**PROYECTO SEGURIDAD EN BASES DE DATOS**

**APLICANDO NIST PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN A LAS BASES DE DATOS**

**LORENA OCAMPO CORREA**

**EDWIN FERNEY MEDINA ROJAS**

**EDINSON QUINTANA HERNANDEZ**

**ANGÉLICA MARÍA MARTÍN RAMÍREZ**

**UNIVERSIDAD PILOTO DE COLOMBIA**

**DIRECCIÓN DE POSTGRADOS**

**MSIC1 - MAESTRÍA DE SEGURIDAD INFORMÁTICA Y COMUNICACIONES BOGOTÁ, D.C.**

**2019**

CONTENIDO

pág.

INTRODUCCIÓN 11

CRONOGRAMA 12

[1 OBJETIVOS](#_Toc245004002) 13

1.1 OBJETIVO GENERAL 13

1.2 OBJETIVOS ESPECÍFICOS 13

[2 MARCO TEÓRICO](#_Toc245004006) 14

[2.1 DESCRIPCIÓN GENERAL DEL MARCO](#_Toc245004006)  14

[2.2 NIVELES DE IMPLEMENTACIÓN](#_Toc245004006)  17

[2.3 PERFIL DEL MARCO](#_Toc245004006)  18

[2.4 COMUNICACIÓN DE LOS REQUISITOS DE CIBERSEGURIDAD CON LOS INTERESADOS 19](#_Toc245004006)

[3 ID.BE IDENTIFICAR](#_Toc245004006)  21

3.1 ID. AM GESTIÓN DE ACTIVOS 21

3.1.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN 21

3.1.2 ROLES Y RESPONSABILIDADES 21

3.1.3 CRITERIOS DE CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN 22

3.1.3.1 Criterios de clasificación 22

3.1.3.2 Criterios de valoración 25

3.1.4 METODOLOGÍA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN 25

3.1.4.1Identificación de los activos de información 26

3.1.5 RESULTADOS LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN PARA

SOLUCIONES S.A.S 28

3.1.5.1 Descripción de activo crítico soluciones S.A.S 28

3.2 ID.BE ENTORNO EMPRESARIAL 32

3.2.1 ESTABLECIMIENTO DE CONTEXTO 32

3.2.1.1 ID.BE-1 32

3.2.1.2 ID.BE-2 32

3.2.1.3 ID.BE-3 34

3.2.1.4 ID.BE-4 34

3.3 ID. GV GOBERNANZA 36

3.3.1 ID. GV-1 36

3.3.2 ID. GV-1-3 36

**3**.3.2.1 Requisitos legales Colombia 36

3.3.2.2 Requisitos Internos 38

3.4 ID.RA EVALUACIÓN DE RIESGOS 38

3.4.1 GESTIÓN DE RIESGOS SOBRE LOS ACTIVOS DE INFORMACIÓN 38

# 3.4.1.1 Nivel aceptable de los riesgos 42

# 3.4.1.2 Metodología para el análisis de riesgos de soluciones S.A.S 42

3.4.1.2.1 Análisis 43

3.4.1.2.2 Identificación de Amenazas y Vulnerabilidades 43

3.4.1.2.3 Valoración del Riesgo Inherente 44

3.4.1.2.4 Identificaciones de controles 46

3.4.1.2.5 Valoración Del Riesgo Residual 46

3.5 ID.RM ESTRATEGIA DE GESTIÓN DE RIESGOS 47

3.5.1 ACEPTACIÓN DEL RIESGO 47

3.5.2 REVISIÓN POR LA DIRECCIÓN 48

3.5.3 TRATAMIENTO 48

3.5.3.1 Planes de tratamiento 48

3.5.3.2 Seguimiento 48

3.5.4 RESULTADOS ANÁLISIS DE RIESGOS BASADO EN ACTIVOS DE INFORMACIÓN PARA SOLUCIONES S.A.S 49

4 PR PROTEGER 51

4.1 PR.AC-4 51

BIBLIOGRAFIA 53

LISTAS DE CUADROS

Cuadro 1. Núcleo del Marco NIST: Categorías, subcategorías y referencias normativas

Cuadro 2. Categoría de función y de identificadores únicos (Versión 1.1)

Cuadro 3. Niveles de implementación del marco (Tiers)

Cuadro 4. Criterios de Clasificación según la Confidencialidad

Cuadro 5. Criterios de Clasificación según la Disponibilidad e Integridad

Cuadro 6. Inventario Activos de Información Tipo BD SOLUCIONES S.A.

Cuadro 7. Administración Empleados

Cuadro 8. Administración Departamentos

Cuadro 9. Departamentos

Cuadro 10. Títulos

Cuadro 11. Empleados

Cuadro 12. Salarios

Cuadro 13. Matriz FODA SOLUCIONES S.A.S.

Cuadro 14. Cuadro de Resultados de la Matriz FODA

Cuadro 15. Zonas de Aceptación de Riesgo

Cuadro 16. Probabilidad del Riesgo

Cuadro 17. Impacto del Riesgo

Cuadro 18. Calificación de las Zonas de Riesgo

Cuadro 19. Valoración del Control

Cuadro 20. Acción que seguir en el Plan de Tratamiento según la Clasificación del Riesgo

Cuadro 21. Resumen Análisis de Riesgos de Seguridad de la Información del activo tipo BD crítico para SOLUCIONES S.A.S.

Cuadro 22. Roles BD Empleados

**LISTAS DE FIGURAS**

Figura 1. Núcleo del Marco

Figura 2. 5 funciones continuas

Figura 3. Descripción Funciones, categorías, subcategorías y referencias normativas

Figura 4. Funciones NIST

Figura 5. Funciones NIST Arquitectura del marco de trabajo de ciberseguridad

del NIST (CSF)

Figura 6. Método para su implementación

Figura 7. Gestión de los Activos de Información

Figura 8. Reconocimiento Activos de Información

Figura 9. Modelo ER BD Empleados

Figura 10 Comunicaciones y flujos de datos BD Empleados

Figura 11. Figura para Gestión de Riesgos ISO 27005

Figura 12. Gestión de los Riesgos de Seguridad de la Información

Figura 13. Zonas de Riesgo Aceptable e Inaceptable

**GLOSARIO**

**ACEPTACIÓN DEL RIESGO:** Decisión de asumir un riesgo.

[Guía ISO/IEC 73:2002]

**ACTIVO:** Cualquier cosa que tenga valor para la organización. Entre los activos de la organización se encuentra hardware, software, el talento humano, documentos, sistemas de información, bases de datos, archivos, portales, etc.

[NTC 5411-1:2006]

**AMENAZAS:** Se entiende por amenaza, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo de seguridad de la información. Son amenazas el talento humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Las amenazas en un contexto de seguridad de la información, incluyen actos dirigidos, deliberados (por ejemplo por crackers) y sucesos no dirigidos, aleatorios o impredecibles (como puede ser un rayo). Amenaza es la causa de riesgo que crea aptitud dañina sobre personas y bienes.

[ISO/IEC 27005:2008]

**ANÁLISIS DE RIESGO:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[Guía ISO/IEC 73:2002]

**ASUMIR EL RIESGO:** Cuando el costo del manejo del riesgo no se justifica, usualmente porque la probabilidad y/o las consecuencias son bajas o al darle un tratamiento al riesgo ya sea reduciéndolo o transfiriéndolo y queda un riesgo residual cuya probabilidad e impacto son mínimos, se puede asumir dicho riego, asegurando su monitoreo constante.

[ISO/IEC 27005:2008]

**CONFIDENCIALIDAD:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[NTC 5411-1:2006]

**CONTROLES:** Medidas dispuestas para reducir el nivel de riesgo, tales como políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal[ISO/IEC 27005:2008]

**DATO:** Representación convencional de un hecho o idea que puede ser tratada por un ordenador.

[ISO/IEC 27005:2008]

**DISPONIBILIDAD:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada cuando esta la requiera.

[NTC 5411-1:2006]

**EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

[ISO IEC TR 18044:2004]

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

[ISO IEC TR 18044:2004]

**INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

[NTC 5411-1:2006]

**MITIGAR EL RIESGO:** cuando se decide prevenir o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo a un nivel aceptable. Se consigue por ejemplo, mediante la optimización de los procedimientos, la implementación de controles, fortalecimiento del ejercicio del autocontrol, fortalecimiento del ejercicio de la autoevaluación de la gestión, las auditorías internas, etc. Existen dos formas de reducir el riesgo: prevenir, que apunta a la disminución de la probabilidad o proteger.

**NO REPUDIO:** Condición en la que quien envía un mensaje o realiza una operación con los sistemas de información no puede negar la validez del resultado del proceso que se utilizó para autenticar la información.

[ISO/IEC 27005:2008]

**REQUERIMIENTOS LEGALES:** Si la información está asociada al personal, a la compañía o alguna ley privada; esta debe ser clasificada.

[ISO/IEC27005:2008]

**RIESGO:** Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas o de imagen por deficiencias, fallas o inadecuaciones, en el talento humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

[ISO/IEC 27005:2008]

**RIESGO DE PÉRDIDA:** Si la información es sensible para la compañía y la pérdida de este activo acarrea implicaciones económicas, de imagen o legales para la compañía.

[ISO/IEC 27005:2008]

**SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas**.**

[NTC ISO/IEC 17799:2006]

**SENSITIVIDAD:** Información con contenido crítico para la compañía.

[ISO/IEC 27005:2008]

**TRANSFERIR EL RIESGO:** Cuando se decide traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las transferencias parciales son conocidas como COMPARTIR el riesgo. La distribución o localización del riesgo en diversos lugares se conoce como DISPERSIÓN o ATOMIZACIÓN del riesgo.

[ISO/IEC 27005:2008]

**VALOR:** El valor es el criterio más utilizado para clasificar la información. Si la información es importante para la organización o sus competidores, debe ser clasificada.

[IS/IEC 27005:2008]

**VULNERABILIDAD:** Es el grado de debilidad de un activo frente a una amenaza, la capacidad que tiene la amenaza de afectar el activo.

