Cartilla

# Gestión de Riesgos de Seguridad de la Información

**Proceso Información, Innovación y Tecnología**

**Subproceso Seguridad de la Información**

**Versión 02**

**Código CT-IIT-0132**

**Año 2023**

## TABLA DE CONTENIDO

1. Introducción ..... 4
2. Objetivo ..... 5
3. Planificación de la gestión de riesgos de seguridad de la información ..... 5
3.1. Contexto interno y externo ..... 5
3.2. Identificación de las necesidades y expectativas de las partes interesadas ..... 5
3.3. Alcance de la gestión de riesgos de seguridad de la información ..... 5
3.4. Definición del perfil de riesgo DIAN ..... 5
3.5. Alineación con la política de gestión de riesgos de seguridad de la información ..... 6
3.6. Análisis de los objetivos de la entidad y los objetivos de los procesos ..... 7
3.7. Roles y responsabilidades ..... 7
3.8. Gestión de riesgos de seguridad de la información en proyectos e iniciativas ..... 8
3.9. Recursos para la gestión de riesgos de seguridad de la información ..... 9
3.10. Gestión de riesgos de seguridad de la información ..... 9
3.10.1. Identificación de activos de información para la gestión de riesgos de seguridad de la información ..... 9
3.10.2. Activos de información objeto de la gestión de riesgos de seguridad de la información ..... 10
3.10.3. Aspectos para considerar en la identificación de riesgos ..... 10
3.10.4. Estructura para describir el riesgo ..... 10
3.10.5. Identificación de amenazas, vulnerabilidades y riesgos tipo ..... 11
3.10.6. Identificar los riesgos Inherentes de seguridad de la información ..... 12
3.10.7. Cálculo de la probabilidad inherente ..... 12
3.10.8. Evaluación del impacto inherente ..... 15
3.10.8.1. Impacto inherente final ..... 16
3.10.9. Evaluación del nivel de riesgo Inherente ..... 17
3.11. Identificación y evaluación de los controles existentes ..... 18
3.11.1. Planificación de la gestión de los controles ..... 19
3.11.2. Atributos para la evaluación individual de controles ..... 19
3.11.3. Evaluación efectividad conjunta de los controles ..... 26
3.11.4. Identificación de controles transversales ..... 28
3.11.5. Evaluación de la Efectividad de los controles transversales en la herramienta GRC ..... 28
3.12. Calculo de riesgo residual ..... 29
3.13. Definición del tratamiento de los riesgos ..... 29
3.13.1. Planes de tratamiento de riesgos de seguridad de la información ..... 29
3.14. Aprobación de riesgos ..... 30
3.15. Protocolo para la aceptación del riesgo ..... 30
3.16. Seguimiento a los planes de tratamiento de riesgos definidos ..... 30
3.16.1. Criterios para el tratamiento de los riesgos de seguridad de la información ..... 31
3.17. Criterios para priorizar el tratamiento del riesgo ..... 31
3.18. Resultados finales de la gestión de riesgos de seguridad de la información ..... 32
3.19. Actualización de nivel de riesgo derivado de incidentes ..... 33
3.20. Identificación del nivel de confianza para la autenticación digital ..... 33
3.21. Identificación de riesgos de proveedores y la cadena de suministro ..... 36
4. Monitoreo y revisión ..... 36
4.1. Reporte Cuatrimestral ..... 41
4.2. Indicadores de gestión ..... 42
4.2.1. Medidas a tomar frente al cumplimiento de los indicadores ..... 43
5. Mejoramiento continuo ..... 43
6. Control de cambios ..... 43
7. Anexos ..... 45

## Tabla de Ilustraciones

**Tabla 1**. Ejemplo de descripción de riesgos ..... 11
**Tabla 2**. Probabilidad por frecuencia de uso. ..... 12
**Tabla 3.** Probabilidad por histórico de ocurrencia ..... 13
**Tabla 4.** Probabilidad final ..... 14
**Tabla 5** Tabla de rangos de la probabilidad identificada ..... 15
**Tabla 6**. Dimensiones de Impacto ..... 16
**Tabla 7.** Impacto final ..... 17
**Tabla 8.** Zonas del mapa de calor ..... 17
**Tabla 9.** Nivel de severidad del riesgo ..... 18
**Tabla 10.** Mapa de calor con niveles de severidad del riesgo ..... 18
**Tabla 11.** Identificación del Control ..... 21
**Tabla 12.** Atributos del diseño del control ..... 22
**Tabla 13.** Atributos de la implementación del control ..... 23
**Tabla 14.** Atributos de la valoración del control ..... 23
**Tabla 15.** Efectividad del Control ..... 24
**Tabla 16.** Calificación diseño del control ..... 24
**Tabla 17.** Calificación del diseño del control ..... 25
**Tabla 18.** Calificación implementación del control ..... 25
**Tabla 19.** Calificación de la implementación del control ..... 25
**Tabla 20.** Calificación valoración del control ..... 25
**Tabla 21.** Calificación de la valoración del control ..... 26
**Tabla 22.** Efectividad del control ..... 26
**Tabla 23.** Posibles tratamientos según las Zonas del mapa de calor ..... 29
**Tabla 24.** Tabla de priorización de tratamiento de riesgo ..... 32
**Tabla 25.** Descripción amenaza, vulnerabilidad y riesgo de autenticación digital ..... 34
**Tabla 26**. Equivalencia autenticación digital y nivel de impacto del riesgo ..... 34
**Tabla 27.** Equivalencia nivel de riesgo inherente frente al nivel de confianza ..... 35
**Tabla 28.** Atributos de nivel de confianza ..... 35
**Tabla 29.** Monitoreos y seguimientos gestión de riesgos de seguridad de la información ..... 41
**Tabla 30.** Tabla nivel de indicador EMTI ..... 42
**Tabla 31.** Tabla nivel de indicador EGR ..... 42
**Tabla 32.** Tabla nivel de indicador AGRSI ..... 43
**Tabla 33.** Tabla de control de cambios ..... 45

## 1. Introducción

La Oficina de Seguridad de la Información como responsable de la gestión de riesgos de seguridad de la información y protección de datos personales, considera importante y relevante incluir dentro de su análisis insumos esenciales que soporten el desarrollo metodológico de una manera eficiente, veraz, preciso, óptimo y claro, que le permitan contribuir en el logro de los objetivos estratégicos de la entidad y el desarrollo económico del país.

Es por ello, que se identifica como punto de partida para el desarrollo metodológico, los aspectos relevantes para la entidad como; el contexto interno y externo, las necesidades y expectativas de las partes interesadas, los objetivos estratégicos, misión, visión, la caracterización de los procesos, los objetivos de los procesos y el impacto de la cadena de valor; elementos que se encuentran inmersos y alineados con el desarrollo del OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – MSPI DIAN.

A su vez, la DIAN cuenta con políticas para la gestión de riesgos de seguridad de la información y protección de datos personales, las cuales, proporcionan la declaración por parte de la Dirección General de la DIAN, de sus intenciones para la identificación, valoración, tratamiento, monitoreo y mejora continua de los riesgos de seguridad de la información y protección de datos personales.

Como base importante, cabe destacar que se definen y establecen los roles y responsables que hacen parte de la gestión de riesgos de seguridad de la información, los cuales, participan activamente en todo el desarrollo del ciclo metodológico.

La metodología establecida para la gestión de los riesgos de seguridad de la información está basada y armonizada con los lineamientos consignados en los siguientes documentos:

- ✓ “Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 - noviembre de 2022” del Departamento Administrativo de la Función Pública-DAFP y la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República
- ✓ Anexo Técnico 4, “Modelo Nacional de Gestión de Riesgos de seguridad de la información en Entidades Públicas” – Versión 4 de octubre de 2021 de MINTIC.

Por último, es importante mencionar que los activos de información considerados de alta criticidad, activos reconocidos como información reservada, información clasificada, ciber-activos y/o activos con autenticación digital tienen un papel importante dentro del desarrollo metodológico de la gestión de riesgos de seguridad de la información, así como, las vulnerabilidades que pueden afectarlos, las amenazas que pueden ser aprovechadas y los controles identificados para mitigar los riesgos identificados.

La gestión de riesgos de seguridad de la información bajo la responsabilidad de la Oficina de Seguridad de la Información – OSI, hace parte de la gestión de riesgos de la entidad, por lo tanto, se encuentra en sincronía con sus lineamientos, metodologías, documentación y definiciones.

## 2. Objetivo

Gestionar los riesgos de seguridad de la información y protección de datos personales, en la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - UAE DIAN, con el fin de facilitar su identificación, análisis, valoración, tratamiento, monitoreo y mejoramiento.

## 3. Planificación de la gestión de riesgos de seguridad de la información

### 3.1. Contexto interno y externo

La Oficina de Seguridad de la Información- OSI, efectuó un análisis del contexto interno y externo, previo al desarrollo metodológico de la gestión de riesgos de seguridad de la información y protección de datos personales, es por ello por lo que armoniza y sincroniza sus definiciones metodológicas con el análisis Político, Económico, Sociocultural, Tecnológico, Ecológico y Legal, (PESTEL por sus siglas en inglés) elaborado por parte de la OSI, el cual puede ser consultado en el documento *análisis PESTEL V1.0.docx*

### 3.2. Identificación de las necesidades y expectativas de las partes interesadas

La Oficina de Seguridad de la Información- OSI, efectuó un análisis de las partes interesadas, y a su vez, lo que es identificado como sus necesidades y expectativas, previo al desarrollo metodológico de la gestión de riesgos de seguridad de la información y protección de datos personales, es por ello por lo que armoniza y sincroniza sus definiciones metodológicas con el análisis elaborado por parte de la OSI, el cual puede ser consultado en el documento de *planes e identificación de las necesidades y expectativas de las partes interesadas.docx*

### 3.3. Alcance de la gestión de riesgos de seguridad de la información

La Oficina de Seguridad de la Información – OSI, a través del OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – MSPI DIAN, el cual incluye la gestión de riesgos de seguridad de la información en lo que corresponde a la Integridad, Disponibilidad y Confidencialidad y la Protección de Datos Personales y Privacidad, determina que su alcance abarca todos los procesos que hacen parte de la UEA-DIAN, y a su vez, a los activos de información que se identifiquen en cada uno de estos procesos de acuerdo con las definiciones del numeral *3.10.2 Activos de información objeto de la gestión de riesgos de seguridad de la información y protección de datos personales*. (Para más información remitirse al documento OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – MSPI DIAN)

### 3.4. Definición del perfil de riesgo DIAN

La DIAN a través de la Oficina de Seguridad de la Información – OSI, identifica las siguientes definiciones para establecer su perfil de riesgo

- **Nivel de riesgo[1]:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos (corrupción, operativos, financiero, ciberseguridad etc.) que la entidad debe o desea gestionar.
- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

**a) Apetito del riesgo**

El apetito de riesgo que se define para los riesgos de seguridad de la información, son aquellos riesgos que luego de determinar su nivel de impacto y probabilidad (residual) se ubiquen en la zona denominada como **aceptable.** Los riesgos que no queden ubicados en esta zona deben seleccionar un tipo de tratamiento aprobado por la entidad.

