contabilidad, tesorería, ventas	Colocar en marcha maquinas replicadas en Data Center	
Falla en Herramienta de Gestión (JQ)	Servidor o Base de datos	Prestación de servicio para registro, gestión y seguimiento de servicios en los clientes.	La Herramienta tiene alta disponibilidad en VMWare con otro servidor en Bogotá, si la falla es total se replica en otro de los servidores de Bogotá. Mientras se repara o restaura la maquina física.	
Falla en Herramienta de Gestión (SEOS)	Servidor o Base de datos	Prestación de servicio para registro, gestión y seguimiento de servicios en los clientes.	Restauración de backup con tiempos de indisponibilidad mientras se hace la restauración	
Falla en el Portal Web de Servicio	Aplicación WEB	Prestación de servicio de soporte y seguimiento a	La Herramienta tiene alta disponibilidad en VMWare con otro servidor en Bogotá,	Gerente del Centro de Datos

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
		usuario interno y externo	si la falla es total se replica en los servidores de Bogota.	

• **Escenario 4:** Acceso Nulo a las instalaciones Head Office SIAP Bogotá/Limitación de Personal o evacuación del edificio (Con funcionamiento del centro de datos): el incidente ocasionó que el personal no tenga acceso a la Head Office Bogotá o las instalaciones fueron evacuada, pero los Centros de Cómputo no han sufrido daños y continúan operando de manera normal.

Tabla 11. Plan de contingencia del escenario 4

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
<ul style="list-style-type: none"> Desastre natural como sismos que ocasionan fuertes daños en la infraestructura de las oficinas Inundaciones que no afectan el centro de cómputo, por lo tanto los sistemas operan con normalidad pero sin acceso a las oficinas 	Oficina Alternativa con equipos para operar en contingencia	La oficina cuenta con una cantidad de equipos limitada para dar prioridad a las operaciones críticas	<ul style="list-style-type: none"> Verificación de la disponibilidad de información en el Centro de Cómputo. Activar el canal de internet alternativo de dicha oficina. Habilitar las oficinas alternas con los respectivos equipos de cómputo y comunicaciones. Acceder a los sistemas de información Realizar pruebas sobre los sistemas de información 	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Presencia de fuego y/o humo en las áreas protegidas	Sistema de detección y extinción de Incendios. Centro de cómputo	El sistema cubre el área del centro de cómputo y de la UPS	El centro de cómputo cuenta con su sistema de extinción de incendios propio, adicional al sistema administrado por la administración de la torre Head Office SIAP Bogotá (los aspersores de agua están deshabilitados del Datacenter y del Cuarto UPS, los sensores de humo están activos.). Se debe validar la activación automática de los sistemas de extinción, en caso negativo activar procedimiento manual de acuerdo a las instrucciones publicadas dentro del centro de cómputo. Si el fuego se extiende en la instalaciones validar plan de acción de activación de Data Center alternativo y Oficina Alternativa	

- Escenario 5:** Acceso limitado a las instalaciones Head Office SIAP Bogotá/Limitación de Personal o evacuación del edificio (Sin funcionamiento del centro de datos): el incidente ocasionó que el personal tenga acceso limitado a los puestos disponibles en la Head Office Bogotá o que las instalaciones fueron evacuadas, y la disponibilidad de los Centros de Cómputo no están operando normalmente.

Tabla 12. Plan de contingencia del escenario 5

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
<ul style="list-style-type: none"> Desastre natural como sismos que ocasionan fuertes daños en la infraestructura de las oficinas Inundaciones que afectan el centro de cómputo, por lo tanto los sistemas están inoperables Presencia de fuego y/o humo en las instalaciones, por lo tanto no es posible el acceso a las oficinas y el centro de datos está inoperable 	Oficina Alternativa con equipos para operar en contingencia. Datacenter Alternativo	La oficina cuenta con una cantidad limitada de equipos para dar prioridad a las operaciones críticas	<ul style="list-style-type: none"> Enrutamiento y activación de las comunicaciones hacia el Centro de Cómputo Alternativo. Activación servicio de controladores de dominio y sistema operativo en servidores Activación servicio de bases de datos y aplicaciones Activar el canal de internet alternativo de dicha oficina. Restauración de Backups, en caso de pérdida de información Habilitar las oficinas alternas con los respectivos equipos de cómputo y comunicaciones. Acceder a los sistemas de información Realizar pruebas sobre los sistemas de información 	