[ISO/IEC 27005:2008]

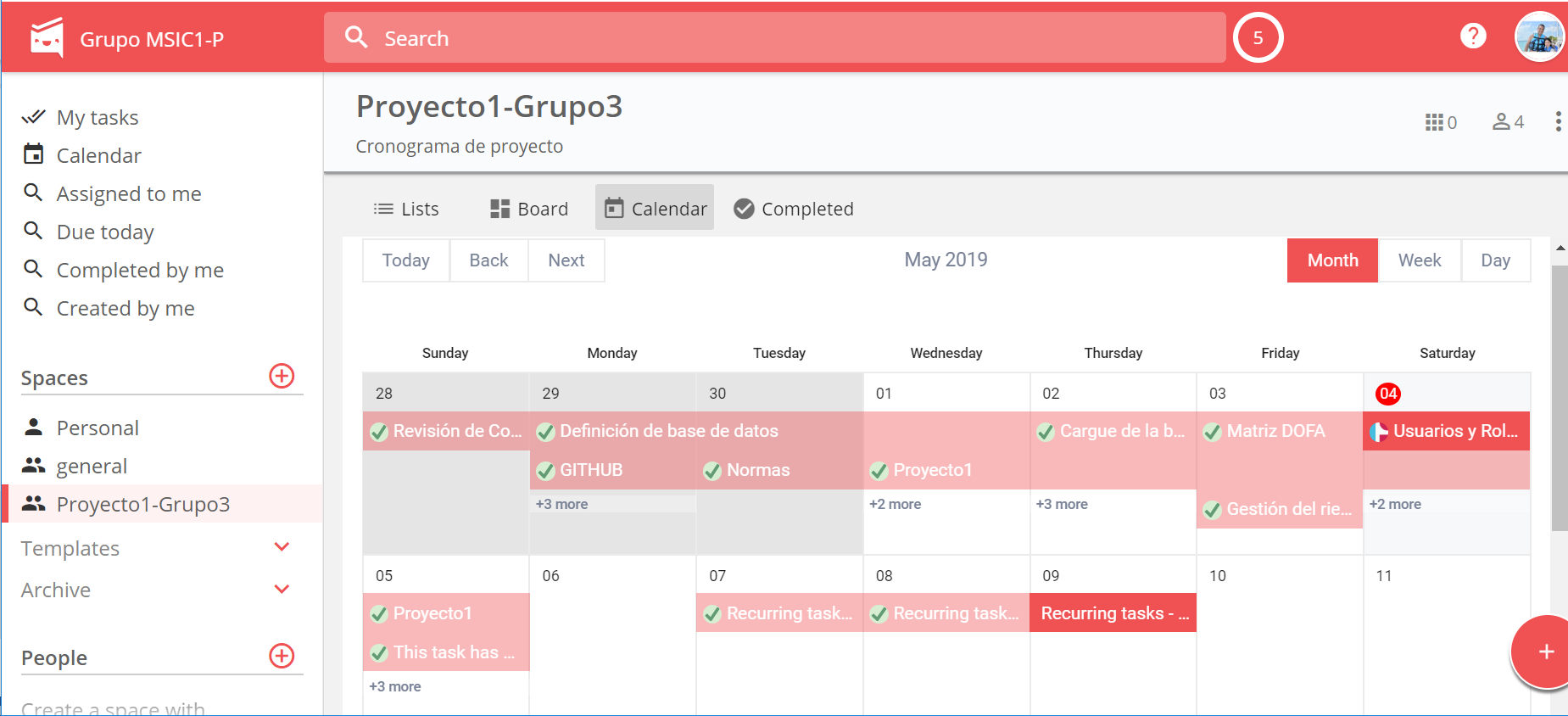
INTRODUCCIÓN

El aseguramiento de la información y de los sistemas que la procesan es un objetivo de primer nivel para cualquier organización, por lo que es necesario establecer diferentes controles para lograr una adecuada administración; velando por el cumplimiento de los principios de disponibilidad, integridad y confidencialidad de la información.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad, cumpliendo con los estándares de calidad.

Este trabajo tiene como finalidad realizar el aseguramiento de la base de datos principal de la compañía *SOLUCIONES S.A.S*.**,** una compañía que ofrece soluciones de productos software;el cual se desarrollará aplicando los conocimientos adquiridos por los autores en la asignatura Seguridad en Bases de Datos de la Maestría de Seguridad Informática y Comunicaciones y en el campo laboral sobre las líneas de gestión de seguridad de la información y administración de bases de datos.

CRONOGRAMA



|  |  |
| --- | --- |
|  |  |

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Aplicar el framework de Ciberseguridad planteado por la NIST a una base de datos de una organización de modo que se protejan su integridad, disponibilidad y confidencialidad.

1.2 OBJETIVOS ESPECÍFICOS

Identificar los datos y su criticidad para definir las variables de control a implementar, mediante un análisis de riesgos.

Alinear a la organización con las directrices en materia de protección de datos personales, para dar cumplimiento a la regulación a nivel nacional.

2 MARCO TEÓRICO

El Instituto Nacional de Normas y Tecnología, es una agencia perteneciente al Departamento de Comercio de los Estados Unidos, el cual, tiene por misión la promoción, innovación y la competencia industrial en Estados Unidos mediante avances en normas y tecnologías.

**2.1 DESCRIPCIÓN GENERAL DEL MARCO**

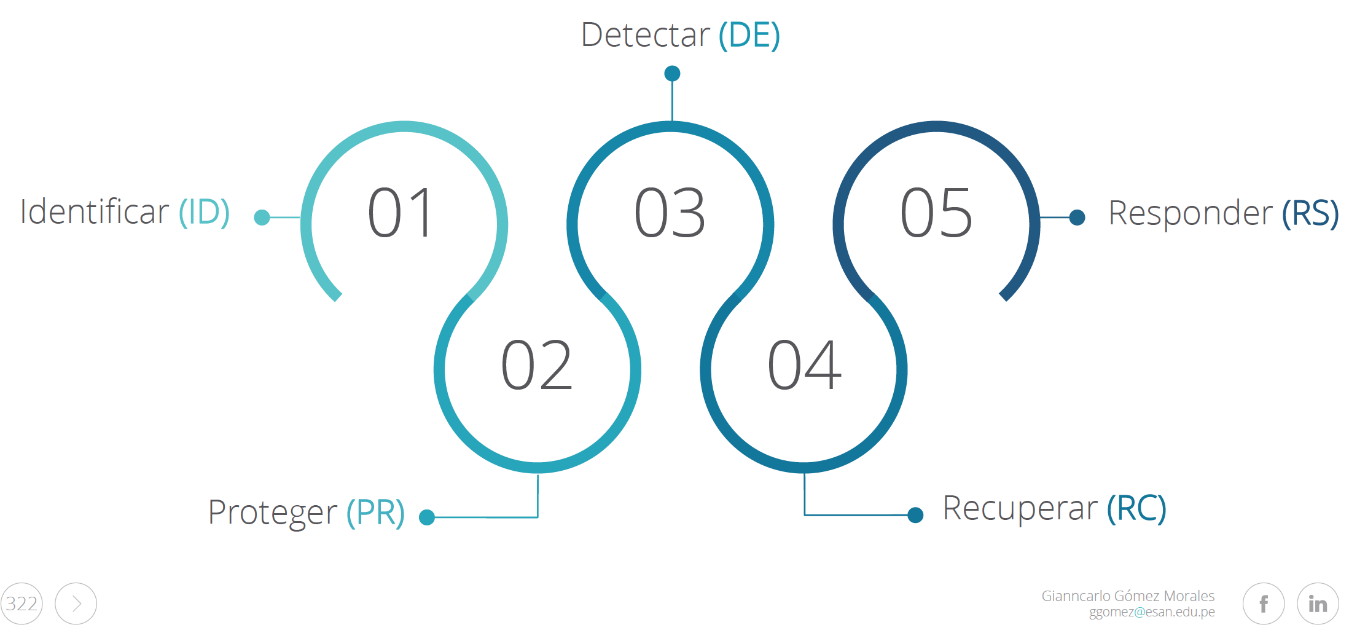
El Marco se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos de ciberseguridad como parte de los procesos de gestión de riesgos de la organización. El Marco consta de tres partes: el Marco básico, el perfil del marco y los Niveles de implementación del marco.

El Framework Core es un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica (Funciones, Categorías y Sub categorías), proporcionando la orientación detallada para el desarrollo de perfiles individuales de la organización. Mediante el uso de los Perfiles, el Marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Los Tiers proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

**Figura 1**. Núcleo del Marco.

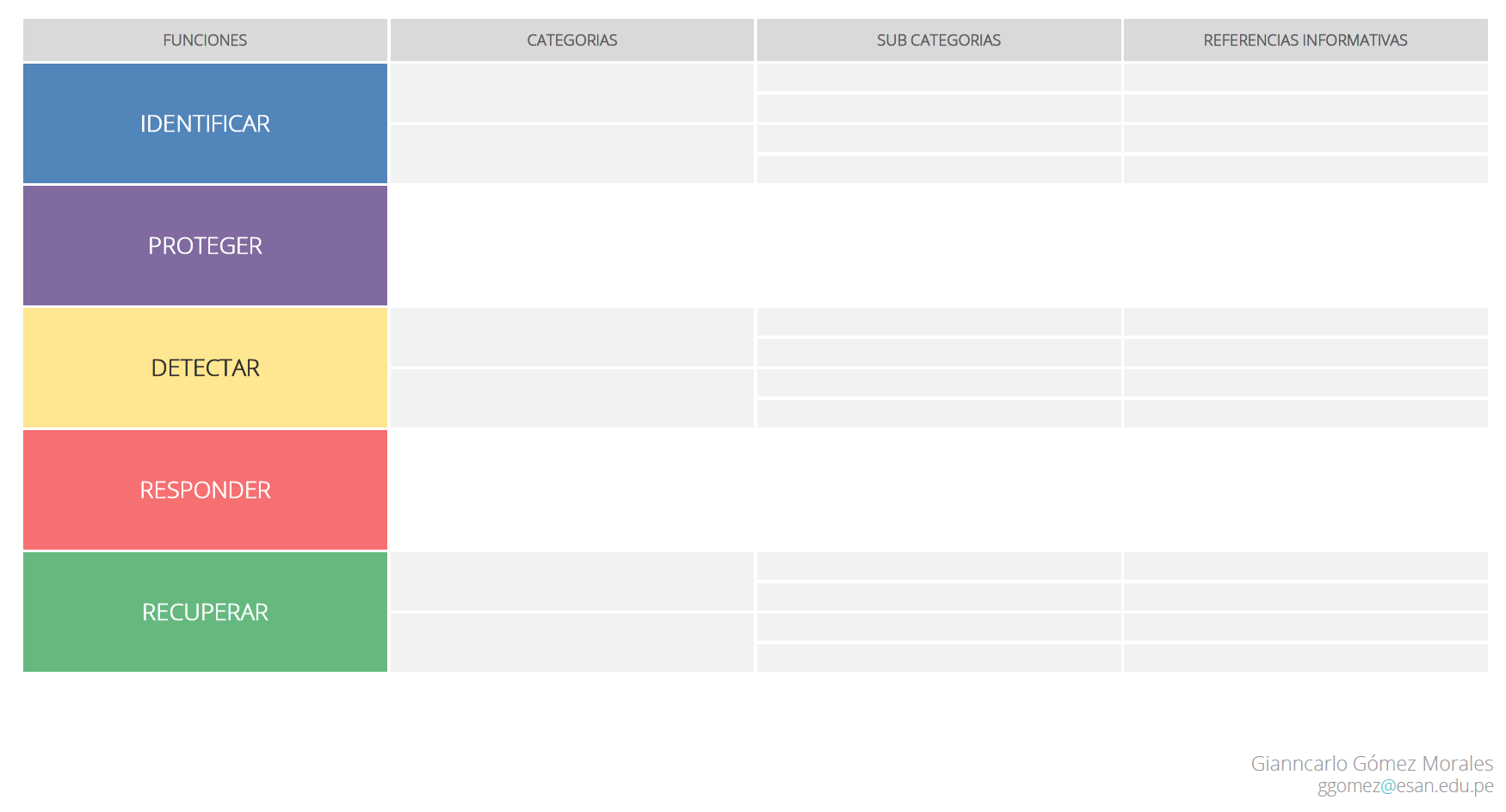


**Figura 2.** 5 funciones continuas.



El núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados. El núcleo no es una lista de comprobación de las acciones a realizar. Presenta los resultados clave de ciberseguridad identificados por la industria como útiles para gestionar el riesgo de ciberseguridad. El núcleo comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