**b) Tolerancia del riesgo**

La tolerancia al riesgo establecido por la entidad es para aquellos riesgos que se ubiquen en la zona determinada como **moderado.** Para los riesgos que se encuentren ubicados en esta zona se debe seleccionar un tipo de tratamiento aprobado para la entidad.

**c) Capacidad del riesgo**

La capacidad máxima del riesgo establecido por la entidad es para aquellos riesgos que se ubiquen en la zona determinada como **importante o inaceptable.** En esta zona la entidad comienza a identificar que pueden verse afectados el logro de sus objetivos, por lo tanto, determina que los riesgos que se encuentren ubicados en esta zona no son admisibles y se debe seleccionar un tipo de tratamiento aprobado, con el objetivo de que los riesgos sean llevados a las zonas de tolerancia o dentro del apetito del riesgo de la entidad. Este tratamiento debe ser conocido por el Comité Institucional Estratégico.

### 3.5. Alineación con la política de gestión de riesgos de seguridad de la información

La Oficina de Seguridad de la Información – OSI, alinea las definiciones de su metodología, con los lineamientos establecidos en la política de gestión de riesgos de seguridad de la información y la política para la protección de datos personales, las cuales, reflejan las intenciones, el liderazgo y el compromiso de la Dirección General y la alta gerencia. Las políticas para la gestión de seguridad de la información pueden ser identificadas dentro del documento OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – MSPI DIAN y en el caso de las políticas para la protección de datos personales pueden ser consultadas en la circular 001 de 2019 o aquella que la modifique.

Así mismo, las definiciones metodológicas para la gestión de riesgos de seguridad de la información se encuentran en sincronía con los lineamientos establecidos en las políticas de gestión de riesgos de la entidad a través de la Coordinación de Procesos y Riesgos.

[1] *Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5 de noviembre de 2020*

### 3.6. Análisis de los objetivos de la entidad y los objetivos de los procesos

Previo al inicio de la gestión de riesgos de seguridad de la información, debe realizarse el análisis e interpretación de los objetivos estratégicos de la entidad y los objetivos estratégicos de los procesos y/o áreas. Lo anterior es importante, toda vez que únicamente se deben identificar y gestionar los riesgos que impacten el logro de estos objetivos; todo riesgo que no cumpla con esta condición, no se debe considerar dentro de la gestión de riesgos de seguridad de la información. A excepción de los riesgos asociados a la protección de la información personal del titular, que no necesariamente están involucrados con los objetivos estratégicos de la entidad.

A su vez la gestión de riesgos de seguridad de la información la cual incluye los riesgos de protección de datos personales y ciberseguridad se sincroniza con los objetivos declarados en la política de seguridad y privacidad de la información de la UAE-DIAN[2], estableciendo los lineamientos, las actividades, los seguimientos y la mejora continua requeridos para apoyar su logro.

### 3.7. Roles y responsabilidades

La Oficina de Seguridad de la Información- OSI, identifica los siguientes participantes junto con sus principales funciones, dentro del desarrollo metodológico para la gestión de riesgos de seguridad de la información:

- ✓ **Comité Institucional Estratégico (línea estratégica):** responsable de identificar y analizar la gestión del riesgo de seguridad de la información y da las directrices en caso de ser requerido la aplicación de mejoras[3].
- ✓ **Comité Institucional de Coordinación de Control Interno (línea estratégica): r**esponsable de analizar situaciones de eventos y riesgos críticos identificados en la entidad.
- ✓ **Dueños de los activos de información (primera línea de defensa)**: responsable(s) de realizar la identificación de los activos bajo su propiedad, para ejecutar las actividades de identificación, valoración y tratamiento de los riesgos de seguridad de la información. De igual forma, verificar la aplicación de controles que permitan la mitigación de los riesgos identificados y realizar seguimiento a los planes de tratamiento establecidos.
- ✓ **Enlaces de seguridad:** encargados de apoyar a la Oficina de Seguridad de la Información - OSI en la articulación de la ejecución de actividades para la gestión de riesgos de seguridad de la información.
- ✓ **Oficina de Seguridad de la Información – OSI (Segunda línea**)**:** es responsable a través del líder de riesgos de seguridad de la información y con el apoyo del líder de protección de datos personales de:

    a. Definir, actualizar, aprobar, publicar y socializar la metodología de gestión de riesgos de seguridad de la información definida para la UAE DIAN. (Teniendo en cuenta el decreto 1742 art 10 numeral 2. Funciones oficina seguridad de la información).
    b. Velar por el cumplimiento de las actividades y definiciones metodológicas para la gestión de riesgos de seguridad de la información.
    c. Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.

[2] https://www.dian.gov.co/Documents/POLITICA_GENERAL_DE_SEGURIDAD_Y_PRIVACIDAD_DE_LA_INFORMACION.pdf
[3] Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6 de noviembre de 2022

d. Realizar seguimientos periódicos a la gestión de riesgos de seguridad de la información realizado por la primera línea de defensa, los cuales, le permitan identificar posibles situaciones que estén en contravía con lo establecido en las definiciones metodológicas.
e. Brindar el acompañamiento requerido a la primera línea de defensa para el desarrollo metodológico de la gestión de riesgos de seguridad de la información.
f. Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información, a través de los protocolos definidos en el documento PR-PEC-0242 planificación de la gestión de riesgos.

- ✓ **Oficina de Control Interno (Tercera línea):** responsable de adaptar sus procedimientos de seguimiento y evaluación, (principalmente a través de la auditoría interna) con el fin de establecer la efectividad de la aplicación de los controles para la mitigación de los riesgos.

Para complementar la anterior información, se incluye dentro del listado maestro de documentos el documento *matriz de roles y responsabilidades en seguridad* el cual incluye el detalle de los roles y responsabilidades específicas para la gestión de riesgos de seguridad de la información.

### 3.8. Gestión de riesgos de seguridad de la información en proyectos e iniciativas

La Oficina de Seguridad de la Información- OSI, considera importante que la gestión de riesgos de seguridad de la información sea concebida desde el diseño de los proyectos o iniciativas que desarrolla la entidad. Es por ello que determina las siguientes actividades que deben ser ejecutadas por los responsables de los proyectos o iniciativas:

I. Identificar a partir del contexto y alcance del proyecto el impacto sobre la seguridad de la información.
II. Identificar en los requerimientos del proyecto los relacionados con la seguridad de la información.
III. Identificar los activos de información que van a ser generados en las diferentes etapas del proyecto y que harán parte de la operación una vez finalizado éste. (Ejemplo: Análisis, diseño, desarrollo, pruebas e implementación).
IV. Identificar las vulnerabilidades y amenazas de los activos de información asociadas a seguridad de la información de acuerdo con lo definido en el *instrumento de consulta para la gestión de riesgos de seguridad de la información*.
V. Determinar los riesgos por cada tipo de activo de acuerdo con las amenazas y vulnerabilidades identificadas y apoyándose en las definiciones del *instrumento de consulta para la gestión de riesgos de seguridad de la información*.
- Determinar los controles mínimos que deben aplicarse teniendo en cuenta las características del activo, los cuales, deberán mantenerse una vez este finalice, de acuerdo con lo definido en el *instrumento de consulta para la gestión de riesgos de seguridad de la información.*

VI. Diseñar e implementar los controles mínimos requeridos sobre el activo de información de acuerdo con el tipo del activo.
VII. Hacer seguimiento a la gestión de riesgos de seguridad de la información a lo largo del proyecto.
*VIII.* Con cada salida en vivo en los ambientes productivos y al momento de finalización el proyecto, se debe realizar o actualizar el registro de los activos de información y ejecutar la gestión de riesgos de seguridad de la información en la herramienta GRC, de acuerdo con lo definido en la *CT-IIT-0079 Cartilla para la Gestión de Activos de Información* y en este documento en las secciones *3.10 Gestión de riesgos de seguridad de la información, 3.11 Identificación y*

*evaluación de los controles existentes, 3.12 Calculo de riesgo residual, 3.13 Definición del tratamiento de los riesgos, 3.14 Aprobación de riesgos, 3.15 Protocolo para la aceptación del riesgo, 3.16 Seguimiento a los planes de tratamiento de riesgos definidos.(Esta actividad deberá completarse como máximo a los 15 días hábiles a la salida en vivo).*

De otra parte, como parte de la gestión de riesgos de seguridad de la información en proyectos, se debe determinar el nivel de confianza de la autenticación digital de los trámites que serán generados, modificados o revisados en el alcance del proyecto, de acuerdo con lo definido en el numeral *3.20 Identificación del nivel de confianza para la autenticación digital* de esta cartilla. Se deben implementar los controles definidos en dicha sección de acuerdo con el nivel de confianza establecido.

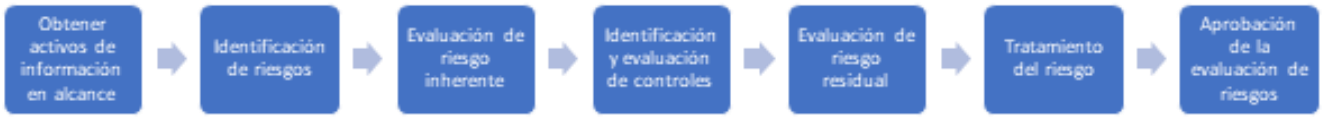
Durante el desarrollo del proyecto los riesgos de seguridad de la información deben registrarse en la M*atriz de Riesgos de Seguridad de la Información para Proyectos* dispuesta por la OSI y anexa a este documento.

## 3.9. Recursos para la gestión de riesgos de seguridad de la información

La Oficina de Seguridad de la Información – OSI, a través del Modelo de Seguridad y Privacidad de la información MSPI-DIAN, determina los métodos que se deben utilizar para disponer y asignar los recursos para su completa gestión; este análisis incluye los recursos para la gestión de riesgos de seguridad de la información. (Para más información por favor remitirse al documento OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – MSPI DIAN Numeral 5.4.1 Recursos)

## 3.10. Gestión de riesgos de seguridad de la información

La gestión de riesgos de seguridad de la información seguirá los siguientes pasos para el desarrollo metodológico:




### 3.10.1. Identificación de activos de información para la gestión de riesgos de seguridad de la información

La entrada más importante para la gestión de riesgos de seguridad de la información es identificar y clasificar los activos que serán tenidos en cuenta en los análisis para la identificación de los riesgos que tiene la organización y sus niveles de impacto y probabilidad.

### 3.10.2. Activos de información objeto de la gestión de riesgos de seguridad de la información

Para la identificación de los activos de información que deben ser objeto del análisis de riesgos, se deben generar un reporte de la herramienta GRC de acuerdo al manual MN-IIT-0075 manual de usuario para los riesgos de seguridad de la información – GRC NOVASEC.

Luego de realizar la generación del reporte se deben seleccionar los activos que cumplan con los siguientes criterios:

- **Activos de información con valoración "Alta":** los activos de información cuya valoración final tengan como resultado un nivel "ALTA".
- **Activos considerados Infraestructura Crítica Cibernética-ICC:** activos de información que en la sección de valoración hayan sido catalogados como "Infraestructura Crítica Cibernética".
- **Activos con Datos Personales:** activos de información que en el momento de su identificación contengan datos personales sensibles, semiprivados o privados.
- **Activos relacionados con autenticación digital:** activos de información tipo software que requieran autenticación digital
- **Activos con valoración con Disponibilidad "Alta":** activos de información cuya valoración final en la perspectiva de "Disponibilidad" tengan como resultado un nivel "ALTA".