En el marco del plan de contingencia relacionado con fallas en la infraestructura, a continuación se presentan los escenarios que pueden llegar a afectar los recursos tecnológicos frente a la seguridad de la información. Con el objeto de garantizar la preservación de la confidencialidad, integridad y disponibilidad de los activos de información, se indican las acciones y los responsables frente a cada escenario elemento o sistema identificado.

Tabla 13. Plan de contingencia – Seguridad de la información

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
Daño del File Server Soft errors o Falla de disco Falta de Disponibilidad de los recursos tecnológicos o de información	Discos SAS 600GB-NL 2TB	Por uso normal o utilización continua del disco, circuitos quemados o daños en los componentes internos de la unidad, aumentos excesivos de temperatura, errores de SW, entre otras, se pueden presentar errores o fallas en disco que obliguen al cambio del mismo.	Migrar la información del disco que falla al disco de respaldo de la configuración Raid Migrar al disco de respaldo de la política HotSpare (1*30) Connecthome para envió alertas a los correos de relay configurados para cada equipo, para reacción inmediata. Actividad transferida soporte del data Center de LEVEL 3 para cambio. Abrir caso para envió de parte o cambio de Disco(S.Premium) Backup Completo de File Server en caso extremo de pérdida de información del disco.	
Daño del File Server Falla de red de HW o lógica en un SP (tecnología de AH)	Storage Procesor	El equipo cuenta con 2 Storage Procesor y dos rutas de red para alta disponibilidad, el cual puede presentar fallas de red, cableado, o daño físico o lógico en un Procesador.	En caso de falla de un procesador el secundario realiza failover y se mantiene el servicio, asumiendo la carga sin presentar indisponibilidades. Connecthome para envió alertas a los correos de relay configurados para cada equipo, para reacción inmediata. Soporte Proactivo de EMC para	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
			soporte o cambio de la parte. Abrir caso para envío de parte o cambio de Disco(S.Premium)	
Falla de File Server Fallo HW DataMover	DataMover	El equipo cuenta con 1 DataMover el cual no se encuentra el AH	No se tiene segundo DM para AH, sin embargo para ello está respaldado el file Server con un RPO de 24 horas por medio de Level 3 y una retención de 30 días.	
Falla File Server Pérdida parcial de archivos Perdida de Disponibilidad de los recursos tecnológicos o de información	Archivos del File Server	Por la mala manipulación de usuarios, se eliminan, se sobre escriben o se depuran archivos equivocados	Se realiza restauración parcial desde solución de Backup LEVEL 3, en sitio origen o en otra ubicación del File Server de acuerdo a la necesidad del usuario Control de accesos con grupos de seguridad para permisos.	
Bloqueo Firewall ASA (Principal)	Firewall ASA 5525X con servicios de Firepower Versión IOS 9.2.2(4)	SERVICIOS AFECTADOS Todas las conexiones donde interfiere el firewall para servicios Internos y Externos además de: * Conexión a nivel de enrutamiento Conexión a internet *Reglas de NAT	Se cuenta con un esquema de Alta Disponibilidad configurado entre dos equipos Cisco ASA, al afectarse el principal, se activa el módulo secundario, dando así continuidad a los servicios internos y externos.	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
		*Servicios VPN usuarios SIAP BOGOTA *Servicio de Internet de Usuarios de red * Servicios de Correo desde Oficina SIAP Bogotá		
Bloqueo Firewall ASA (Principal y Secundario).	Firewall ASA 5525X con servicios de Firepower Versión IOS 9.2.2(4)	SERVICIOS AFECTADOS Conexión a nivel de enrutamiento •Servidor Correo •Red Interna *Conexión a internet *Reglas de NAT •Servicios VPN usuarios •Servicios de internet para los usuarios	<p>Los servicios internos de La Compañía se alcanzaran de forma manual en la sede de Alterna, por medio del canal que existe entre las dos ciudades enrutado por medio de los Nexus. Se tendrá un tiempo de respuesta de 2 horas para recuperar los servicios principales</p> <p>Al fallar los dos Firewall se procede a realizar los siguientes pasos en el módulo primario para recuperar el servicio en dos (2) horas:</p> <ul style="list-style-type: none"> •Actualización del IOS del módulo primario, versión 9.0 (1) a la versión 9.2 (2)4. •Restauración del Backup de Configuración del módulo principal. <p>Al recuperar el servicio con el módulo principal se procede a realizar los pasos relacionados anteriormente en el módulo secundario y se realiza la</p>	