**Cuadro 1.** Núcleo del Marco NIST: Categorías, subcategorías y referencias normativas.



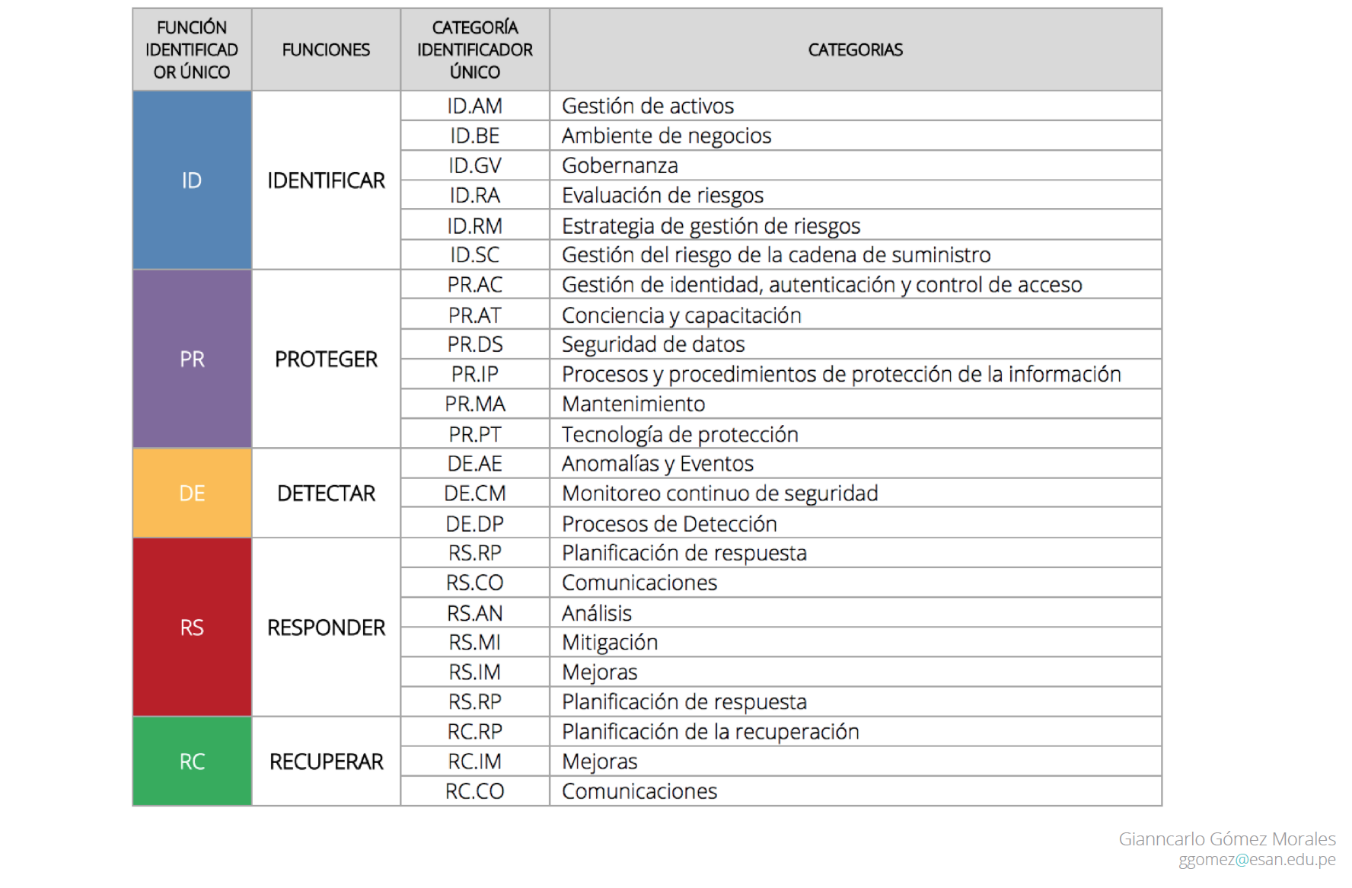
**Figura 3.** Descripción Funciones, categorías, subcategorías y referencias normativas.



**Figura 4.** Funciones NIST.



**Cuadro 2.** Categoría de función y de identificadores únicos (Versión 1.1).

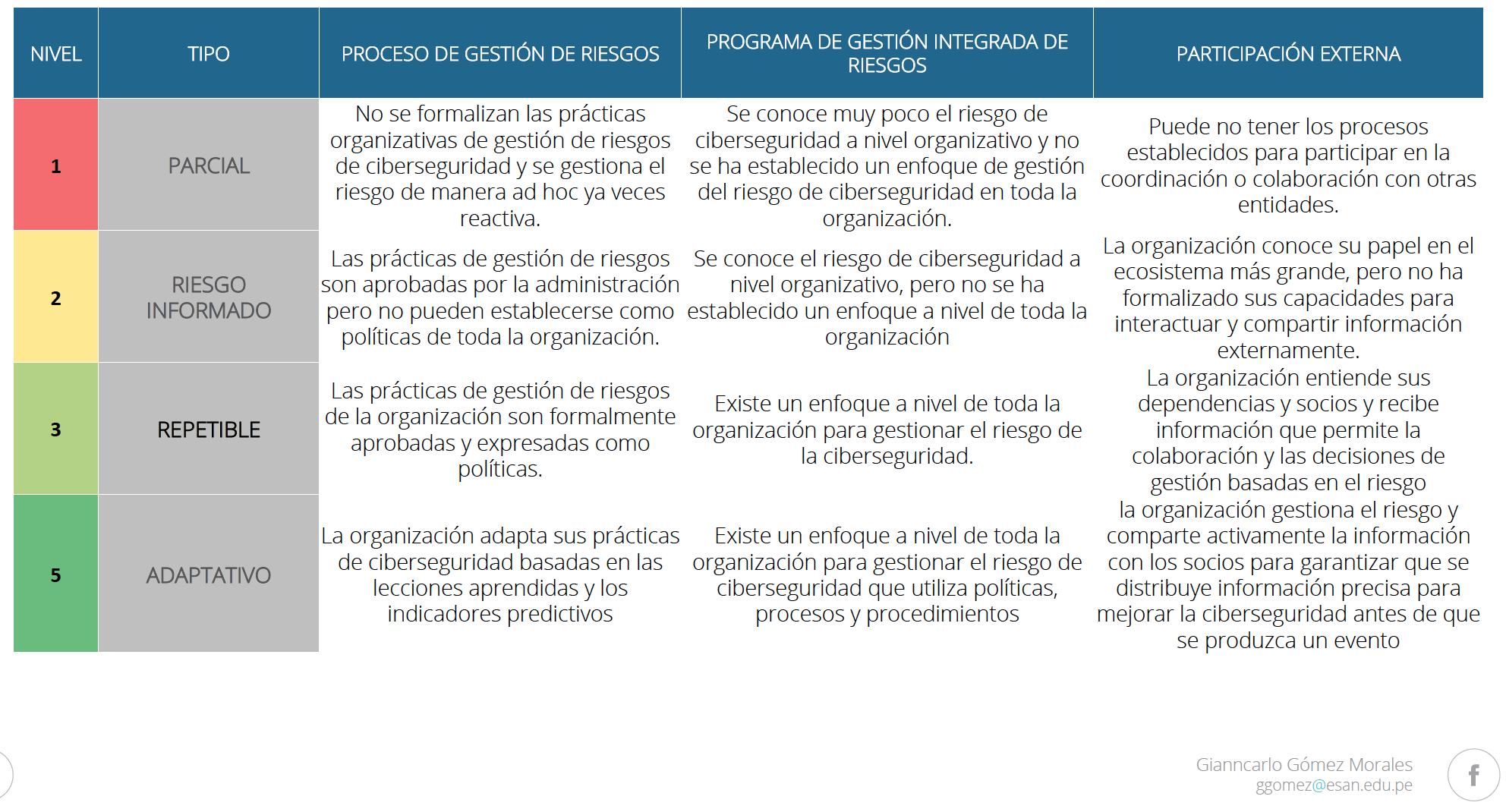


**2.2 NIVELES DE IMPLEMENTACIÓN**

Los niveles de implementación del marco ("Tiers") proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad y los procesos implementados para manejar ese riesgo. Las escalas describen el grado en que las prácticas de gestión de riesgo de ciberseguridad de una organización exhiben las características definidas en el Marco (por ejemplo, riesgo y amenaza, repetible y adaptable).

Los Tiers caracterizan las prácticas de una organización en un rango, desde Parcial (Tier 1) hasta Adaptativo (Tier 4). Estos niveles reflejan una progresión desde respuestas informales y reactivas a enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un Tier, una organización debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización.

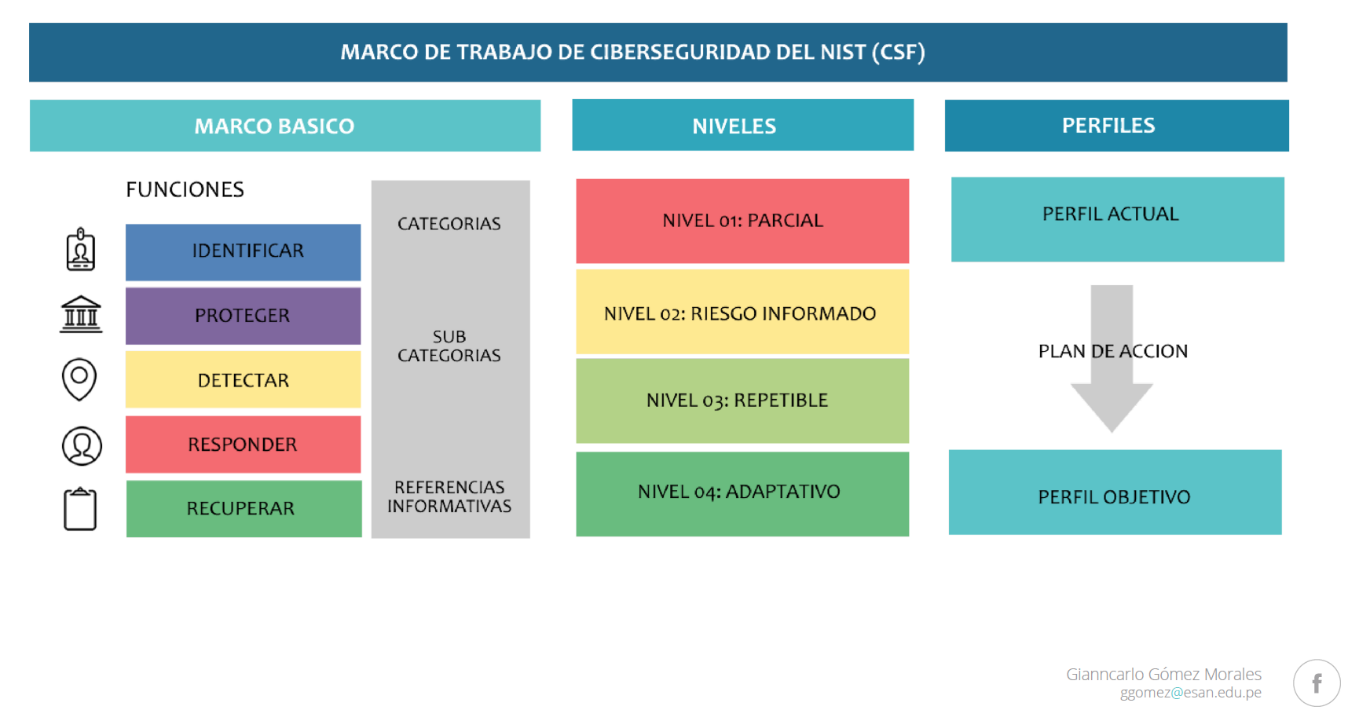
**Cuadro 3.** Niveles de implementación del marco (Tiers).