### 3.10.3. Aspectos para considerar en la identificación de riesgos

Una vez identificados los activos de información, sobre los cuales se va a desarrollar la metodología de gestión de riesgos, se deben considerar las siguientes variables:

**Área/proceso:** se deben gestionar los riesgos de aquellos activos de información que pertenezcan a la misma área.

**Tipo[4]:** de acuerdo con el tipo de activo (información, software, recurso humano, servicio, hardware, infraestructura física) se deben identificar los riesgos, amenazas, vulnerabilidades y controles con base en la información descrita en el *Instrumento de consulta para la gestión de riesgos de seguridad de la información* en las tablas de vulnerabilidades, amenazas, controles y análisis de riesgos tipo.

### 3.10.4. Estructura para describir el riesgo

La descripción del riesgo se construye de acuerdo con la siguiente estructura:

La VULNERABILIDAD puede materializar una(s) AMENAZA(s), lo cual causaría el NOMBRE RIESGO (Pérdida de la confidencialidad / integridad / disponibilidad) del ACTIVO DE INFORMACIÓN.

En la siguiente tabla de ejemplo, se relacionan los datos del riesgo identificado y la forma de describirlos.

[4] *Fuente: Guía para la gestión y clasificación de activos de información, MinTic, versión 1.0 de marzo de 2016*

| ACTIVO | TIPO DE RIESGO | DESCRIPCIÓN DEL RIESGO | AMENAZA | VULNERABILIDADES |
|---|---|---|---|---|
| Base de datos de nómina | Pérdida de la integridad | La falta de políticas de seguridad de la información puede facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina. | Modificación no autorizada | Falta de políticas de seguridad de la información |

***Tabla 1**. Ejemplo de descripción de riesgos*

### 3.10.5. Identificación de amenazas, vulnerabilidades y riesgos tipo

Una vez identificados y seleccionados los activos a los cuales se aplicarán los análisis para la gestión de riesgos de seguridad de la información, se debe identificar el atributo (disponibilidad, integridad o confidencialidad) predominante sobre el cual se va a clasificar el riesgo de la siguiente manera:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Los tipos de amenazas son los siguientes:

- AI: Ataques Intencionados
- DN: Desastres Naturales
- DOI: De Origen Industrial
- EFNI: Errores y Fallos No Intencionados
- ADP: Afectación Datos Personales
- CI: Ciberseguridad

Para identificar las amenazas, vulnerabilidades y los riesgos tipo a las que está expuesto cada activo de información, es necesario contar con el apoyo del dueño del activo y de su equipo de trabajo. Adicionalmente, se puede recurrir a la revisión de los eventos e incidentes presentados previamente y/o a los catálogos de amenazas disponibles en organismos industriales, compañías de seguros o metodologías de valoración de riesgos. (Ver documento *Instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de vulnerabilidades, Tabla de Amenazas, Tabla de Controles, Tabla de riesgos tipo).

Es importante tener claro que se deben escoger vulnerabilidades verdaderas, es decir, debilidades o fallas que realmente existan en el activo de información o en los controles, y que puedan ser explotadas por una o más amenazas. (numeral 8.2.1.5 NTC-ISO/IEC 27005).

También es importante tener en cuenta la siguiente recomendación de MINTIC:

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

### 3.10.6. Identificar los riesgos Inherentes de seguridad de la información

A continuación, se describen las actividades metodológicas que deben ser desarrolladas para el cálculo del riesgo inherente considerando los niveles iniciales de probabilidad e impacto.

### 3.10.7. Cálculo de la probabilidad inherente

La probabilidad será evaluada a partir de la combinación de los factores: probabilidad por frecuencia de uso y probabilidad por histórico de ocurrencia.

#### A) Probabilidad por frecuencia de uso

La probabilidad por frecuencia de uso basa su medición en la probabilidad de la materialización de un riesgo, derivado del número de veces que es utilizado un determinado activo de información. De este modo, la probabilidad inherente por frecuencia de uso resultará del número de veces que se usa el activo en el periodo de 1 año.

La probabilidad por frecuencia de uso se determina de acuerdo con la siguiente tabla:

| Escala | Por frecuencia de Uso | Probabilidad |
|---|---|---|
| Muy Alta | El activo de información es usado más de 5000 veces al año. | 100% |
| Alta | El activo de información es usado de 501 a 5000 veces al año. | 80% |
| Media | El activo de información es usado de 25 a 500 veces al año. | 60% |
| Baja | El activo de información es usado de 3 a 24 veces al año. | 40% |
| Muy baja | El activo es usado como máximo 2 veces al año | 20% |

***Tabla 2**. Probabilidad por frecuencia de uso.*
*Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 – DAFP-2020 y ajustado por la UAE -DIAN*.

A continuación, se brindan algunos ejemplos para dar claridad sobre el significado de “uso” para cada uno de los tipos de activos de información:

- **Software:** el significado de “uso” se refiere a la cantidad de horas al año que este activo de información se encuentra en funcionamiento. Una (1) hora se toma como una (1) vez. No debe confundirse que el “uso” es las veces que se abre o cierra un software determinado. Ejemplo: Cantidad de horas que el software GRC se encuentra en funcionamiento para ser utilizado por los funcionarios de la entidad.

- **Hardware:** el significado de "uso" se refiere a la cantidad de horas al año que este activo de información se encuentra en funcionamiento. Una (1) hora se toma como una (1) vez. Ejemplo: Cantidad de horas que el token físico se utiliza para el acceso a una plataforma.

- **Servicios:** el significado de "uso" se refiere a la cantidad de horas al año que este activo de información se encuentra en funcionamiento. Una (1) hora se toma como una (1) vez. No se debe confundir que el "uso" para este tipo de situaciones es las veces que se autentica el servicio electrónico determinado. Ejemplo: Cantidad de horas que el servicio electrónico que consulta el estado de declaración de renta de las personas naturales se encuentra habilitado.

- **Infraestructura física:** el significado de "uso" se refiere al número de veces al año que las personas interactúan con la infraestructura física. Ejemplo: Cantidad de veces que las personas acceden o salen del Data Center principal.

- **Recurso Humano:** el significado de "uso" se refiere a la cantidad de veces al año en la que el individuo o grupo realiza actividades relacionadas con la situación de riesgo. Ejemplo: El riesgo identificado es la modificación involuntaria de la información de nómina; con base en esto, cuantas veces se realizan cambios en la información de nómina por parte del recurso humano.

- **Información:** el significado de "uso" se refiere a la cantidad de veces al año que se utiliza la información para una determinada actividad. Ejemplo: Cantidad de veces que se utiliza la información para la elaboración de los informes a la alta dirección.

**B) Probabilidad por histórico de ocurrencia:**

La probabilidad por histórico de ocurrencia basa su medición en los resultados de los riesgos materializados sobre un activo de información. De este modo, para el cálculo de la probabilidad inherente por ocurrencia se tomará la información del número de veces que se ha materializado el riesgo en un determinado activo de información a través del tiempo.

| Escala | Por histórico de ocurrencia | Probabilidad |
|---|---|---|
| Muy Alta | El riesgo se ha materializado por lo menos 1 vez en el último mes. | 100% |
| Alta | El riesgo se ha materializado por lo menos 1 vez en el último trimestre. | 80% |
| Media | El riesgo se ha materializado por lo menos 1 vez en el último semestre | 60% |
| Baja | El riesgo se ha materializado por lo menos 1 vez en el último año | 40% |
| Muy Baja | El riesgo no se ha materializado en el último año | 20% |

***Tabla 3.*** *Probabilidad por histórico de ocurrencia*
*Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 – DAFP-2020 y ajustado por la UAE -DIAN.*

### C) Probabilidad Inherente Final

Se define un promedio ponderado para el cálculo de la probabilidad inherente final; se han determinado las siguientes proporciones medidas en términos porcentuales, para la probabilidad *por frecuencia de uso* y para la probabilidad por *histórico de ocurrencia:*

- Probabilidad por frecuencia de uso = 70%
- Probabilidad por histórico de ocurrencia = 30%

Con base en lo anterior, la fórmula para el cálculo de la *probabilidad final* tendrá la siguiente composición:

$$\boldsymbol{Probabilidad\ Inherente\ Final} = Resultado\ de\ la\ probabilidad\ por\ frecuencia\ de\ uso * (70\%) + Resultado\ de\ la\ probabilidad\ por\ historico\ de\ ocurrencia * (30\%)$$

La siguiente tabla ilustra las posibles combinaciones entre la probabilidad por *frecuencia de uso* y la probabilidad por *histórico de ocurrencia* dependiendo de los resultados obtenidos en el momento del análisis:

| | | **Probabilidad Final** | | | | |
|---|---|---|---|---|---|---|
| | | **Probabilidad por frecuencia de uso (70%)** | | | | |
| | | **20%** | **40%** | **60%** | **80%** | **100%** |
| **Probabilidad por histórico de ocurrencia (30%)** | **100%** | 44% | 58% | 72% | 86% | 100% |
| | **80%** | 38% | 52% | 66% | 80% | 94% |
| | **60%** | 32% | 46% | 60% | 74% | 88% |
| | **40%** | 26% | 40% | 54% | 68% | 82% |
| | **20%** | 20% | 34% | 48% | 62% | 76% |

***Tabla 4.*** *Probabilidad final*
*Fuente: Diseño propio de la UAE -DIAN, Oficina de Seguridad de la Información - OSI*.

Luego de realizar los analices para el cálculo de la probabilidad, el resultado se ubicará en los siguientes rangos

| Escala | Rango |
|---|---|
| Muy Alta | Entre 81% y 100% |
| Alta | Entre 61% y 80% |

| | |
|---|---|
| Media | Entre 41% y 60% |
| Baja | Ente 21% y 40% |
| Muy Baja | Entre 0% y 20% |

***Tabla 5*** *Tabla de rangos de la probabilidad identificada*
*Fuente: Diseño propio de la UAE -DIAN, Oficina de Seguridad de la Información - OSI*.

### 3.10.8. Evaluación del impacto inherente

Los factores utilizados para la medición del impacto son los siguientes, los cuales se alinean a la Gestión de Riesgo General definida por la entidad:

- Recaudo (dimensión económica)
- Presupuesto (dimensión económica)
- Legal
- Imagen/reputación.