Incidente	Elemento / Sistema	Descripción	Acciones	Responsable
			<p>configuración de la Alta Disponibilidad.</p> <p>Se realizarán las pruebas correspondientes:</p> <ul style="list-style-type: none"> •Pruebas de red con los clientes afectados. •Pruebas de servicios de internet a diferentes páginas. •Pruebas de Failover, apagando el Firewall Active. •Pruebas de publicación de servicios con CA 	

9.5. Fase de Restauración (Plan de retorno a la normalidad)

La meta de la recuperación y restauración es recobrar la operatividad de la organización manteniendo la entrega de productos y servicios críticos. En esta etapa se incluyen las siguientes actividades:

9.5.1. Decidir donde reiniciar operaciones

Es necesario establecer si las facilidades estropeadas se pueden reparar o si es necesario mantenerse en el sitio alternativo. Lo anterior deberá decidirse entre el Coordinador del DRP, el Gestor de Incidentes y el equipo de contingencia.

9.5.2. Adquirir los recursos adicionales para restaurar por completo la operación.

El Coordinador del DRP y el Gestor de incidentes establecerán apoyándose en las Gerencias y áreas de apoyo, qué se requiere para reparar las facilidades estropeadas a nivel de

recursos económicos y de personal y presentarán al equipo de contingencia sus estimados y tiempos para realizarlo.

9.6. Regreso del personal a las instalaciones

9.6.1. Restablecer las operaciones normales de la organización.

Con el personal operando en las instalaciones recuperadas, el coordinador del DRP con el apoyo del Gestor de Incidentes, procederán a evaluar y monitorear la entrega de los servicios afectados con el objetivo de en el menor tiempo posible, llegar a los niveles de entrega anteriores a la interrupción

9.6.2. Reanudación de las operaciones en los niveles anteriores a la interrupción

Al conseguir operar a los niveles previos a la interrupción el coordinador del DRP y el Gestor de Incidentes notificarán al Equipo el retorno a normalidad en la entrega de los servicios afectados vía correo electrónico y por este mismo medio se procederá con la notificación a los clientes afectados por la interrupción. Los líderes de frente tienen la responsabilidad de informar a cada cliente afectado.

CONCLUSIONES

- El análisis de riesgos, brindo a la organización un conocimiento de las debilidades y compromisos que la empresa afronta en el desarrollo de las actividades del negocio, permitió evaluar el conocimiento del entorno y del interior de la entidad e identificar la condición en la que se encuentra la compañía para afrontar una situación de desastre.
- Con el análisis de riesgos, se logra determinar la criticidad de la tecnología en la organización, permitiendo identificar y evaluar la exposición de los activos de información frente a situaciones de riesgo, para proceder a diseñar una estrategia que permita la protección de los mismos.
- El análisis de Impacto en el Negocio (BIA), permite priorizar los procesos críticos de tecnología en las áreas de negocio, los recursos requeridos para soportar la operación e identificar los tiempos mínimos y máximos tolerables de recuperación de los activos de información para la organización.
- El análisis de Impacto en el Negocio (BIA) para la Compañía SIAP Nivel 1, permitió identificar los componentes esenciales como: personal requerido, aplicativos críticos, dependencias de otras áreas, dependencia de terceros, criticidad de los recursos de información, indispensables para llevar a cabo un DRP y poder brindar continuidad a la operación de tecnología que soportan las demás áreas del negocio.
- Las estrategias de recuperación propuestas en este plan de recuperación de desastres (DRP), le da a la organización un marco o referente para responder de manera sistemática y organizada a la materialización de un escenario de desastre ajustándose a la infraestructura de TI y los procesos de negocio de la organización.