**2.3 PERFIL DEL MARCO**

Perfil del Marco representa los resultados basados en las necesidades empresariales que una organización ha seleccionado de las Categorías y Subcategorías. El Perfil puede caracterizarse como la alineación de estándares, directrices y prácticas con el Framework Core en un escenario de implementación particular. Los perfiles pueden ser utilizados para identificar las oportunidades para mejorar la postura de ciberseguridad mediante la comparación de un perfil "actual" (el estado "tal cual") con un perfil "destino" (el estado "ser"). Para desarrollar un Perfil, una organización puede revisar todas las Categorías y Subcategorías y, sobre la base de los impulsores del negocio y una evaluación del riesgo, determinar cuáles son los más importantes; pueden añadir categorías y subcategorías, según sea necesario para hacer frente a los riesgos de la organización.

**Figura 5.** Funciones NIST Arquitectura del marco de trabajo de ciberseguridad del NIST (CSF).

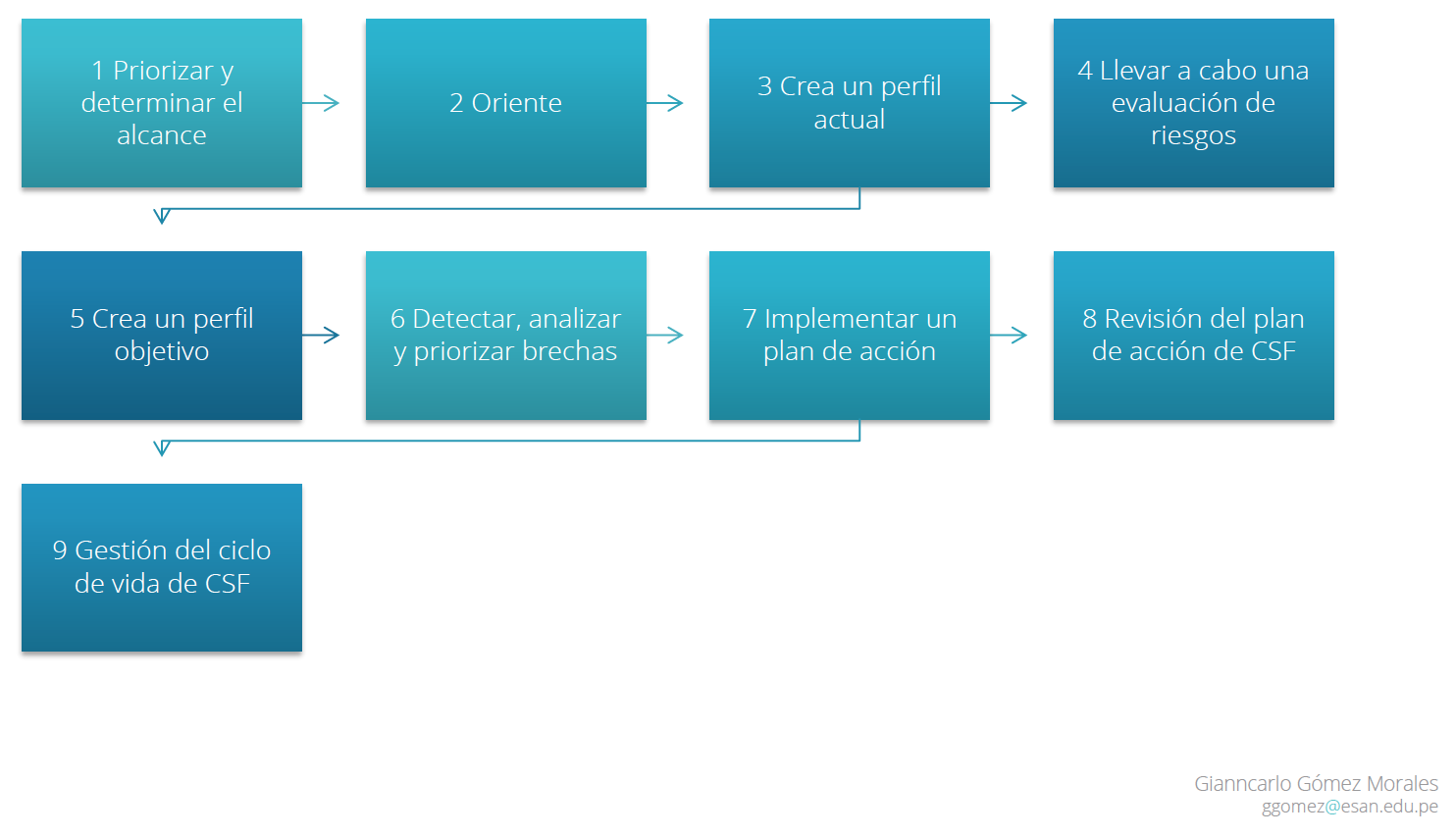


**2.4** **COMUNICACIÓN DE LOS REQUISITOS DE CIBERSEGURIDAD CON LOS INTERESADOS**

Comunicación de los requisitos de ciberseguridad con los interesados El Marco proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la entrega de productos y servicios esenciales de infraestructura crítica, por ejemplo:

* Una organización puede usar un Perfil de destino para expresar los requisitos de gestión del riesgo de ciberseguridad a un proveedor de servicios externo (por ejemplo, un proveedor de la nube al que está exportando datos).
* Una organización puede expresar su estado de seguridad cibernética a través de un perfil actual para informar resultados o comparar con los requisitos de adquisición.
* Un propietario/operador de infraestructura crítica, habiendo identificado un socio externo del que depende esa infraestructura, puede usar un Perfil de destino para transmitir categorías y subcategorías requeridas.
* Un sector de infraestructura crítica puede establecer un Perfil de Destino que se pueda utilizar entre sus componentes como un Perfil de referencia inicial para construir sus Perfiles de Destino personalizados.
* Una organización puede gestionar mejor el riesgo de ciberseguridad entre las partes interesadas mediante la evaluación de su posición en la infraestructura crítica y la economía digital más amplia utilizando niveles de implementación.
* Cyber SCRM es el conjunto de actividades necesarias para gestionar el riesgo de seguridad cibernética asociado con partes externas. Más específicamente, el cyber SCRM aborda tanto el efecto de ciberseguridad que una organización tiene en las partes externas como el efecto de ciberseguridad que las partes externas tienen en una organización.

**Figura 6.** Método para su implementación.



3 ID.BE IDENTIFICAR

**3.1** **ID. AM GESTIÓN DE ACTIVOS**

**3.1.1** **IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

El Sistema de Gestión de Seguridad de la Información (SGSI) se basa en gestionar los riesgos que se presentan sobre los activos de información y que puedan atentar contra los principios de seguridad de los activos que son la Integridad, Confidencialidad y Disponibilidad.

La metodología de identificación, clasificación y valoración de los activos, permite identificar cada uno de los activos de información que se utilizan en el proceso o los procesos del alcance del SGSI junto con sus características principales como lo son: ubicación, responsable, custodio, tipo y usuarios. Además, se describen los criterios que se han definido para clasificar el nivel de confidencialidad, integridad y disponibilidad que debe tener cada activo de información y posteriormente determinar el valor que el activo tiene para la organización, según la clasificación dada.

La identificación, clasificación y valoración es un paso previo a la identificación de riesgos sobre los activos de información, debido a que da una idea clara de los diferentes riesgos a los que puede estar expuesta la organización debido a su ubicación, a su manejo, o debido al impacto que pueda degradar algunos o todos los principios de seguridad.

La metodología planteada para la identificación, clasificación y valoración de los activos de información está basada en los estándares ISO 27001 e ISO27002.

**3.1.2 ROLES Y RESPONSABILIDADES**

El responsable de la información será la única persona encargada de realizar la tarea de clasificación, porque para él fueron asignados dichos activos y solo él tiene la competencia para identificar el nivel de exposición y valor que tiene la información; también determinará los colaboradores responsables que ayudarán al proceso de clasificación de la información.

Por lo tanto el responsable de la información tiene las siguientes obligaciones:

* Definir el nivel de clasificación para cada uno de los activos de información que se encuentren en su área.
* Revisar periódicamente y asegurarse de mantener actualizados los niveles de clasificación de la información.
* Identificar y minimizar los riesgos a los que puede estar sometida la información y reportar los que requieran de la intervención del encargado de la Seguridad de la Información.
* Tomar decisiones de seguridad con respecto a su uso y acceso.
* Preservar su confidencialidad, integridad y disponibilidad.

**3.1.3 CRITERIOS DE CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

A continuación se describen los criterios de clasificación para poder realizar la respectiva valoración de los activos de información.

**3.1.3.1 Criterios de clasificación**. Los activos de información identificados dentro del inventario, deberán ser clasificados tanto en su confidencialidad, integridad como en su disponibilidad. El nivel seleccionado determina que el activo de información debe mantener las condiciones de seguridad definidas en dicha escala porque de lo contrario podría impactar a la organización en aspectos legales, contractuales, operativos, económicos o de imagen.

Para clasificar el nivel de confidencialidad de los activos de información, se debe plantear la siguiente pregunta:

*¿La pérdida de confidencialidad del activo de información, que sea conocido por personas no autorizadas, o que sea publicado sin la debida autorización o fuera del momento establecido podría…..?*

La respuesta a esta pregunta deberá ubicarse en el cuadro 4:

**Cuadro 4.** Criterios de Clasificación según la Confidencialidad.

| **NIVEL DE CLASIFICACIÓN** | **DEFINICIÓN** |
| --- | --- |
| Confidencial | Información sensible al interior de la compañía que sólo puede ser conocida por un limitado número de colaboradores. La divulgación de esta información a personas no autorizadas puede comprometer la supervivencia o los resultados de la organización, causándole severos problemas de tipo financiero e imagen. |
| Privada | Información sensitiva dentro de la compañía usada para propósitos del negocio por grupos específicos de empleados. |
| Pública | Información no sensible que puede ser conocida por los colaboradores de la compañía o terceros, sin que se ponga en riesgo la compañía. |
| **Fuente:** La autores | |

Toda información que no se clasifique y no se divulgue será considerada como confidencial.

El criterio que más se acomode dentro de la tabla a lo que sucedería en la organización si el activo pierde su confidencialidad, deberá ser el elegido y asignado al activo de información en el formato de inventario de activos de la información.

**Ejemplo:** El portafolio de negocios de una compañía, se considera pública ya que puede ser conocida por externos (este es el objetivo); sin que se ponga en juego la supervivencia de esta.