Por cada uno de los factores de impacto se han determinado las siguientes escalas de evaluación:

| Valor/peso | Nivel de impacto | Recaudo (Económica) | Presupuesto (Económica) | Legal | Imagen Reputación |
|---|---|---|---|---|---|
| **20%** | **LEVE** | De 0 a 1000 Salarios Mínimos Legales Vigentes (SMLV). | De Cero a 4 Salarios Mínimos Legales Vigentes (SMLV). | Representa un impacto mínimo y en ocasiones imperceptibles para la entidad. | Es conocido por algunos funcionarios de la DIAN. El número de Peticiones Quejas Reclamos y Solicitudes (PQRS) es muy bajo menor a 100. |
| 40% | **MENOR** | de 1000 SMLV a 25 000 SMLV. | De 4 SMLV a 20 SMLV. | Se identifican las situaciones, pero no se generan investigaciones ni sanciones / No representa incumplimientos legales. | Es conocido por una o varias áreas de la DIAN, o en la seccional. Se pueden presentar de 100 a 1000 PQRS. |
| **60%** | **MODERADO** | De 25 000 SMLV a 500 000 SMLV. | De 20 SMLV a 400 SMLV. | Genera investigaciones, pero sin sanción. | Es conocido en la totalidad de la DIAN, pero no trasciende a los medios. Se pueden |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | presentar 1000 o más PQRS |
| **80%** | **MAYOR** | De 500 000 SMLV a 1 000 000 SMLV. | de 400 SMLV a 2000 SMLV. | Genera investigaciones con sanciones internas / incumplimientos legales internos o externos /Demandas. | Es conocido en los medios de comunicación a nivel local (ciudad, departamento). |
| **100%** | **CATASTROFICO** | Mayor a 1 000 000 SMLV. | Mayor a 2000 SMLV. | Genera investigaciones externas/ multas /Intervención/Reportes de entes de Control / Investigaciones penales / Entes Internacionales. | El riesgo o sus consecuencias es conocido en los medios de comunicación masiva a nivel nacional e internacional. |

***Tabla 6**. Dimensiones de Impacto.*
*Fuente: Construcción propia. UAE DIAN 2023 Oficina de Seguridad de la Información OSI, adaptado de la guía de riesgos operativos de la UEA-DIAN*

### 3.10.8.1. Impacto inherente final

Se define un promedio ponderado para el cálculo del impacto final; se han determinado las siguientes proporciones medidas en términos porcentuales, para el impacto por *Recaudo (económica),* para el impacto por *Presupuesto (económica),* para el impacto *Legal* y para el impacto por *Imagen/Reputación:*

Impacto económico: 40% = (Recaudo(20%)+Presupuesto(20%))

- Impacto legal = 30%
- Impacto imagen/reputación = 30%

Con base en lo anterior, la fórmula para el cálculo del *impacto económico* tendrá la siguiente composición:

$$\boldsymbol{Impacto\ economico} = Resultado\ del\ Recadudo * (20\%) + Resultado\ dePresupuesto * (20\%)$$

La fórmula para el cálculo del *impacto final* tendrá la siguiente composición:

$$\boldsymbol{Impacto\ Final} = Resultado\ del\ impacto\ económico * (40\%) + Impacto\ legal * (30\%) + Impacto\ imagen - reputación * (30\%)$$

**Impacto final:** El resultado del impacto final debe ubicarse en los siguientes rangos:

| Rango | Impacto Final |
|---|---|
| **Entre 0% y 20%** | Leve |
| **Entre 21% y 40%** | Menor |
| **Entre 41% y 60%** | Moderado |
| **Entre 61% 80%** | Mayor |
| **Entre 81% y 100%** | Catastrófico |

**Tabla 7.** *Impacto final*
*Fuente: Construcción propia. UAE DIAN 2023 Oficina de Seguridad de la Información OSI*

### 3.10.9. Evaluación del nivel de riesgo Inherente

Este se obtiene al combinar la evaluación de la probabilidad y el impacto para determinar el nivel de riesgo inherente. Este nivel indica la ubicación del riesgo en una de las siguientes zonas del mapa de calor:

| | | | |
|---|---|---|---|
| ACEPTABLE | MODERADO | IMPORTANTE | INACEPTABLE |

***Tabla 8.*** *Zonas del mapa de calor*

Las combinaciones posibles probabilidad-impacto y la zona donde se ubicará el riesgo inherente en el mapa de calor, se relacionan en la siguiente tabla:

| Nivel de severidad del riesgo | | |
|---|---|---|
| **Probabilidad** | **Impacto** | **Zona en el mapa de calor** |
| Muy baja | Leve | ACEPTABLE |
| Muy baja | Menor | ACEPTABLE |
| Baja | Leve | ACEPTABLE |
| Baja | Menor | ACEPTABLE |
| Media | Leve | ACEPTABLE |
| Alta | Leve | MODERADO |
| Muy Alta | Leve | MODERADO |
| Alta | Menor | MODERADO |
| Muy Alta | Menor | MODERADO |
| Media | Menor | MODERADO |
| Media | Moderado | MODERADO |
| Baja | Moderado | MODERADO |
| Muy baja | Moderado | MODERADO |

| Nivel de severidad del riesgo | | |
|---|---|---|
| **Probabilidad** | **Impacto** | **Zona en el mapa de calor** |
| Muy Alta | Moderado | IMPORTANTE |
| Alta | Moderado | IMPORTANTE |
| Media | Mayor | IMPORTANTE |
| Baja | Mayor | IMPORTANTE |
| Muy baja | Mayor | IMPORTANTE |
| Muy baja | Catastrófico | INACEPTABLE |
| Baja | Catastrófico | INACEPTABLE |
| Media | Catastrófico | INACEPTABLE |
| Alta | Mayor | INACEPTABLE |
| Alta | Catastrófico | INACEPTABLE |
| Muy Alta | Mayor | INACEPTABLE |
| Muy Alta | Catastrófico | INACEPTABLE |

***Tabla 9.*** *Nivel de severidad del riesgo*

En el mapa de calor se observan las zonas en las que quedan ubicados los riesgos:

| **Probabilidad** | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 100% | Muy Alta | Moderado | Moderado | Importante | Inaceptable | Inaceptable |
| | 80% | Alta | Moderado | Moderado | Importante | Inaceptable | Inaceptable |
| | 60% | Media | Aceptable | Moderado | Moderado | Importante | Inaceptable |
| | 40% | Baja | Aceptable | Aceptable | Moderado | Importante | Inaceptable |
| | 20% | Muy baja | Aceptable | Aceptable | Moderado | Importante | Inaceptable |
| | | | Leve 20% | Menor 40% | Moderado 60% | Mayor 80% | Catastrófico 100% |
| | | | | | **Impacto** | | |

***Tabla 10.*** *Mapa de calor con niveles de severidad del riesgo*

### 3.11. Identificación y evaluación de los controles existentes

Para la identificación, evaluación y monitoreo de los controles que mitiguen los riesgos de seguridad de la información se establecieron las siguientes actividades.

### 3.11.1. Planificación de la gestión de los controles

Dentro del plan de gestión de riesgos de seguridad de la información, se establecen las siguientes actividades que permitan medir los resultados de la gestión de los controles definidos para la mitigación de los riesgos:

- Incluir las áreas que tienen pendientes el desarrollo de actividades para la gestión de los controles.
- Incluir las fechas de revisión de la gestión de los controles por área
- Incluir las fechas de presentación de los resultados frente a los resultados de la gestión de los controles.

**Nota:** como parte del cumplimiento del decreto 612 de 2018, el cual contempla incluir la información del resultado de los planes de tratamiento de riesgos, se debe programar el envío de esta información al responsable de la consolidación antes del 20 de diciembre del año en curso.

### 3.11.2. Atributos para la evaluación individual de controles

En las siguientes tablas se relacionan los atributos de identificación, diseño, implementación y valoración de controles. Algunos atributos se tienen en cuenta para evaluación y otros son informativos y no tienen incidencia en el resultado de la efectividad.

#### a) Atributos de Diseño

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **Control** | Corresponde al nombre del control diseñado por la norma ISO 27002 para gestionar los riesgos identificados. | Diseño-Informativo |
| **Descripción** | Corresponde a la información detallada del control ISO 27002. Se debe escribir la funcionalidad del control. | Diseño-Informativo |
| **Responsable de diseño** | Dependencia encargada de diseñar el control. | Diseño-Informativo |
| **Responsable de implementación** | Dependencia encargada de que el control se implemente. | Diseño-Informativo |
| **Tipo de control** | **Preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Está diseñado para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.<br>Está encaminado a mitigar la probabilidad de ocurrencia del riesgo.<br>**Detectivo**: control accionado durante la ejecución del proceso. Detecta el riesgo, pero genera reprocesos. Está diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las | Diseño-Evaluación |

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| | acciones correspondientes. Está encaminado a mitigar la probabilidad de ocurrencia del riesgo.<br>**Correctivo**: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Está encaminado a mitigar el impacto por la materialización del riesgo. | |
| **Frecuencia** | El control debe tener una frecuencia específica de ejecución (diario, mensual, trimestral, anual, etc.) y esta debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la frecuencia se debe evaluar si el control previene o detecta de manera oportuna el riesgo. Cada vez que se releva un control, evaluar si la frecuencia en que se ejecuta el control ayuda a prevenir o detectar el riesgo de manera oportuna. | Diseño-Informativo |
| **Observaciones de implementación** | Contiene el detalle del control: responsable de ejecutarlo, la acción de control que realiza y un complemento. El complemento describe la frecuencia o periodicidad de ejecución, el propósito del control y las observaciones o qué hacer si se observan diferencias o aspectos que ya no se cumplen.<br>**Responsable de ejecutar el control**: identifica el cargo del servidor y la dependencia asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si el responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. En caso de que sea un control automático se identifica el sistema que realiza la actividad.<br>**Acción**: establece cómo se realiza la actividad de control. El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Se determina mediante verbos que indican la acción que deben realizar como parte del control.<br>**Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.<br>**Propósito del control**: el control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las amenazas que generan el riesgo (monitorear, verificar, validar, conciliar, comparar, revisar, cotejar, reportar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí | Diseño-Informativo |

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| | sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas.<br>**Observaciones o Desviaciones**: indica qué pasa si se observan diferencias o aspectos que ya no se cumplen. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas. | |
| **Responsable de implementación adicional** | Dependencia encargada de que los diseños adicionales sean implementados. | Diseño-Informativo |
| **Tipo de mitigación** | Corresponde a las opciones de mitigación que tiene el control:<br>**Impacto:** escoja esta opción si al momento de la mitigación, se redujo el impacto.<br>**Probabilidad:** escoja esta opción si al momento de la mitigación, se redujo la probabilidad.<br>**Impacto y Probabilidad:** escoja esta opción si al momento de la mitigación, se redujo el impacto y la probabilidad. | Diseño-Evaluación |
| **Porcentajes de mitigación** | Se calcula automáticamente de acuerdo con la cantidad de controles | Diseño-Evaluación |
| **¿Se ha implementado el control? Sí/No** | Corresponde a si alguna vez el control existente ha sido implementado | Implementación-Informativo |
| **Fecha de seguimiento** | Relacione la fecha en que se va a realizar el registro del seguimiento del control en la herramienta GRC. Formato AAAA-MM-DD | Diseño-Informativo |
| **Observaciones** | Relacione cualquier tipo de observación sobre el seguimiento de la calificación del control. Si no presenta observaciones, diligencia “No aplica”. | Diseño-Informativo |

***Tabla 11.*** *Identificación del Control*

**b) Atributos de Diseño del Control**

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **Nivel de mitigación** | La forma específica que asume la mitigación depende del grado de cumplimiento del objetivo para el que fue diseñado el control ante las amenazas determinadas y las vulnerabilidades que puedan existir.<br>**Alta:** ocurre cuando el control cumple su objetivo frente a la eliminación o mitigación de la amenaza y las vulnerabilidades se pueden subsanar fácilmente. | Diseño-Evaluación |