- Al diseñar el Plan de recuperación de desastres (DRP) para la Agencia de Aduanas Profesional Siap Nivel 1 se identificó que los activos de información de la dirección de tecnología se encuentran en un alto nivel de exposición frente a un desastre y que puede ocasionar una interrupción en sus operaciones, por lo tanto se considera importante e indispensable que la compañía implemente un DRP estructurado y organizado teniendo en cuenta los riesgos evidenciados y la criticidad de las operaciones de negocio.

REFERENCIAS

- SANS Institute Disaster Recovery Plan Strategies and Processes Febrero 2002
- SANS Institute Disaster Recovery Plan. Cycle The Plan, Plan the Cycle. Febrero 2002
- NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems. Mayo de 2010
- CISCO Systems. White_paper_c11-453495 Disaster Recovery: Best Practices. Agosto 2008.
- Guía de recuperación ante desastres en Pymes usando computación en la nube. Departamento de Ciencias de la Computación; Escuela Politécnica del Ejército, Sangolquí, Ecuador.
- Computerworld. (2011). La nube computacional un modelo de aprovechamiento de infraestructura que avanza para quedarse. Ediworld, Ed. Computerworld Ecuador (230), 19-21.
- Disaster Recovery. (2012). Disaster Recovery. Recuperado el 12 de Abril de 2012, de <http://www.disasterrecovery.org/index.html>
- Torres, D. (1998). Metodología para la preparación de un plan de recuperación de aplicaciones críticas y datos en casos de desastre. Tesis. EPN. Quito, Ecuador.
- Vision Solutions. (2008). La guía fundamental para la recuperación de desastres: Cómo garantizar la continuidad en equipos informáticos y actividades comerciales. Whitepaper, Irvine, California. EE.UU.
- <http://www.eoi.es/blogs/nataliasuarez-bustamante/2012/02/11/%C2%BFque-es-el-metodo-delphi/>

- Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. (2010). Contingency Planning Guide for Information Technology Systems. Estados Unidos: National Institute of Standards and Technology.
- Jim Hoffer. (2001). Plan de recuperación ante desastres. 2001, de Synertech, Harrisburg, PA
Sitio web: https://es.wikipedia.org/wiki/Plan_de_recuperación_ante_desastres
- Pintos Fernández, Joaquín. Auditorías y continuidad de negocio (UF1895). Madrid, ES: IC Editorial, 2014. ProQuest ebrary.
- Jairo Romero, Jennifer Ramírez. (2013). Diseño e implementación de un prototipo que permita el despliegue de un plan de recuperación de desastres aplicable a empresas mipymes colombianas. Bogotá: Universidad Católica de Colombia.
- María Alejandra Castaño, Cristhian Ortégón. (2015). Diseño de un plan de recuperación de desastres en el área de tecnologías de la información para la fundación neumológica colombiana. Bogotá: Fundación Universitaria los Libertadores.

APÉNDICE A

- Plantilla_BIA_2016 - Dirección administrativa.xlsx
- Plantilla_BIA_2016 - Dirección Operativa.xlsx
- Plantilla_BIA_2016 - Dirección TI.xlsx
- Plantilla_BIA_2016 – Dirección Comercial.xlsx

APÉNDICE B

- Análisis proceso gestión comercial.xlsx
- Análisis proceso dirección administrativa.xlsx
- Análisis proceso exportaciones.xlsx
- Análisis proceso importaciones.xlsx
- Matriz riesgos dirección tecnología.xlsx