Para clasificar la integridad y la disponibilidad de la información, se debe plantear las siguientes preguntas:

*¿La pérdida de integridad del activo de información, su pérdida de exactitud y completitud o su alteración no autorizada podría…..?*

*¿La pérdida de disponibilidad del activo, o que el mismo no se encuentre a disposición del personal autorizado en el momento requerido, podría…..?*

Las respuestas a estas preguntas deberán ubicarse en el cuadro 5:

**Cuadro 5.** Criterios de Clasificación según la Disponibilidad e Integridad.

| **NIVEL** | **ASPECTO** | **REPERCUSIÓN** |
| --- | --- | --- |
| **ALTO** | Operativo | * Interrupción de las operaciones de la organización por más de 2 días. * Pérdida de información crítica de la organización o de terceros que no se pueda recuperar fácilmente. |
| Económico | * Impacto que reduzca el patrimonio de la organización en un rango superior a 100 SMLV. |
| Imagen | * Impacto que genera una imagen negativa de la organización en el mercado. * Incremento en el número de reclamos formulados por los clientes. * Pérdida de Clientes. |
| Legal | * Intervención a la Organización por parte de organismos de control por incumplimientos legales y/o contractuales. * Demandas provenientes de actividades de la organización. |
| **MEDIO** | Operativo | * Interrupción de las operaciones de la Compañía de 5 horas a 2 días. * Inoportunidad de la información ocasionando retrasos en las labores de las áreas y/o en la respuesta a los entes reguladores. * Reproceso de actividades y aumento de la carga operativa. * Reconstrucción de información crítica. |
| Económico | * Impacto que reduzca el patrimonio de la organización entre 20 y 100 SMLV. |
| Imagen | * Reclamaciones de clientes que requieran de un plan de acción a corto plazo y podrían afectar la continuidad de la relación. |
| Legal | * Observaciones por incumplimiento de las normas establecidas por los entes reguladores que generen un plan de acción a corto plazo. * Incumplimiento de un contrato. |
| **BAJO** | Operativo | * No hay interrupción o la Interrupción de las operaciones de la Compañía es por menos de 4 horas. * No afecta la oportunidad de la información de manera significativa, no altera el funcionamiento de las áreas receptoras y procesadoras de información. |
| Económico | * Impacto que reduzca el patrimonio de la organización en un valor inferior a 20 SMLV. |
| **BAJO** | Imagen | * Existen reclamaciones por parte de los clientes pero no se afecta la continuidad de la relación. |
| Legal | * Generan sanciones económicas y/o administrativas leves. |
| **Fuente:** Los autores | | |

Según los criterios que mejor se acomoden a la situación real de lo que podría pasar en los aspectos operativo, económico, legal o de imagen si el activo pierde su integridad o su disponibilidad, será seleccionado el nivel de integridad o de disponibilidad.

Si los criterios seleccionados están ubicados en diferentes niveles (Alto, medio o bajo), se escogerá el nivel donde más hayan coincidido los criterios seleccionados, y si la cantidad de criterios entre un nivel y otro es igual, se escogerá el nivel más alto.

**Ejemplo:** Se incurrió en incumplimiento de las política de un ente regulador, pero esto no generó ningún tipo de interrupción a la operación y puede costar entre 5 y 20 SMLV, quedaría evaluado como impacto alto porque la cantidad de criterios entre un nivel y otro son iguales, pero este es el nivel superior.

## 3.1.3.2 Criterios de valoración

* **Alta:** Aquellos activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) sea alta.
* **Media:** Aquellos activos de información en los cuales la clasificación de la información es alta en sólo una de sus propiedades o al menos una de ellas es de nivel medio.
* **Baja:** Aquellos activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

# 3.1.4 METODOLOGÍA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

La identificación, clasificación y valoración de los activos de información debe realizarse para conocer cuáles son los activos que pertenecen o son utilizados en las actividades de la compañía, sus características, el nivel de confidencialidad, integridad y disponibilidad que deben tener y el valor que tiene para el servicio y la organización.

Como resultado se obtendrá un inventario completo de los activos de información de la empresa y se podrán seleccionar los activos de información a los que se les deberá hacer el análisis de riesgos, siendo estos, los activos que representen un mayor valor para la entidad.

El proceso de identificación, clasificación y valoración de activos deberá ser realizado mínimo anualmente y cuando se presenten cambios sustanciales en el negocio. La metodología (Figura 7) se divide en tres fases que son descritas a continuación:

**Figura 7**. Gestión de los Activos de Información.

**Fuente:** *NTC - ISO 27005.*

## 3.1.4.1 Identificación de los activos de información. Para la identificación de activos de información, se debe tener presente cuáles son las entradas y salidas de cada uno de los procesos de la compañía, las personas, los recursos necesarios para prestar el servicio, y todos los documentos que se utilizan como manuales, políticas, metodologías, etc.

Los activos de información a identificar son

* **Información:** Corresponden a este tipo documentos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros. A este tipo de activos se les evalúa el impacto en confidencialidad, integridad y disponibilidad.
* **Software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas. A este tipo de activos se les evalúa el impacto en confidencialidad, integridad y disponibilidad.
* **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos. A este tipo de activos se les evalúa el impacto en confidencialidad, integridad y disponibilidad.
* **Servicio:** Servicios de computación, comunicaciones y de información, tales como Internet, páginas de consulta, directorios compartidos, sistemas de información y la intranet. A este tipo de activos se les evalúa el impacto en confidencialidad, integridad, disponibilidad.
* **Personas:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información. A este tipo de activos se les evalúa el impacto en confidencialidad y disponibilidad únicamente.

El reconocimiento de estos activos (Figura 8), se puede establecer haciéndose las siguientes preguntas:

**Figura 8.** Reconocimiento Activos de Información.

**Fuente**: Los autores

Todos los activos de información identificados, deben ser incluidos dentro del inventario de clasificación de activos.

**3.1.5 RESULTADOS LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN PARA SOLUCIONES S.A.S.**

De acuerdo con el objetivo de este proyecto se tomaron solo los activos de información tipo bases de datos como se muestra a continuación:

**Cuadro 6.**  Inventario Activos de Información Tipo BD SOLUCIONES S.A.S.

| **ACTIVO DE INFORMACIÓN** | **CRITICIDAD** | | |
| --- | --- | --- | --- |
| **ALTA** | **MEDIA** | **BAJA** |
| **BD EMPLEADOS** | X |  |  |
| **BD PRODUCTOS** |  | X |  |
|
| **BD SERVICIOS** |  |  | X |
| **BD PROVEEDORES** |  | X |  |
| **Fuente:** Los autores | | | |

Analizado el cuadro 6, del resumen del levantamiento de inventario de activos de información, se tomó el activo de información que tuvo una valoración alta para realizar el análisis de riesgos de acuerdo con la metodología de la compañía.

**3.1.5.1 Descripción de activo crítico soluciones S.A.S**

La BD es una RDBMS Relacional, ejemplo de base de datos de empleados creada en MySQL AB, a continuación, se describen las tablas que la conforman y la clasificación de sus campos de acuerdo con la ley 1581, legislación que se debe acatar en este caso, al tratarse de una base de datos personales de empleados:

**Cuadro 7.** Administración Empleados.

|  |  |  |
| --- | --- | --- |
| **dept\_emp** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Privado |
| dept\_no | Número de departamento | Privado |
| from\_date | Fecha inicial | Privado |
| to\_date | Fecha final | Privado |

**Cuadro 8.** Administración Departamentos.

|  |  |  |
| --- | --- | --- |
| **dept\_manager** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Semiprivado |
| dept\_no | Número de departamento | Semiprivado |
| from\_date | Fecha inicial | Semiprivado |
| to\_date | Fecha final | Semiprivado |

**Cuadro 9.** Departamentos.

|  |  |  |
| --- | --- | --- |
| **departments** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Semiprivado |
| dept\_no | Número de departamento | Semiprivado |

**Cuadro 10.** Títulos.

|  |  |  |
| --- | --- | --- |
| **titles** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Semiprivado |
| title | Título | Semiprivado |
| from\_date | Fecha inicial | Semiprivado |
| to\_date | Fecha final | Semiprivado |

**Cuadro 11.** Empleados.

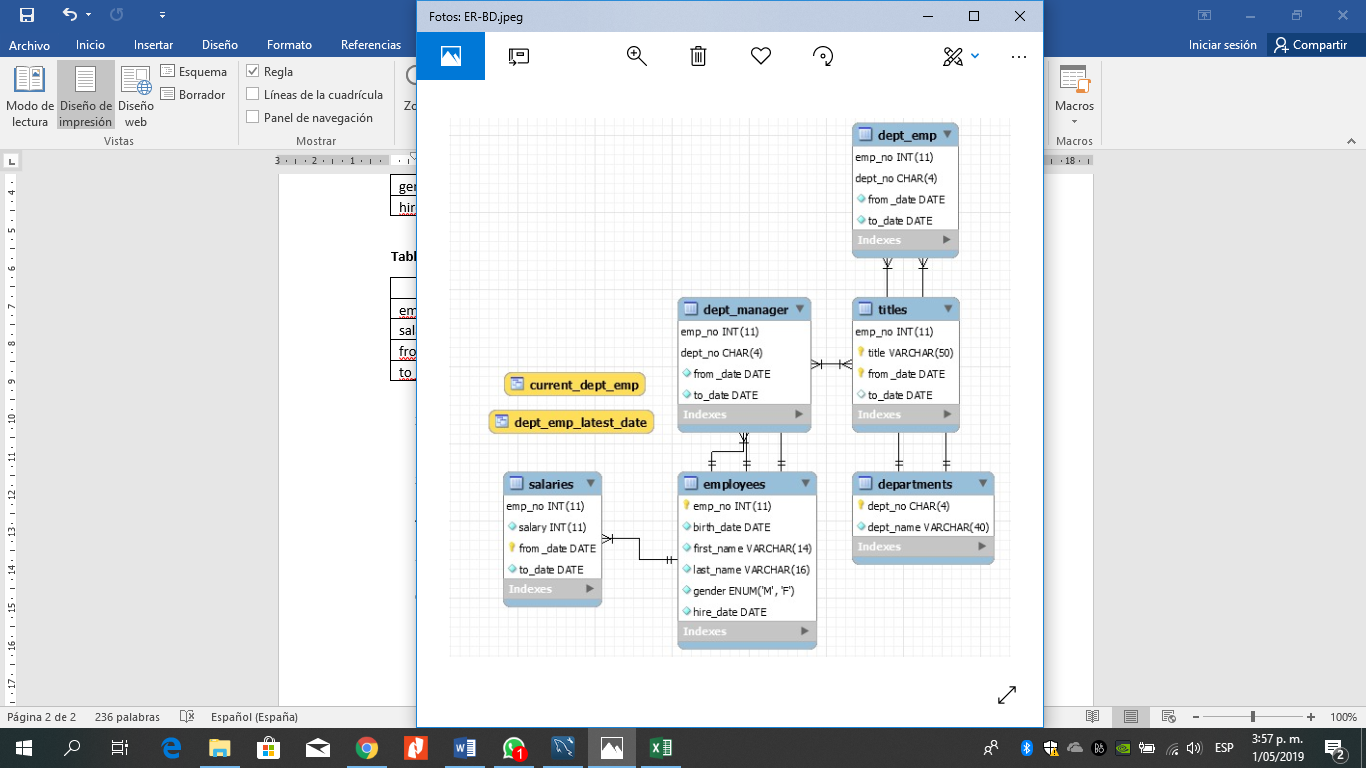
|  |  |  |
| --- | --- | --- |
| **employees** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Semiprivado |
| birth\_date | Fecha de Nacimiento | Semiprivado |
| first\_name | Primer Nombre | Público |
| last\_name | Apellido | Público |
| gender | Género | Público |
| hire\_date | Fecha contratación | Semiprivado |

**Cuadro 12.** Salarios.

|  |  |  |
| --- | --- | --- |
| **salaries** | **Descripción del campo** | **Clasificación Ley 1581** |
| emp\_no | Número de empleado | Semiprivado |
| salary | Salario | Privado |
| from\_date | Fecha inicial | Semiprivado |
| to\_date | Fecha final | Semiprivado |

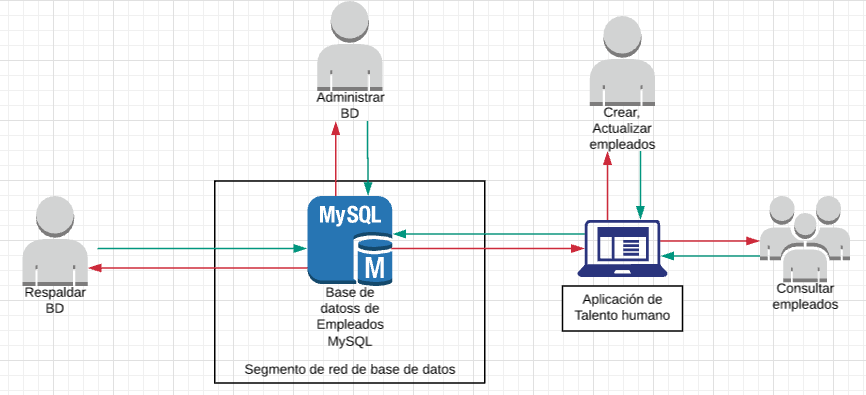
En la figura 9 se puede observar su modelo entidad relación:

**Figura 9.** Modelo ER BD Empleados.



Las comunicaciones y flujos de datos hacia la base de datos de empleados se encuentran en la figura 10.