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| | **Media:** se presenta cuando el control cumple parcialmente su objetivo frente a la eliminación o mitigación de la amenaza y las vulnerabilidades son más significativas. | |
| **Forma de ejecución** | **Automático**: son actividades de procesamiento o validación de información que se ejecutan por un sistema, aplicativo y/o servicio informático de manera automática sin la intervención de personas para su realización.<br>**Semiautomático**: son controles que se llevan a cabo mediante el ingreso de datos a un sistema o aplicativo de manera manual.<br>**Manual**: son los controles que son ejecutados por una persona, por lo que tienen implícito el error humano. | Diseño-Evaluación |
| **Nombre del sistema donde se ejecuta el control** | Si la forma de ejecución (respuesta del punto anterior) es "Automático" o "Semiautomático", se debe especificar el nombre del sistema, servicio informático, programa o aplicativo donde se ejecuta el control, de lo contrario no aplica. | Diseño-Informativo |
| **Nivel de ejecución 1** | Se refiere al dónde se ejecuta del control, teniendo en cuenta para ello los siguientes niveles: Todos los niveles, Nivel central, Nivel local y delegado. | Diseño-Informativo |
| **¿El control está documentado? Sí/No/Parcial** | Corresponde a si el control está documentado en los procedimientos, lineamientos, instructivos, manuales u otros documentos del Sistema de Gestión de Calidad de la Entidad, como una actividad recurrente y formal. | Diseño-Evaluación |
| **Nombre de los documentos** | Si el control está parcial o totalmente documento (respuesta del punto anterior) diligenciar los códigos de los procedimientos, instructivos, formatos, manuales o demás documentos del Sistema de Gestión de Calidad; donde se encuentran relacionados los controles identificados y el cargo o dependencia responsables de su ejecución. | Diseño - Informativo |
| **Calificación diseño** | Cálculo diseño >= 27%: **Adecuado**<br><br>19% >= Cálculo diseño <= 26%: **Parcialmente adecuado**<br><br>0% > Cálculo diseño <= 19%: **Inadecuado** | Diseño-Evaluación<br><br>**Se calcula automáticamente** |

**Tabla 12.** Atributos del diseño del control

**c) Atributos de Implementación del Control**

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **¿El control deja evidencia de su ejecución? Sí/No** | El control deja un registro que permite evidenciar la ejecución del control (formato, lista de chequeo, actas u otros documentos o registros) | Implementación-Evaluación |

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **Nombre y tipo de archivo/soporte de la evidencia** | Corresponde a diligenciar el nombre y tipo del archivo/soporte de la evidencia. Si no existe dicho archivo y/o soporte, colocar "No aplica" | Implementación Informativo |
| **Ruta donde reposa la evidencia** | Corresponde a diligenciar la ruta donde reposa la evidencia. Si no existe un repositorio, colocar "No aplica" | Implementación Informativo |
| **Archivo soporte de la evidencia (Cargar sino se encuentra en repositorio oficial)** | Se refiere a que en caso de que no exista un repositorio se debe cargar el archivo/soporte de la evidencia en el repositorio oficial. Extensiones permitidas: pdf, jpeg, jpg, png, tif, rtf, zip. Tamaño máximo 5M | Implementación Informativo |
| **Frecuencia de ejecución del control** | **Siempre:** El control se ejecuta siempre que se realiza la actividad que conlleva al riesgo.<br>**Aleatorio:** El control se ejecuta aleatoriamente.<br>**Nunca:** El control no se ejecuta | Implementación-Evaluación |
| **Calificación implementación** | Cálculo implementación >= 16%: **Adecuada**<br>11%>= Cálculo implementación <= 15%: **Parcialmente adecuada**<br>0% > Cálculo implementación <= 10%: **Inadecuada** | Implementación Evaluación<br><br>**Se calcula automáticamente** |

**Tabla 13.** Atributos de la implementación del control

**d) Atributos de Valoración del Control:**

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **¿La evidencia es pertinente al control? Sí/No** | Se refiere a que si la evidencia existente es pertinente con el control. | Valoración-Evaluación |
| **¿La evidencia es completa frente al control? Sí/No** | Se refiere a que si la evidencia existente cubre completamente al control. | Valoración-Evaluación |
| **¿Se ha materializado el riesgo asociado a este control? Sí/No** | Corresponde a que si en alguna oportunidad el riesgo asociado a este control se ha materializado. | Valoración-Evaluación |
| **¿Existen hallazgos de auditoria asociados a este control? Sí/No** | Corresponde a que si este control ha tenido en alguna oportunidad hallazgos de auditoría. | Valoración-Evaluación |
| **Calificación valoración** | Cálculo valoración >= 7%: **Adecuada**<br>3% >= Cálculo valoración <= 6%: **Parcialmente adecuada**<br>0% > Cálculo valoración <= 2%: **Inadecuada** | Valoración-Evaluación<br><br>**Se calcula automáticamente** |

**Tabla 14.** *Atributos de la valoración del control*

### e) Sección seguimiento – Evaluación de Efectividad del control

| Atributos | Descripción | Evaluación del Control |
|---|---|---|
| **Nivel de efectividad** | Calculo efectividad >= 53%: **Efectivo**<br>38% <= Calculo efectividad <= 52%: **Efectivo con Oportunidad de Mejora**<br>0% > Calculo efectividad <= 37%: **Inefectivo** | Efectividad-Evaluación<br><br>**Se calcula automáticamente** |
| **Calificación efectividad** | Calculo efectividad >= 53%: **Efectivo**<br>38% <= Calculo efectividad <= 52%: **Efectivo con Oportunidad de Mejora**<br>0% > Calculo efectividad <= 37%: **Inefectivo** | Diseño-Evaluación<br><br>**Se calcula automáticamente** |
| **Plan de acción** | Corresponde a la necesidad o no de definición e implementación de plan de acción para el tratamiento del control (aplica controles Efectivos con oportunidad de mejora o controles inefectivos) | Diseño-Informativo<br><br>**Se calcula automáticamente** |

**Tabla 15.** *Efectividad del Control*

### f) Criterios para calificación de controles

A continuación, se describen los criterios y valores obtenidos en la evaluación de los controles, con el fin de determinar su efectividad:

**Calificación Diseño del control**: un control está bien diseñado si provee un aseguramiento razonable, es decir, si es adecuado para mitigar o eliminar la amenaza y las vulnerabilidades se pueden subsanar fácilmente.

Las escalas de calificación son automáticas y se determinan teniendo en cuenta las diferentes combinaciones de los atributos del diseño del control como se muestran a continuación:

| Calificación diseño del control | | | |
|---|---|---|---|
| Atributo | Aspecto evaluado | | Peso |
| Diseño | Tipo | Preventivo | 15% |
| | | Detectivo | 10% |
| | | Correctivo | 5% |
| | Ejecución | Automático | 12% |
| | | Semiautomático | 8% |
| | | Manual | 4% |
| | Documentado | Sí | 8% |
| | | Parcial | 4% |
| | | No | 0% |

**Tabla 16.** *Calificación diseño del control*

| Diseño |
|---|

| Calificación | Criterio / Rango | Resultado |
|---|---|---|
| Diseño | Cálculo diseño >= 27% | Adecuado |
| | 19% >= Cálculo diseño <= 26% | Parcialmente adecuado |
| | 0% > Cálculo diseño <= 19% | Inadecuado |

***Tabla 17.*** *Calificación del diseño del control*

**Calificación Implementación del control:** la evaluación de la implementación del control, indica si en el momento de la evaluación el control se encuentra funcionando como está diseñado.

Las escalas de calificación son automáticas y se determinan teniendo en cuenta los atributos de Frecuencia de ejecución del control y Evidencia, como se muestra a continuación.

| Calificación implementación del control | | | |
|---|---|---|---|
| Atributo | Aspecto evaluado | | Peso |
| Implementación | Evidencia | Sí | 10% |
| | | No | 0% |
| | Frecuencia | Siempre | 10% |
| | | Aleatorio | 5% |
| | | Nunca | 0% |

***Tabla 18.*** *Calificación implementación del control*

| Implementación | | |
|---|---|---|
| Calificación | Criterio/Rango | Resultado |
| Implementación | Cálculo implementación >= 16% | Adecuada |
| | 11%>= Cálculo implementación <= 15% | Parcialmente adecuada |
| | 0% > Cálculo implementación <= 10% | Inadecuada |

***Tabla 19.*** *Calificación de la implementación del control*

**Calificación Valoración del control:** se valora el control en términos de la pertinencia y completitud de la evidencia, así como la materialización y hallazgos asociados al riesgo, de acuerdo con la siguiente escala

| Calificación valoración del control | | | |
|---|---|---|---|
| Atributo | Aspecto evaluado | | Peso |
| Valoración | Pertinencia | SÍ | 3% |
| | | NO | 0% |
| | Completitud | SÍ | 3% |
| | | NO | 0% |
| | Materialización | SÍ | 0% |
| | | NO | 2% |
| | Hallazgos | SÍ | 0% |
| | | NO | 2% |

**Tabla 20.** *Calificación valoración del control*

| Valoración | | |
|---|---|---|
| Atributo | Criterio/Rango | Resultado |
| Valoración | Cálculo valoración >= 7% | Adecuada |
| | 3% >= Cálculo valoración <= 6% | Parcialmente adecuada |
| | 0% > Cálculo valoración <= 2% | Inadecuada |

***Tabla 21.*** *Calificación de la valoración del control*

- **Efectividad individual del control:** se calcula por medio de la sumatoria de los valores obtenidos en la calificación de cada atributo (Diseño, Implementación y Valoración). Los resultados de esta evaluación se clasifican en:

- **Efectivo**: indica que el control establecido en su diseño y aplicación es seguro para mitigar o eliminar la causa que podría generar la materialización del riesgo.

- **Efectivo con oportunidad de mejora**: se refiere a un control que a pesar de que se encuentra determinado para mitigar o eliminar la causa debe mejorar su diseño o requiere ser documentado en el proceso y procedimientos y aplicarse en todos los niveles correspondientes.

- **Inefectivo**: esta calificación puede determinarse por la deficiencia en su diseño, no estar documentado en el proceso y procedimientos o la no aplicación de control.

A continuación, se describen los rangos para determinar la efectividad del control:

| Efectividad | | |
|---|---|---|
| Calificación Efectividad | Criterio/rango | Resultado |
| Efectividad del Control | Cálculo efectividad >= 53% | Efectivo* |
| | 38% <= Cálculo efectividad <= 52% | Efectivo con Oportunidad de Mejora |
| | 0% > Cálculo efectividad <= 37% | Inefectivo |

**Tabla 22.** *Efectividad del control*

La evaluación individual de efectividad en controles llegará máximo al 65%.

### 3.11.3. Evaluación efectividad conjunta de los controles

La evaluación individual de los controles mitiga máximo un 65% del riesgo asociado. Este cálculo se realiza automáticamente en la herramienta GRC.

Después de establecer el nivel de efectividad para cada control, se debe analizar la efectividad conjunta de todos los controles asociados para la mitigación del riesgo y así poder determinar el nivel de riesgo residual. El objetivo es determinar si la aplicación conjunta de los controles asociados al riesgo es suficiente para mitigarlo y cubrir las amenazas y vulnerabilidades identificadas.

Nota: La efectividad de los controles se calcula de manera proporcional al número de controles.