**Figura 10.** Comunicaciones y flujos de datos BD Empleados.



3.2 ID.BE ENTORNO EMPRESARIAL

3.2.1 ESTABLECIMIENTO DE CONTEXTO

# 3.2.1.1 ID.BE-1 Se identifica y se comunica la función de la organización en la cadena de suministro.

# QUIÉNES SOMOS

Somos una empresa de tecnología informática que busca crear soluciones de talla global, con el propósito de mejorar la calidad de vida y la competitividad a nivel país.

**CLIENTES**

Sector real

Pymes

Compañías de publicidad

# 3.2.1.2 ID.BE-2 Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.

**MATRIZ FODA SOLUCIONES S.A.S**

La matriz FODA que se muestra en el cuadro 1, resume el contexto estratégico de la organización y la propuesta desde la adecuada gestión de Seguridad de la Información para optimizar las fortalezas y oportunidades de la compañía, controlando las debilidades y amenazas.

**Cuadro 13.** Matriz FODA SOLUCIONES S.A.S.

|  |  |  |
| --- | --- | --- |
| **EXTERNAS**  **INTERNAS** | **DEBILIDADES**  • No están bien estructurados los procesos y estos cambian muy seguido, en concordancia a los cambios del negocio, pero esto no se documenta. • Las áreas no conocen sus interdependencias con todos los procesos de la compañía. • El personal dedica gran cantidad de su tiempo a atacar lo urgente pero no lo importante. | **FORTALEZAS**  • Cultura de trato digno en la organización con internos y externos. • Entorno flexible acorde a la economía cambiante. |
| **OPORTUNIDADES**  • Posibilidad de crear nuevos productos y servicios  • El sector de desarrollo sigue fuerte en la economía del país. • Alineación con procesos y prácticas de socio capitalista mayoritario. | **ESTRATEGIAS (DO)**  • Acompañar a las áreas para estructurar sus procesos, identificando las dependencias entre ellos y sus riesgos de seguridad de la información, promoviendo el mejoramiento continuo. • Aprovechar las buenas prácticas del socio capitalista mayoritario en todo lo relacionado a la protección de la información. | **ESTRATEGIAS (FO)**  • Aprovechar el entorno flexible de la organización para poder ofrecer nuevos productos y servicios en tiempo récord, donde se contemplen todos los aspectos de seguridad desde la propuesta inicial de cada uno de ellos, garantizando su continuidad. |
| **AMENAZAS**  • Compañías que prestan este mismo servicio y tienen una estructura organizacional más competitiva. • Inobservancia a las disposiciones de la ley de protección de datos personales. | **ESTRATEGIAS (DA)**  • Mejorar la capacidad competitiva en el mercado ofreciendo nuevos productos y servicios más estructurados, revisando desde el inicio todos los puntos relevantes de seguridad de la información, para garantizar que los servicios entregados son de alta calidad. • Estructurar el modelo a seguir para dar cumplimiento a la ley de protección de datos personales y demás normativa o legislación aplicable. | **ESTRATEGIAS (FA)**  • Capacitar frecuentemente a todo el personal de la compañía en los aspectos legales y del cuidado de la información. • Fomentar el elemento diferenciador del trato digno e implementar una cultura organizacional en Seguridad de la Información, para que se interiorice con mayor facilidad. • Revisar constantemente cambios en la estructura organizacional, disposiciones legales y comunicarlas a todos los colaboradores. |
| **Fuente:** Los autores | | |

# 3.2.1.3 ID.BE-3 Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.

# MISIÓN

### Crear, construir y operar servicios informáticos innovadores que impacten positivamente la sociedad.

# VISIÓN

### SOLUCIONES S.A.S, será una organización global, referente en la concepción, desarrollo e implementación de servicios informáticos innovadores.

**VALORES**

### Calidad Innovación Impacto

# 3.2.1.4 ID.BE-4 Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.

En el cuadro 14, se puede identificar que estrategias se proponen y cuáles pueden ser respaldadas con este proyecto

**Cuadro 14.** Cuadro de Resultados de la Matriz FODA.

|  |  |
| --- | --- |
| **OBJETIVO DEL SGSI** | **ESTRATEGIAS** |
| **DO.**   Identificar y administrar los riesgos de seguridad de la información de SOLUCIONES S.A.S. | • Acompañar a las áreas para estructurar sus procesos, identificando las dependencias entre ellos y sus riesgos de seguridad de la información, promoviendo el mejoramiento continuo. • Aprovechar las buenas prácticas del socio capitalista mayoritario en todo lo relacionado a la protección de la información. |
| **DA.**  Por medio de políticas, herramientas físicas y tecnológicas proporcionar los controles necesarios para la protección de la información crítica, apoyando los objetivos estratégico de la compañía. | • Mejorar la capacidad competitiva en el mercado ofreciendo nuevos productos y servicios más estructurados, revisando desde el inicio todos los puntos relevantes de seguridad de la información, para garantizar que los servicios entregados son de alta calidad. • Estructurar el modelo a seguir para dar cumplimiento a la ley de protección de datos personales y demás normativa o legislación aplicable. |
| **FO.**  Respaldar el plan de continuidad de negocio, garantizando la continuidad de la información. | • Aprovechar el entorno flexible de la organización para poder ofrecer nuevos productos y servicios en tiempo récord, donde se contemplen todos los aspectos de seguridad desde la propuesta inicial de cada uno de ellos, garantizando su continuidad. |
| **FA.**   Promover el mejoramiento continuo en seguridad de la información a nivel cultural. | • Capacitar frecuentemente a todo el personal de la compañía en los aspectos legales y de seguridad de la información. • Fomentar el elemento diferenciador del trato digno e implementar una cultura organizacional en Seguridad de la Información, alineada con la cultura del principal capitalista, para que se interiorice con mayor facilidad. • Revisar constantemente cambios en la estructura organizacional, disposiciones legales y comunicarlas a todos los colaboradores. |
| **Fuente:** Los autores | |

3.3 ID.GV GOBERNANZA

3.3.1 ID.GV-1 Se establece y se comunica la política de seguridad cibernética organizacional. POLÍTICA DE SEGURIDAD CIBERNÉTICA

Para Soluciones S.A.S la información es el segundo activo más importante y constituye un recurso estratégico para el cumplimiento de su misión, por lo que es un compromiso de primer nivel protegerla, cuidarla y manejarla apropiadamente teniendo en cuenta los criterios de confidencialidad, integridad disponibilidad y confiabilidad para asegurar cumplimiento de requisitos técnicos, normativos, regulatorios y operativos a los cuales está sujeta, con base en un proceso de gestión de riesgos periódico y mejorando de manera continua la idoneidad, suficiencia y eficacia del Sistema de Gestión de Seguridad de la Información.

3.3.2 ID.GV-1-3 Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.

A continuación se enuncian las leyes, decretos y circulares externas a las que SOLUCIONES S.A.S debe dar cumplimiento, verificar constantemente su actualización o disposiciones nuevas y estar pendiente de cualquier normativa adicional que se genere.

**3.3.2.1 Requisitos legales Colombia**

Constitución Política de Colombia 1991.

* Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
* Artículo 20. Libertad de Información.
* Artículo 61.El Estado protegerá la propiedad intelectual por el tiempo y las formalidades que establezca la ley.
* Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.”
* Ley 599 de 2000. “Por medio de la cual se aprueba el Código Penal Colombiano”.
* Art. 199. Espionaje.
* Art. 258. Utilización indebida de información.
* Art. 418. Revelación de Secreto.
* Art. 419. Utilización de asunto sometido a secreto o reserva.
* Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos.
* Artículo 272. Violación a los mecanismos de protección de derecho de autor, derechos conexos y otras defraudaciones.
* Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
* Ley 1343 de 2009 – “Por medio de la cual se aprueba el Tratado sobre el Derecho de Marcas” y su “Reglamento”, adoptado el 21 de octubre de 1994.
* Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
* Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la Protección de Datos Personales.”
* Decreto 2952 de 2010 “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.”
* Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012.”
* Decreto 886 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.”

**3.3.2.2 Requisitos Internos**

* Código de Ética.
* Reglamento Interno.

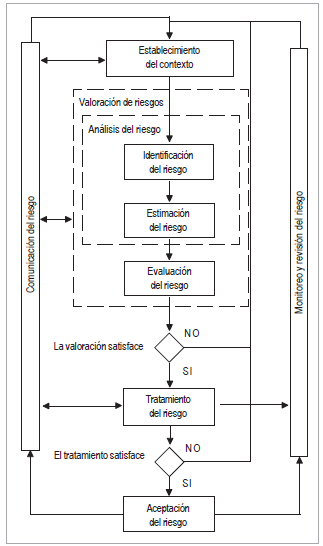
**3.4 ID.RA EVALUACIÓN DE RIESGOS**

**3.4.1 GESTIÓN DE RIESGOS SOBRE LOS ACTIVOS DE INFORMACIÓN**

La metodología de riesgos permite identificar, analizar, evaluar y definir el manejo de los riesgos, para así apoyar el cumplimiento de los objetivos del negocio; la gestión de los riesgos por parte de los responsables de los procesos hace más efectiva la implementación de los controles y las acciones de mejora.

La metodología utilizada para la valoración de riesgo se basó en la metodología propuesta por el estándar ISO 27005, que se ilustra en la Figura 11 y se describe a continuación:

**Figura 11.** Figura para Gestión de Riesgos ISO 27005.

**

**Fuente:** *NTC - ISO 27005.*

* **Establecimiento del Contexto Organizacional (Interno y Externo)**

Las organizaciones tienen un contexto interno que incluye misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normatividad entre otros. De igual forma interactúa con su medio por lo cual podemos indicar que tiene un contexto externo en el cual deben considerarse aspectos como la competencia, regulaciones legales que apliquen, economía, política, tecnología, cultura y los demás aspectos que se consideren necesarios.