Para determinar la efectividad de la aplicación de los controles frente a la mitigación de un determinado riesgo, se debe verificar la posición en la que se ubica el riesgo en la matriz de calor de riesgo residual y con ello determinar si:

- Los controles son efectivos para mitigar el riesgo identificado, por lo tanto, se debe proceder a que el dueño del riesgo acepte este nuevo nivel de riesgo residual.
- Los controles son parcialmente efectivos y pese a su implementación, el riesgo residual no se ubica en las zonas de riesgo aceptable de la entidad, por lo tanto, se deben tomar medidas que permitan ubicar el riesgo en zonas aceptables por la entidad o escalar la situación al Comité Institucional Estratégico para que en este espacio se tome la decisión del tipo de tratamiento del riesgo que se debe seleccionar.
- Los controles no apoyan en la disminución sustancial del nivel de riesgo, por lo tanto, escalar la situación al Comité Institucional Estratégico para que en este espacio se tome la decisión del tipo de tratamiento del riesgo que se debe seleccionar.

A continuación, se relacionan las fórmulas que se aplican para el cálculo de la evaluación conjunta de controles:

**Distribución porcentual de los controles (DPC)**

$$\mathbf{DPC} = \left( \frac{100\%}{\#\ de\ controles\ asociados\ al\ riesgo} \right)$$

**Cálculo aporte de los controles a la mitigación del riesgo**

$$\mathbf{CAC} = (DPC * Evaluación\ efectividad\ individual\ del\ control\ \#1 + DPC * Evaluación\ efectividad\ individual\ del\ control\ \#2 \ldots)$$

**Cálculo riesgo residual**

$$\mathbf{RS} = Probabilidad\ o\ Impacto\ inherente\ inicial - CAC$$

En las fórmulas anteriores se describe el proceso teniendo como premisa que se analizan 2 controles; en caso de ser requerido, las veces que se repite el proceso es directamente proporcional al número de controles asociados al riesgo.

El resultado final después de evaluar todos los controles de manera conjunta será determinado como **probabilidad y/o impacto residual.** Significa que será el resultado de tomar el riesgo inherente, analizar la efectividad de sus controles asociados, para determinar la disminución de su probabilidad o impacto y así determinar el nuevo nivel de riesgo (riesgo residual).

Los cálculos son realizados de manera automática en la herramienta GRC-NOVASEC

### 3.11.4. Identificación de controles transversales

De acuerdo con los riesgos, amenazas y vulnerabilidades relacionadas en la etapa de identificación, se seleccionan uno o más controles, de los que se encuentran parametrizados en la herramienta, según el documento *instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de Controles, con el fin de tratar el riesgo asociado.

**Nota:** en la selección de los controles se debe determinar si el control es de diseño e Implementación transversal; en este caso la evaluación del control ya está calculada y únicamente nos va a ayudar para la mitigación del riesgo. En caso contrario debe desarrollar la evaluación de los controles como se describe en el contenido de este documento.

### 3.11.5. Evaluación de la Efectividad de los controles transversales en la herramienta GRC

Los controles transversales se aplican para toda la entidad y en general, su diseño, implementación y valoración corresponden a una dependencia específica de la UAE-DIAN. Por lo anterior, la dependencia responsable del diseño, implementación y valoración del control debe realizar su evaluación de acuerdo con lo descrito en el numeral *3.11 Identificación y evaluación de los controles existentes.* Así mismo, si como resultado de la evaluación, es necesario mejorar un control, la dependencia responsable debe adelantar las acciones de mejora.

A continuación, se relacionan los controles que son considerados como transversales para la entidad:

- Controles de la norma NTC-ISO/IEC 27001:2022 (ver documento *instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de Controles) están incluidos en la sección de controles transversales (Modulo de riesgos – Administración) para su evaluación
- Controles de seguridad en nube (ver documento *instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de Controles) están incluidos en la sección de controles a nivel de aplicación (Modulo de riesgos – Administración)
- Controles de protección de datos personales (ver documento *instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de Controles) están incluidos en la sección de controles a nivel de aplicación (Modulo de riesgos – Administración) para su evaluación
- Controles relacionados con la analítica de datos (ver documento *instrumento de consulta para la gestión de riesgos de seguridad de la información*; Tabla de Controles) están incluidos en la sección de controles a nivel de aplicación (Modulo de riesgos – Administración)

Existen controles identificados como trasversales, los cuales, tienen un diseño, implementación y valoración centralizada, lo que significa que aplicación puede ayudar a mitigar uno o más riesgos asociados a un activo de información, sin embargo, estos controles también pueden evaluarse independientemente en cada proceso y para cada activo de información.

Por otra parte, existe la posibilidad que la dependencia pueda identificar controles exclusivos para un proceso en específico, los cuales, no se encuentran categorizados dentro de los controles trasversales. Para estos casos, el responsable de la dependencia deberá realizar todo el proceso en la herramienta lo cual incluye el registro, valoración seguimiento y mejora continua de acuerdo con lo descrito en el numeral *3.11 Identificación y evaluación de los controles existentes.* Esta actividad estará apoyada por el enlace de seguridad y en determinados casos cuando se considere necesario, podrá solicitar el

apoyo a la Oficina de Seguridad de la Información. Así mismo, si como resultado de la evaluación, es necesario mejorar un control, la dependencia responsable debe adelantar las acciones de mejora.

### 3.12. Cálculo de riesgo residual

Una vez aplicados los controles se realiza el cálculo del riesgo residual con base en la disminución de la probabilidad y el impacto, dependiendo de la naturaleza de los controles, esto es calculado de manera automática en la herramienta GRC. El riesgo residual deberá ser aceptado por parte del dueño del proceso en el módulo de cumplimiento de la herramienta GRC.

### 3.13. Definición del tratamiento de los riesgos

El **tratamiento del riesgo** es la respuesta establecida por la primera línea de defensa (dependencias de la UAE DIAN) para la mitigación de los diferentes riesgos. En el momento de evaluar las opciones para el tratamiento del riesgo, los dueños de los riesgos deben apoyarse de los resultados de los análisis de los riesgos y evaluar la relación costo-beneficio de las medidas de tratamiento.

Los dueños de los riesgos deben identificar la zona del mapa de calor donde esté ubicado el riesgo y decidir el tratamiento que se le puede dar.

Los riesgos que se encuentren en la zona “Aceptable”, no se les da ningún tratamiento.

Para los riesgos en la zona “importante”, “inaceptable” o “moderado” se decide si el riesgo se evita, comparte o reduce y de acuerdo con eso se definen los planes de acción.

| Nivel de riesgo – Zona en el mapa | Tratamiento | Definición de planes de acción |
|---|---|---|
| ACEPTABLE | Aceptar | Monitorear controles |
| MODERADO | Evitar, Compartir, Reducir | Planes a largo Plazo |
| IMPORTANTE | Evitar, Compartir, Reducir | Planes a mediano Plazo |
| INACEPTABLE | Evitar, Compartir, Reducir | Planes a corto plazo |

***Tabla 23.*** *Posibles tratamientos según las Zonas del mapa de calor*

#### 3.13.1. Planes de tratamiento de riesgos de seguridad de la información

El **plan de tratamiento de riesgos** define las acciones para gestionar los **riesgos** residuales ubicados en las zonas de riesgo inaceptable, importante o moderado y que en el momento de la valoración se escogió como opción de tratamiento “Reducir”. Los planes de tratamiento tienen como objetivo definir nuevos controles o mejorar el diseño y/o implementación de los controles actuales, estos deben quedar registrados en el plan de tratamiento de riesgos de acuerdo como se define en el documento “*MN-IIT-0075 Manual de Usuario para la Gestión de Riesgos de Seguridad de la Información-GRC NOVASEC*

Los riesgos residuales que quedan ubicados en estas zonas indican que los controles definidos no son suficientes y/o no son efectivos. Si los controles no son suficientes, es necesario identificar nuevos controles que permitan mitigar el riesgo.

### 3.14. Aprobación de riesgos

La aprobación de un riesgo se puede realizar en cualquiera de las secciones del módulo de riesgos en GRC (Identificación, Valoración o Tratamiento) y no es necesario aprobarlo en cada etapa. Esta aprobación, la debe realizar el Superior Jerárquico líder del proceso (director de Gestión / subdirector / jefe de Oficina / Director Seccional).

Es importante tener en cuenta que los riesgos aprobados ya no se pueden modificar, ni eliminar.

### 3.15. Protocolo para la aceptación del riesgo

La Oficina de Seguridad de la Información – OSI, determina como necesario que todos los riesgos tengan la aprobación por parte del dueño del riesgo, y a su vez, para aquellos riesgos aceptados pero que se encuentran ubicados fuera del apetito de riesgo de la entidad, establece como requisito que la aceptación final deba ser realizada por parte del Comité Institucional Estratégico. Así entonces, ha definido el siguiente protocolo:

1. El dueño del riesgo debe enviar al Jefe de la Oficina de Seguridad de la Información – OSI, un correo electrónico con la relación de(el) (los) riesgo(s) que desea aceptar y la justificación para cada uno de ellos.
2. El Jefe de la Oficina de Seguridad de la Información debe notificar su recibido y realizar comentarios frente a lo enviado por el dueño del riesgo.
3. El Jefe de la Oficina de Seguridad de la Información debe identificar los riesgos aceptados que se encuentran dentro del apetito del riesgo, y los riesgos ubicados en las zonas *inaceptable e importante*.
4. Para los casos de aquellos riesgos ubicados en las zonas *inaceptables e importantes*, el dueño del riesgo con el apoyo del Jefe de la Oficina de Seguridad de la Información o quien este designe, debe exponer la situación ante el Comité Institucional Estratégico; en este espacio se decidirá si se ratifica o declina la decisión tomada por parte del dueño del riesgo.
5. El Comité Institucional Estratégico determinará las acciones a seguir para los riesgos que no cuentan con una viabilidad para ser aceptados, estas acciones deben ser aceptadas por parte del dueño del riesgo y deben ser definidas como un plan de tratamiento de riesgos.

### 3.16. Seguimiento a los planes de tratamiento de riesgos definidos

Es responsabilidad del dueño del riesgo, realizar el seguimiento al cumplimiento de los planes de tratamiento de riesgos. Luego de ello, se debe determinar el nivel de su efectividad y ejecutar las actividades de calificación de controles y cálculo del nivel de riesgo residual definidos en el *3.11. Identificación y evaluación de los controles existentes* y *3.10. Gestión de riesgos de seguridad de la información* (respectivamente), de acuerdo con los siguientes lineamientos:

### 3.16.1. Criterios para el tratamiento de los riesgos de seguridad de la información

**a) Criterios para la aceptación del riesgo**

Es la situación en la que se decide no implementar ningún control que mitigue el riesgo; se debe cumplir por los menos 1 de los criterios establecidos para dar por ***aceptado*** el riesgo. Los criterios establecidos para este tipo de tratamiento del riesgo son:

- Si los riesgos se ubican en un nivel bajo de riesgo (aceptable)
- Si la relación de los costos generados por su materialización es menor respecto de los costos en los que habría que incurrir para crear e implementar los controles para su mitigación.
- Si la alta dirección de manera independiente decide aceptar el riesgo.
- Que no exista una amenaza cierta que explote las vulnerabilidades aplicadas

**Nota aclaratoria:** Si bien el dueño del riesgo puede tomar la decisión de aceptar el riesgo si se cumple alguno de los criterios mencionados, se debe realizar el seguimiento a estos riesgos aceptados, para verificar que no haya cambiado su condición a través del tiempo.

**b) Criterios para compartir el riesgo**: la aplicación de este criterio de tratamiento de riesgos implica el traslado del riesgo para que sea gestionado por un tercero ajeno a la entidad, el cual asume el costo en caso de la materialización del riesgo, para esto se pueden hacer:

- Contratos
- Asociaciones o Joint ventures
- Adquirir pólizas de seguros

**c) Criterios para evitar el riesgo**: se refiere a eliminar o abandonar las actividades de negocio que están generando el riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. Este criterio solo puede ser aplicado con la aprobación del Comité Institucional Estratégico.

**d) Criterios para reducir/mitigar el Riesgo**: este criterio se adopta para reducir la probabilidad, el impacto del riesgo, o ambos; esto conlleva la implementación de nuevos controles y/o la evaluación de los ya existentes.

**Nota:** este seguimiento debe ser actualizado en la herramienta GRC tanto en la calificación del control, como en el plan de acción definido en cada riesgo, con base en el documento *M-IIT-0075 Manual de usuario Gestión de Riesgos de Seguridad de la Información -GRC NOVASEC*.

### *3.17.* Criterios para priorizar el tratamiento del riesgo

Luego de realizar la evaluación de los riesgos y determinar que la opción para reducir el riesgo es la de "reducir/mitigar", es requerido priorizar los riesgos que puedan afectar de manera considerable a la entidad, verificando el siguiente orden:

| Nivel de riesgo identificado | Nivel de priorización |
|---|---|
| **Inaceptable** | Inmediata: Se debe establecer un plan de tratamiento en el menor tiempo que sea posible. |
| **Importante** | Urgente: Se necesita establecer un plan de tratamiento en un tiempo no mayor a 15 días calendario |
| **Moderado** | Relevante: Se requiere establecer un plan de tratamiento en un periodo de tiempo no mayor a 30 días calendario. |
| **Aceptable** | Indiferente: Al encontrarse dentro de la zona de apetito de riesgo, no es requerido un análisis de priorización. |

***Tabla 24.*** *Tabla de priorización de tratamiento de riesgo*

**Nota:** en dado caso que el riesgo a aceptar se encuentre por fuera del apetito de riesgo, se debe aplicar el protocolo para la aceptación del riesgo (*ver numeral 3.15 Protocolo para la aceptación del riesgo*).

### 3.18. Resultados finales de la gestión de riesgos de seguridad de la información

La entidad determina si después de ejecutar las actividades incluidas en la metodología, el resultado de los riesgos residuales es satisfactorio respecto a las definiciones de *nivel de riesgo*, *apetito del riesgo, tolerancia al riesgo*, *capacidad de riesgo.*

En determinado caso que los resultados no sean satisfactorios comparados con el perfil de riesgo de la entidad, se debe ejecutar nuevamente las actividades incluidas dentro de la metodología con el fin de reducir el riesgo al máximo, de lo contrario se debe optar por decidir por otro tipo de tratamiento diferente al de “reducir/mitigar”.

Los riegos clasificados como *inaceptables, importantes o moderados* que no hayan sido mitigados con los controles existentes posterior a la aplicación de los planes para el tratamiento de riesgo, y hayan sido aceptados por parte del dueño del riesgo de acuerdo con lo definido en el protocolo de aceptación del riesgo *(ver numeral 3.15 Protocolo para la aceptación del riesgo*), deben ser escalados al **Comité Institucional Estratégico**.

El escalamiento de los riesgos *inaceptables*, *importantes* o moderados debe llevarse a cabo de la siguiente forma:

a) Previo a la presentación de seguimiento de la gestión integral de riesgo al Comité Institucional Estratégico, la Oficina de Seguridad de la Información - OSI, deberá determinar cuáles riesgos han sido calificados recientemente (desde el último Comité Institucional Estratégico al que se presentó el seguimiento) como riesgos *inaceptables*, *importantes o moderados*, con el fin de presentar dentro de la agenda estos riesgos y los tratamientos establecidos, con el propósito de comunicar y obtener una retroalimentación. Los riesgos mencionados en esta sección deberán contar con la aceptación por parte del dueño de este.

b) También debe revisarse si existen riesgos adicionales/nuevos que hayan sido identificados y hayan sido calificados como *inaceptables* o *importantes*, y que de acuerdo con su criticidad se haya considerado presentar de forma prioritaria en el Comité Institucional Estratégico o la búsqueda de un espacio fuera del tiempo establecido para el seguimiento.

c) De acuerdo con la criticidad de los riesgos presentados y conforme las recomendaciones del Comité Institucional Estratégico, se debe considerar si es necesario trasladar la situación a una instancia mayor.

d) Conforme al pronunciamiento del Comité Institucional Estratégico, la instancia que es la encargada de la última decisión podrá modificar los planes de tratamiento o incluir controles o acciones adicionales que se hayan considerado con el fin de mitigar los riesgos, y con base en un análisis de costo beneficio.

### 3.19. Actualización de nivel de riesgo derivado de incidentes

Cada vez que se identifique un incidente que afecte la gestión de seguridad de la información y protección de datos personales, el dueño del activo de información relacionado con el incidente debe:

- Establecer si el incidente presentado se encuentra relacionado con un riesgo ya identificado, y de ser así, el dueño del riesgo debe actualizar el nivel del riesgo a través de la ejecución de las actividades incluidas en la metodología para la gestión de riesgos de seguridad de la información.
- Si el incidente presentado **NO** se encuentra relacionado con un riesgo ya identificado, se debe identificar el riesgo por parte del dueño del activo a través de la ejecución de las actividades incluidas en la metodología para la gestión de riesgos de seguridad de la información.
- Si el activo de información asociado al incidente no se encuentra incluido en la gestión de riesgos de seguridad de la información, debe revisarse la valoración del activo de información con base en las definiciones del documento CT-IIT-0079 Gestión de activos de información, actualizarla y en el caso de que aplique, ejecutar la metodología para la gestión de riesgos de seguridad de la información.

### 3.20. Identificación del nivel de confianza para la autenticación digital

La UAE-DIAN identifica su exposición frente a los trámites ciudadanos a través de servicios digitales que requieran de algún tipo de autenticación digital y por lo tanto requiere determinar el nivel de confianza con base en la exposición del trámite o servicio. El nivel de confianza se determina por cada trámite o servicio digital implementado en la entidad y se basa en la medición semicuantitativa de:

| Amenaza | Vulnerabilidad | Riesgo |
|---|---|---|
| **Falsificación de derechos, sobre el activo de software (tramites y/o servicios digitales).** | Ausencia o debilidades en los mecanismos de identificación y autentificación, como la autentificación de usuario | La ausencia o debilidades de mecanismos de identificación y autenticación permiten la falsificación de derechos digitales lo cual causaría pérdida de confidencialidad de los activos de software que |

| | | |
|---|---|---|
| | | soportan los trámites y/o servicios |

***Tabla 25.*** *Descripción amenaza, vulnerabilidad y riesgo de autenticación digital*

La calificación de este riesgo debe realizarse por cada trámite identificado en la entidad basado en las definiciones de probabilidad del numeral *3.10.7. Cálculo de la probabilidad inherente* de este documento y con la siguiente calificación del impacto:

| Valor/peso | Nivel de impacto | Riesgo de Autenticación Errónea |
|---|---|---|
| **20%** | **LEVE** | La autenticación errónea o suplantación de identidad no tiene efectos adversos en la información o trámites realizados por la entidad. |
| **40%** | **MENOR** | La autenticación errónea o suplantación de identidad conlleva revelación de documentos públicos. |
| **60%** | **MODERADO** | La autenticación errónea o suplantación de identidad conlleva revelación de documentos confidenciales o sensibles. |
| **80%** | **MAYOR** | La autenticación errónea o suplantación de identidad conlleva pérdida de integridad en la información |
| **100%** | **CATASTROFICO** | La autenticación errónea o suplantación de identidad conlleva pérdida de integridad y completitud en la información o riesgo de fraude en el trámite o servicio. |

***Tabla 26****. Equivalencia autenticación digital y nivel de impacto del riesgo*

El resultado del cálculo de la probabilidad se ubicará en los rangos indicados en la ***Tabla 5.*** *Tabla de rangos de la probabilidad identificada.*

Luego de calcular la probabilidad y el impacto inherente para los trámites relacionados con autenticación digital, los resultados se ubicarán en el mapa de calor (***Tabla 10.*** *Mapa de calor con niveles de severidad del riesgo)* de acuerdo a lo establecido en la ***Tabla 9.*** *Nivel de severidad del riesgo*

A continuación, se hace una tabla de equivalencias entre las zonas del mapa de calor y el nivel de confianza:

| Zonas del mapa de calor | Nivel de Confianza |
|---|---|
| **Aceptable** | Bajo |
| **Moderado** | Medio |
| **Importante** | Alto |

| | |
|---|---|
| **Inaceptable** | Muy Alto |

***Tabla 27.*** *Equivalencia nivel de riesgo inherente frente al nivel de confianza*

Las zonas del mapa de calor son tomadas de la ***Tabla 8.*** *Zonas del mapa de calor.*

Una vez definido el nivel de confianza, se deben considerar los siguientes controles de autenticación y así mismo todos los aplicables de acuerdo con las disposiciones gubernamentales en materia de autenticación digital:

| Nivel de confianza | Descripción del nivel de confianza | Controles mínimos |
|---|---|---|
| **Bajo** | Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo. | a). Las credenciales de usuarios deben estar asociadas al correo electrónico del usuario del usuario.<br>b) Se debe configurar que las contraseñas estén alienadas con lo solicitado en el estándar NIST SP 800-63B de un solo factor OTP. |
| **Medio** | Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado. | a). Las credenciales de usuarios deben estar asociadas al correo electrónico del usuario del usuario.<br>b) Se debe configurar que las contraseñas estén alienadas con lo solicitado en el estándar NIST SP 800-63B de un solo factor OTP.<br>c) Solicitar preguntas y respuestas retro, mecanismo de factor múltiple de autenticación con base en el estándar NIST SP 800-63B de un solo factor OTP. |
| **Alto** | Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo alto. | a) Las credenciales de usuario deben estar asociadas al uso de certificados digitales. |
| **Muy Alto** | Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo extremo. | a) Se deben asociar a los mecanismos de validación que disponga la Registraduría Nacional del Estado Civil las cuales permitan validar la información del ciudadano. |

**Tabla 28.** *Atributos de nivel de confianza*

La Oficina de Seguridad de la Información debe verificar la implementación de los controles de autenticación digital basado en el nivel de confianza definido para cada trámite.