La importancia de entender estos aspectos es saber que requiere ser protegido y cuáles son las limitaciones existentes para esta protección. Como fuentes de información se recomienda emplear documentación existente en la organización relacionada con calidad, seguridad, planeación estratégica y continuidad que brinden información y que permitan posicionar a la organización con respecto a su medio: entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones y las demás que se consideren necesarias.

El objetivo de esta etapa es conocer a la organización para determinar que los puede afectar a nivel interno y externo, que requieren proteger y de acuerdo a los recursos actuales como podría darse esa protección para establecer el nivel de aceptación de riesgo al cual están dispuestos, determinar los alcances y limitaciones existentes.

* **Valoración de Riesgos de Seguridad de la Información**

Comprende dos actividades principales: Análisis y Evaluación de Riesgos. En la etapa de valoración de riesgos se identifican los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestos. En este punto se recomiendan posibles controles para mitigación de los riesgos.

Para la valoración se deben tener en cuenta los posibles activos que sean relevantes, incluyendo procesos, información, datos y activos de soporte. La valoración para activos de soporte debe incluir costos por adquisición, renovación o reposición, mantenimiento y tener en cuenta los factores de depreciación.

Luego de establecer el listado de activos es posible validar si el alcance definido de forma preliminar es correcto o debe ser ajustado para cumplir con los propósitos. También se debe tener en cuenta los tipos de amenazas que pueden presentarse (estas pueden ser físicas, lógicas o estratégicas y su origen puede ser natural, técnico, humano accidental o intencional), los daños que pueden implicar las amenazas, la determinación sobre las pérdidas causadas por los riesgos en términos de impacto. A partir de lo anterior es posible determinar los controles y priorizar los riesgos.

Los controles a usar se clasifican en controles preventivos, controles detectivos, y controles correctivos. De igual forma dependiendo de si se usa o no una base tecnológica para la implementación, los controles pueden ser técnicos o no técnicos. Como parte de la identificación es importante tener en cuenta las dependencias entre activos y procesos, la cadena de valor y el valor mismo por activo y proceso.

Los procesos deben ser priorizados con el fin de determinar niveles de criticidad de los mismos. Las vulnerabilidades pueden ser determinadas por varios medios como la realización de pruebas y listas de chequeo. Las amenazas deben clasificarse de forma acorde y el análisis de su impacto con respecto a la frecuencia de ocurrencia es importante para la determinación correcta de los riesgos.

En la valoración se pueden usar técnicas cuantitativas y/o cualitativas para la estimación de riesgos y hay formas variadas de presentación de la información como los vectores de ataque o las matrices, todo depende de los requerimientos, conocimientos, recursos y habilidades del personal de la organización.

* **Tratamiento de Riesgos de Seguridad de la Información**

Con la etapa de tratamiento de riesgos se establece e implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización, dentro de las acciones a tomar encontramos principalmente: reducir, aceptar, eliminar y transferir. Como parte del tratamiento se definen las posibles acciones a seguir sobre los riesgos y se establece un plan de tratamiento según la priorización previa que se realizó.

Este plan debe definir recursos, responsabilidades y actividades teniendo en cuenta las posibles restricciones a nivel económico, legal, temporal, técnico, operativo, político, cultural y las demás que sean determinadas. Los controles que sean recomendados deben incluir un análisis costo-beneficio (incluyendo costos de implementación y mantenimiento).

El plan debe ser documentado y finalmente definidas las políticas a seguir. Con la definición de políticas se establece los lineamientos base y se logra ejercer la línea de mando el don de mando requerida para cumplir con las definiciones de seguridad indicadas con anterioridad. En este punto es importante que el plan sea consistente con las metas y objetivos en la parte de planificación del proceso de gestión, maneje tiempos acordes con los definidos al inicio y con el tiempo de vida útil de los activos, además de dar paso a la siguiente etapa de mejora continua.

El plan de tratamiento debe definir los pasos pormenorizados para gestionar los riesgos sin dejar espacio a nuevos posibles riesgos que ocurran como consecuencia de errores en la implementación de las acciones del tratamiento mismo[[1]](#footnote-1).

* **Comunicación y Consulta**

La comunicación del riesgo es una actividad para activar acuerdos de cómo gestionar los riesgos intercambiando y/o compartiendo información entre los encargados de tomar decisiones y otros interesados.

Una organización debe desarrollar planes de comunicación de riesgo tanto para operaciones normales como para las situaciones de emergencia. Por lo tanto las actividades de comunicación de riesgo deben ser revisadas continuamente.2

* **Monitoreo y Mejora Continua del Proceso de Gestión de Riesgos**

Los riesgos no son estáticos. El Monitoreo constante es necesario para detectar estos cambios. Esto puede ser soportado por servicios externos que proveen información de nuevas amenazas y vulnerabilidades.

Para esta fase el elemento primordial es el control de cambios, por lo cual el monitoreo debe realizarse sobre activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas y procedimientos con el fin de establecer acciones a seguir ante cambios (tales como agregar activos, riesgos o amenazas nuevas o que algo se modifique o requiera ser eliminado) y lograr que la gestión este continuamente actualizada para lograr evaluar indicadores de cumplimiento de los planes.

Con el monitoreo y la mejora continua se busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos. También, permite agregar al análisis riesgos nuevos que puedan aparecer luego de la definición de los planes teniendo en cuenta posibles cambios internos y externos.

Para aplicarla en SOLUCIONES S.A.S.; se plantearon las siguientes directrices:

* Los niveles de impacto y probabilidad de ocurrencia de riesgo fueron definidos de acuerdo a las necesidades de la compañía[[2]](#footnote-2).
* El plan de tratamiento de riesgos se realiza para los riesgos que no se encuentren en un nivel aceptable para la organización.

# 3.4.1.1 Nivel aceptable de los riesgos

El nivel de aceptación de los riesgos (cuadro 15), ha sido definido según las necesidades de este sector con el fin de garantizar que las acciones a realizar para mitigar, transferir o asumir los riesgos serán las adecuadas para llevar los riesgos a un nivel aceptable.

El nivel de aceptación de los riesgos estará compuesto por aquellos riesgos que no expongan a la organización a pérdidas sustanciales en términos económicos, operativos o de imagen.

**Cuadro 15.** Zonas de Aceptación de Riesgo.

|  |  |
| --- | --- |
| **Zona de Riesgo** | **Aceptación de los Riesgos** |
| **Zona Aceptable** | Se aceptan los riesgos. |
| **Zona Tolerable** | Se aceptan los riesgos. |
| **Zona Moderada** | Se aceptan los riesgos y se realiza monitoreo semestral. |
| **Zona Importante** | No se aceptan los riesgos, se requiere tratamiento. |
| **Zona Inaceptable** | No se aceptan los riesgos se requiere tratamiento inmediato. |
| **Fuente:** Los autores | |

Todos los riesgos que se encuentren en la zonas de no aceptación, necesitarán de un tratamiento idóneo para disminuir su nivel; los riesgos aceptables deberán ser monitoreados.

# 3.4.1.2 Metodología para el análisis de riesgos de soluciones S.A.S

El análisis, evaluación y tratamiento de los riesgos permite determinar cuáles son, cuánto valen, a qué están expuestos y como están protegidos los activos de información en coordinación con los objetivos, estrategias y políticas corporativas de la organización. Las actividades a realizar permiten elaborar planes de acción al alcance de la organización, que al implantarlos y operarlos, satisfacen los objetivos propuestos por la Alta Dirección.

Este esquema de trabajo es constante y se encuentra en mejoramiento continuo tanto en búsqueda de nuevos activos como de nuevas amenazas y vulnerabilidades, con el fin de aprender de la experiencia y adaptarse fácilmente a los nuevos contextos, lo que exige una revisión periódica de los riesgos por parte de los miembros de la dirección de la compañía. En la figura 12 se especifican las etapas de esta metodología:

**Figura 12**. Gestión de los Riesgos de Seguridad de la Información.

**Fuente:** Los autores.

## 3.4.1.2.1 Análisis. Los riesgos a identificar están asociados a la pérdida de integridad, confidencialidad y disponibilidad de los activos de información, definiéndolos así:

* Acceso no autorizado al activo de información que permite la utilización indebida o fraudulenta del mismo.
* Pérdida de la integridad del activo de información que permite la utilización indebida o fraudulenta del mismo.
* Pérdida de la disponibilidad del activo de información que impida la secuencia del proceso.

## 3.4.1.2.2 Identificación de Amenazas y Vulnerabilidades. Para reconocer los riesgos sobre los activos de información, se deben determinar las vulnerabilidades y amenazas que pueden afectar la integridad, confidencialidad y disponibilidad de cada activo. Las amenazas son “cosas que ocurren”, y las vulnerabilidades son las debilidades inherentes al activo o a la falta de controles sobre el mismo. Este par amenaza – vulnerabilidad debe ser analizado en el caso que la vulnerabilidad presente en el activo haga mayor el impacto al presentarse la amenaza.

## 3.4.1.2.3 Valoración del Riesgo Inherente. La calificación del riesgo se obtiene a través de la estimación de dos variables: la probabilidad de ocurrencia de que la amenaza se presente y se aproveche de la vulnerabilidad y el impacto que puede causar la materialización del riesgo. La primera variable (Probabilidad de ocurrencia) representa el número de veces que el riesgo se ha presentado o puede presentarse en un determinado tiempo, y la segunda variable (Impacto) se refiere a la magnitud de sus efectos.

**Probabilidad:** Es la posibilidad de que un riesgo se materialice. Es un criterio de frecuencia expresado en la cantidad de veces que el riesgo se ha presentado en un tiempo dado. Los rangos posibles de probabilidad se detallan en el cuadro 16:

**Cuadro 16**. Probabilidad del Riesgo.

| **Rango Probabilidad** | **Probabilidad Hipotética** | **Probabilidad Matemática** | **Valor** |
| --- | --- | --- | --- |
|
| **BAJA** | * Podría ocurrir en circunstancias excepcionales. * Existe la suficiente información para determinar una frecuencia baja. | 1 vez al año | 1 |
|
| **MEDIA** | * Existe alguna posibilidad de que el evento ocurra. * No se tiene la información suficiente para determinar su ocurrencia. | 2 - 3 veces al año | 2 |
|
| **ALTA** | * Podría ocurrir la mayoría de veces * Se tiene la suficiente información para determinar una frecuencia alta. | Mayor a tres veces al año | 3 |
| **Fuente:** Los autores | | | |

**Impacto:** Es el efecto que causaría la materialización del riesgo a la Organización, sin tener en cuenta si se ha presentado o no. Los rangos posibles de impacto se detallan en el cuadro 17.

**Cuadro 17.** Impacto del Riesgo.

| **Rango Impacto** | **Reputación** | **Legal** | **Operativo** | **Económico** | **Valor** |
| --- | --- | --- | --- | --- | --- |
| **LEVE** | Existen reclamaciones por parte de los clientes pero no se afecta la continuidad de la relación. | Generan sanciones económicas y/o administrativas leves. | No hay interrupción o la Interrupción de las operaciones de la Compañía es por menos de 4 horas.  No afecta la oportunidad de la información de manera significativa, no altera el funcionamiento de las áreas receptoras y procesadoras de información. | Impacto que reduzca el patrimonio de la organización en un valor inferior a 20SMLV. | 5 |
| **MODERADO** | Reclamaciones de clientes que requieran de un plan de acción a corto plazo y podrían afectar la continuidad de la relación. | Observaciones por incumplimiento de las cláusulas establecidas en los contratos que generen un plan de acción a corto plazo.  Incumplimiento de un contrato. | Interrupción de las operaciones de la Compañía de 5 horas a 2 días.  Inoportunidad de la información ocasionando retrasos en las labores de las áreas y/o en la respuesta a los clientes.  Reproceso de actividades y aumento de la carga operativa.  Reconstrucción de información crítica. | Impacto que reduzca el patrimonio de la organización entre 20 y 100 SMLV. | 10 |
| **CATASTRÓFICO** | Impacto que genera una imagen negativa de la organización en el mercado.  Incremento en el número de reclamos formulados por los clientes.  Pérdida de Clientes. | Intervención a la Organización por parte de organismos de control por incumplimientos legales y/o contractuales  Demandas provenientes de actividades de la organización. | Interrupción de las operaciones de la organización por más de 2 días  Pérdida de información crítica de la organización o de terceros que no se pueda recuperar fácilmente. | Impacto que reduzca el patrimonio de la organización en un rango superior a 100 SMLV. | 20 |
| **Fuente:** Los autores | | | | | |

Una vez seleccionada la probabilidad y el impacto del riesgo, se debe ubicar el riesgo, según la valoración dada, así como se muestra en el cuadro 18.

**Cuadro 18.** Calificación de las Zonas de Riesgo.



**Fuente:** Los autores

## 

## 3.4.1.2.4 identificaciones de controles. Varios de los activos de información tienen controles establecidos con el fin de evitar que sufran algún daño, ya sea a nivel de la pérdida de confidencialidad, integridad o disponibilidad.

La identificación de estos controles permite visualizar realmente que tan expuestos se encuentran los activos a la materialización de los riesgos.

Los controles se valorarán según la efectividad en la mitigación del riesgo. Para esto se utilizará la escala que se muestra en el cuadro 19:

**Cuadro 19.** Valoración del Control.

| **Criterios** | **Definición** | **Valor** |
| --- | --- | --- |
| **DÉBIL** | No existen controles o existen pero no son efectivos. | 1 |
| **MODERADO** | Los controles existentes no son del todo efectivos. Pueden o no estar documentados. | 2 |
| **FUERTE** | Los controles existentes son efectivos y están documentados. | 3 |
| **Fuente:** Los autores | | |

## 

## 3.4.1.2.5 Valoración Del Riesgo Residual. El cálculo del riesgo residual se efectúa con base en las escalas de valoración del impacto y la probabilidad definidas previamente, la diferencia es que para seleccionar el valor de probabilidad e impacto de los riesgos se debe tener en cuenta los controles actualmente implementados en la organización para la mitigación de los riesgos, estén o no documentados.

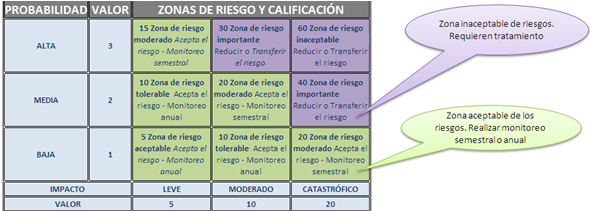
**3.5 ID.RM ESTRATEGIA DE GESTIÓN DE RIESGOS**

Para realizar la evaluación del riesgo se requiere la participación activa de la alta dirección, como se describe a continuación.

**3.5.1 ACEPTACIÓN DEL RIESGO**

La evaluación de los riesgos se hace en base al nivel aceptable definido por la organización, aquellos riesgos que no se encuentren en el nivel aceptable deberán ser tratados, de acuerdo con las necesidades de la compañía, como se muestra en la Figura 13.

**Figura 13.** Zonas de Riesgo Aceptable e Inaceptable.



**Fuente:** Los autores.

Todos los riesgos residuales que hayan quedado en la zona inaceptable de riesgo (morada), deberán ser tratados.

**3.5.2 REVISIÓN POR LA DIRECCIÓN**

Una vez se tengan los riesgos estratificados entre los aceptables e inaceptables, la lista de los inaceptables debe ser revisada por la alta dirección.

El objetivo de esta revisión es asegurar que los riesgos sean conocidos y aceptados por la Organización y que todas las áreas de la Organización se comprometan a trabajar sobre el tratamiento de estos riesgos. La revisión debe realizarse anualmente.

**3.5.3 TRATAMIENTO**

**3.5.3.1 Planes de tratamiento.** Una vez se ha calculado tanto el riesgo residual y se han evaluado cuales están en la zona inaceptable, se procede a definir los proyectos que van a permitir disminuir los riesgos de los niveles aceptables definidos por la Organización.

Los planes deben ser definidos por los líderes de los procesos, el responsable y custodio del activo de información y deberán ser aprobados por la alta dirección.

Estos planes deben ser seguidos mínimo trimestralmente, para asegurar su ejecución. Los planes podrán estar entre las opciones de Mitigar, Transferir o Evitar el riesgo, según como se especifica en el cuadro 20.

**Cuadro 20.** Acción a seguir en el Plan de Tratamiento según la Clasificación del Riesgo.



## Fuente: Los autores

## 3.5.3.2 Seguimiento. Para los riesgos bajos, la acción a tomar es hacer monitoreo de los mismos con el fin de detectar si en algún momento llega a cambiar este estado.

Para los riesgos medios y altos, la acción a seguir es que trimestralmente como mínimo se realizará la revisión por parte del área encargada y de la alta dirección de los planes de tratamiento definidos.

**3.5.4 RESULTADOS ANÁLISIS DE RIESGOS BASADO EN ACTIVOS DE INFORMACIÓN PARA SOLUCIONES S.A.S**

**Cuadro 21.** Resumen Análisis de Riesgos de Seguridad de la Información del activo tipo BD crítico para SOLUCIONES S.A.S.

| **Riesgo** | **Riesgo Inherente** | | | | | | | **Riesgo para Tratar** | **Control NIST Aplicable** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **5** | **10** | **15** | **20** | **30** | **40** | **60** |
| Privilegios excesivos e inutilizados. |  |  | X |  |  |  |  |  | **PR.AC-4** |
| Abuso de Privilegios |  |  |  |  | X |  |  |  | **PR.AC-1**  **PR.AC-4** |
| Inyección por SQL |  |  |  |  |  | X |  | SI | **ID.RA-1** |
| Auditorías débiles | X |  |  |  |  |  |  |  | **PR.AC-1** |
| Exposición de los medios de almacenamiento para **backup** |  |  | X |  |  |  |  |  | **PR.DS-1**  **PR.DS-3** |
| Explotación de vulnerabilidades y bases de datos mal configuradas |  |  |  | X |  |  |  | SI | **ID.RA-1**  **ID.RA-2** |
| Datos sensibles mal gestionados |  |  |  |  | X |  |  | SI | **PR.AC-4**  **PR.DS-3** |
| Denegación de servicio (DoS) |  |  |  |  |  | X |  | SI | **PR.DS-4** |
| Destrucción de la información / sabotaje |  |  |  |  | X |  |  | SI | **PR.DS-3** |
| Limitado conocimiento y experiencia en seguridad y educación. |  |  |  |  | X |  |  | SI | **ID.RA-3** |
| Nombre de usuario/password en blanco o bien hacer uso de uno débil |  |  |  |  |  | X |  | SI | **PR.AC-1** |
| Preferencia de privilegios de usuario por privilegios de grupo |  |  |  |  |  | X |  | SI | **PR.AC-4** |
| Características de bases de datos innecesariamente habilitadas |  |  |  | X |  |  |  | SI | **PR.DS-1** |
| Desbordamiento de búfer |  |  |  |  | X |  |  | SI | **PR.DS-4** |
| Bases de datos sin actualizar |  |  |  |  |  | X |  | SI | **PR.DS-4** |
| Datos sensibles sin cifrar |  |  |  |  |  |  | X | SI | **PR.DS-1** |
| **Fuente:** Los autores | | | | | | | | | |

El tratamiento a los riesgos se desarrolló por planes, priorizando los de mayor criticidad o impacto para la organización.

Los riesgos críticos y los planes de tratamiento propuestos basados en el framework NIST se detallan en el siguiente capítulo.

**4** **PR PROTEGER**

**4.1 PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.

El acceso a la BD Empleados está supeditado a un rol. Un rol de MySQL es una colección de privilegios con nombre. Al igual que las cuentas de usuario, los roles pueden tener privilegios otorgados y revocados.

A una cuenta de usuario se le pueden otorgar roles, lo que otorga a la cuenta los privilegios asociados con cada rol. Esto permite la asignación de conjuntos de privilegios a las cuentas y proporciona una alternativa conveniente para otorgar privilegios individuales, tanto para conceptualizar las asignaciones de privilegios deseadas como para implementarlas.

Los roles definidos en la base de datos se detallan en el cuadro 22.

**Cuadro 22.** Roles BD Empleados.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Usuario** | **Rol** | **Privilegio** | **Recurso** | **Descripción** |
| U.consulta1 | Consulta | Grant select | BD Empleados | Este rol solo puede hacer consultas los registros dentro de la tabla de empleados de la base de datos. |
| U.consulta2 | Consulta | Grant select | BD Empleados | Este rol solo puede hacer consultas los registros dentro de la tabla de empleados de la base de datos. |
| U.crea-actualiza | Creación | Grant Insert | BD Empleados | Este rol puede adicionar empleados a la base de datos. |
| U.crea-actualiza | Actualizar | Grant update | BD Empleados | Este rol puede actualizar los empleados de la base de datos. |
| u.admin | Crea, modifica y elimina tablas | Grant insert, update, delete | BD empleados | Este rol puede administrar creando, actualizando y borrando tablas sobre la base de datos. |
| U.respalda | Respaldo | Grant backup | BD Empleados | Este rol solo puede tomas respaldos de la base de datos. |

* **Administrar:** Tiene privilegio de creación, actualización y eliminación totales sobre la base de datos.
* **Respaldar:** Tiene privilegio para el respaldo de la estructura y la data de la base de datos.
* **Crear:** Tiene privilegio de adicionar nuevos empleados a la base de datos
* **Actualizar:** Tiene privilegio de adición de datos sobre las tablas de la base de datos.
* **Consultar:** Solo tiene privilegios de consulta sobre los datos de la base de datos.

**BIBLIOGRAFÍA**

Compendio de Gestión de la Seguridad de la Información (SGSI). 2009.

ISO/IEC Guide 73:2002, Risk Management Vocabulary. Guidelines for use in Standards

NIST SP 800-30, Risk Management Guide for Information Technology Systems.

NTC - ISO 27005.

NTC - ISO 27001 – 2013.

PORTAL DE SEGURIDAD CLM

https://protegete.jccm.es/protegete/opencms/index.html <https://protegete.jccm.es/protegete/opencms/Administracion/Seguridad/Metodologias/magerit.html>

El portal de ISO 27001 en Español. 2005. Disponible en http://www.iso27000.es/herramientas.html#section7b

<file:///E:/Users/ammartinr/Downloads/Dialnet-GestionDeRiesgosTecnologicosBasadaEnISO31000EISO27-4797252.pdf>

<https://www.linkedin.com/pulse/implementando-el-cybersecurity-framework-del-nist-g%C3%B3mez-morales/>

<https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf>

<https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1>

1. 1. file:///E:/Users/ammartinr/Downloads/Dialnet-GestionDeRiesgosTecnologicosBasadaEnISO31000EISO27-4797252.pd

   [↑](#footnote-ref-1)
2. Material de estudio Modulo Gestión de Seguridad de la Información. [↑](#footnote-ref-2)