### 3.21. Gestión de riesgos de proveedores y la cadena de suministro

La UAE-DIAN identifica la gestión de riesgos de seguridad de la información como relevante en proveedores y la cadena de suministro de la entidad, dado esto, establece las siguientes medidas para identificar, gestionar y controlar los riesgos que puedan presentarse durante la duración de cualquier contrato:

- **Clausulas para la gestión de riesgos de seguridad de la información:** En las cláusulas descritas en el *Anexo cláusulas del contrato* de la subdirección de compras y contratos, se establecen las medidas que deben ser consideradas y ejecutadas por las partes para la gestión de riesgos de seguridad de la información, una vez sean firmados los contratos con los proveedores de la entidad.
- **Medidas de los supervisores del contrato:** Dentro del documento *CT-ADF-0109 Cartilla de supervisión e interventoría,* se describen las responsabilidades de los supervisores de los contratos de la DIAN en cuanto a la gestión de riesgos de seguridad de la información.
- **Actualización de la matriz de riesgos de proveedores: Dentro** del documento *LP-00-001-2023 Anexo No 3 Matriz de riesgo*, se encuentran definidos los riesgos de seguridad de la información que deben ser identificados, valorados y tratados en el momento en el que se realiza la contratación con un proveedor.

Estas medidas soportan y fortalecen la gestión de riesgos de seguridad de la información de la UAE-DIAN, en caso de presentar alguna situación especial que requiera un análisis diferenciado, se debe poner en conocimiento del líder de riesgos de la Oficina de Seguridad de la Información OSI.

## 4. Monitoreo y revisión

La DIAN a través de la Oficina de Seguridad de la Información – OSI, se encuentra en sincronía con las definiciones para la gestión de riesgos DIAN, y es así como se ajusta a los procedimientos definidos para el seguimiento de las actividades que se encuentran en el documento “PR-PEC-0243 Implementación, monitoreo y mejoramiento de la gestión de riesgos”, sin embargo, a continuación define las siguientes actividades desarrolladas de manera autónoma por la Oficina de Seguridad de la Información - OSI como complemento de dicho documento.

| Actividad | Periodicidad | Objetivo | Responsable | Método de revisión |
|---|---|---|---|---|
| **Realizar seguimiento a los planes de tratamiento de riesgos definidos** | Trimestral | Identificar la ejecución de los planes definidos y los nuevos niveles de riesgo | Director de Gestión/Sub-director/Jefe de Oficina/Director Seccional | Módulo de gestión de riesgos GRC |

| | | | | |
|---|---|---|---|---|
| **Actualizar las matrices de riesgos de las áreas** | Anual | Identificar la aparición de nuevos riesgos o cambios que se puedan presentar en los ya existentes. | Director de Gestión/Sub-director/Jefe de Oficina/Director Seccional | Módulo de gestión de riesgos GRC |
| **Revisar la implementación de los planes de tratamiento de riesgos** | Semestral | Identificar el estado de ejecución de los planes de tratamiento de riesgos establecidos por los líderes de cada área. | Líder de riesgos Oficina de Seguridad de la Información | Módulo de gestión de riesgos GRC |
| **Revisar el diligenciamiento pleno de los riesgos nuevos/adicionales** | semestral | Identificar que los líderes de cada área incluyan toda la información solicitada para el desarrollo metodológico de los riesgos de seguridad de la información y protección de datos. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Módulo de gestión de riesgos GRC |
| **Revisar la efectividad de los controles existentes** | Semestral/por demanda | Identificar el grado de efectividad de un control relacionado con un riesgo especifico; esta actividad se puede programar de manera aleatoria para algunos procesos de la organización o puede ser ejecutada una vez se identifique la materialización de un evento o incidente relacionado con | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Módulo de gestión de riesgos GRC |

| | | | | |
|---|---|---|---|---|
| | | seguridad de la información y protección de datos personales. | | |
| **Entregar la información de la gestión de riesgos para la construcción del plan de gestión de riesgos de seguridad de la información** | Anual | Apoyar el cumplimiento del decreto 612 de 2018 el cual solicita información relacionada con la gestión de riesgos de seguridad de la información. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Excel<br><br>Correo electrónico |
| **Revisar la documentación que soporta la gestión de riesgos de seguridad de la información y protección de datos** | Anual | Verificar que la documentación se mantenga actualizada, conforme a los cambios que se puedan presentar en la entidad o en los procesos para la gestión de riesgos de seguridad de la información y protección de datos personales. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Suite Office 365<br><br>Correo electrónico |
| **Revisar los cambios en las entradas de la gestión de riesgos de seguridad de la información** | Por demanda | Considerar los cambios que se tengan en la información relevante para la gestión de riesgos de seguridad de la información como: Cambios en el contexto interno/externo, partes interesadas externas/internas, cambios en lineamientos de gobierno/marcos de referencia/guías | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Correo electrónico<br><br>DIANNET<br><br>Entrevistas |

| | | | | |
|---|---|---|---|---|
| | | estatales, cambios en el alcance del MSPI – DIAN, | | |
| **Revisar la aplicación de la gestión de riesgos de seguridad de la información y protección de datos en terceros y la cadena de suministro** | Por demanda | Identificar la participación de terceros de la cadena de suministro nuevos, con el objetivo de identificar nuevos riesgos o posibles riesgos que puedan afectar a la entidad de forma similar. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Entrevistas<br><br>Contratos<br><br>Solicitudes de oferta |
| **Revisar la ejecución del plan de gestión de riesgos de seguridad de la información** | Trimestral | Revisar el estado de ejecución del plan de gestión de riesgos de seguridad de la información para identificar desviaciones significativas que requieran medidas o planes de choque para su cumplimiento. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información. | Correo electrónico<br><br>DIANNET<br><br>Entrevistas |
| **Revisar el registro de los incidentes relacionados con la gestión de riesgos de seguridad de la información y protección de datos personales** | Por demanda | Confirmar que se realice el registro de los incidentes de seguridad cada vez que ocurran y que con base a ello se haya realizado lo definido en el numeral *3.19. Actualización de nivel de riesgo derivado incidentes.* | Oficina de Seguridad de la Información - OSI | Correo electrónico<br><br>Módulo de gestión de riesgos GRC |
| **Revisar la aplicación metodológica de riesgos de** | Por demanda | Participar en los proyectos que desarrolla la entidad para que | Líder de riesgos de seguridad de la información/profesional de riesgos de | Correo electrónico |

| | | | | |
|---|---|---|---|---|
| **seguridad de la información en los proyectos de la entidad** | | sean implementadas las medidas definidas para la aplicación de la metodología de riesgos de seguridad de la información y protección de datos. | seguridad de la información | |
| **Incluir los resultados de la gestión de riesgos en las revisiones por la Dirección General** | Anual | Capturar e incluir los resultados de la gestión de riesgos de seguridad de la información en las revisiones realizadas por la Dirección General o quien este designe. Se debe incluir información relacionada con: Recursos, roles y responsabilidades, riesgos vigentes con niveles elevados, amenazas críticas y recurrentes, vulnerabilidades críticas y recurrentes, activos más afectados, estado de la ejecución de los planes de gestión de riesgos u otros que se consideren importantes. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Correo electrónico<br><br>Suite office 365<br><br>Módulo de gestión de riesgos GRC |
| **Atender los requisitos de autoridades o entidades especiales** | Por demanda | Recolectar la información necesaria relacionada con la gestión de riesgos de seguridad de la información cada | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Correo electrónico<br><br>Suite office 365 |

| | | | | |
|---|---|---|---|---|
| | | vez que sea requerida por una entidad especial o autoridad en cumplimiento de la ley. | | Módulo de gestión de riesgos GRC |
| **Revisar las políticas relacionadas con la gestión de riesgos de seguridad de la información y protección de datos** | Anual | Verificar la vigencia de la política de gestión de riesgos de seguridad de la información para identificar si se presentan ajustes o cambios. | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Correo electrónico<br><br>DIANNET<br><br>Módulo de gestión de riesgos GRC |
| **Revisar los cambios en la declaración de aplicabilidad** | Anual | Verificar que cambios han existido en la declaración de aplicabilidad de la entidad y confirmar si se deben realizar ajustes o modificaciones en la gestión de riesgos de seguridad de la información | Líder de riesgos de seguridad de la información/profesional de riesgos de seguridad de la información | Correo electrónico<br><br>DIANNET<br><br>Módulo de gestión de riesgos GRC |

**Tabla 29.** *Monitoreos y seguimientos gestión de riesgos de seguridad de la información*

Todos los seguimientos mencionados deben ser considerados para la presentación de sus resultados ante el Comité Institucional Estratégico para su análisis y propuesta de mejora continua.

### 4.1. Reporte Cuatrimestral

La Oficina de Seguridad de la Información -OSI en sincronía con la gestión de riesgos de la entidad, establece que los dueños de los riesgos de cada dirección, subdirección, jefatura o seccional deben generar un reporte cada 4 (cuatro) meses con la información de los resultados de la gestión de riesgos de seguridad de la información.

El informe debe ser presentado en el documento *FT-PEC-2097 reporte gestión de riesgos* y enviarlo al responsable de la gestión de riesgos de seguridad de la información de la OSI.

El informe debe ser enviado en los primeros 5 días del mes siguiente a la finalización del 4 mes del periodo analizado a través de correo electrónico.

## 4.2. Indicadores de gestión

La Oficina de Seguridad de la Información – OSI identifica como necesario medir la gestión de riesgos de seguridad de la información. Por ello, ha establecido los siguientes indicadores que le permitan identificar las desviaciones frente al cumplimiento de sus objetivos, y así, poder tomar las medidas requeridas de manera eficaz y oportuna:

**a) Indicador de efectividad de las medidas de tratamiento implementadas (EMTI)**

**Objetivo:** identificar el nivel de cumplimiento de los planes de acción definidos para la mitigación de los riesgos, identificados en la gestión de riesgos de seguridad de la información.

$$\boldsymbol{EMTI} = \frac{\sum \begin{matrix} Medidas\ de \\ tratamiento\ ejecutadas \end{matrix}}{\sum \begin{matrix} Total\ de \\ medidas\ de \\ tratamiento \\ definidas \end{matrix}}$$

Los resultados se ubicarán en la siguiente escala para su interpretación:

| Nivel | Descripción |
|---|---|
| **Adecuado** | Si el resultado del indicador es => 70% |
| **En alerta** | Si el resultado del indicador es <=69% y >=20% |
| **Critico** | Si el resultado del indicador es <= 19% |

***Tabla 30.*** *Tabla nivel de indicador EMTI*

**Periodos de medición:** Este indicador se debe medir en periodos *trimestrales*.

**b) Efectividad de la gestión de los riesgos (EGR)**

**Objetivo:** identificar la proporción de riesgos residuales ubicados en zonas *importante* y/o *inaceptables* frente al total de los riesgos residuales en la entidad.

Los resultados se ubicarán en la siguiente escala para su interpretación:

| Nivel | Descripción |
|---|---|
| **Adecuado** | Si el resultado del indicador es =< 30% |
| **En alerta** | Si el resultado del indicador es >=31% y <=40% |
| **Critico** | Si el resultado del indicador es >= 41% |

***Tabla 31.*** *Tabla nivel de indicador EGR*

**Periodos de medición:** Este indicador se debe medir en periodos *anuales*.

**c) Alcance del sistema de gestión riesgos de seguridad de la información (AGRSI)**

**Objetivo:** identificar el nivel de implementación de la gestión de riesgos de seguridad de la información en la entidad.

$$\boldsymbol{AGRSI} = \frac{\sum \textit{Areas con la gestión de riesgos de SI y PDP implementada}}{\sum \textit{Total de áreas DIAN}}$$

Los resultados se ubicarán en la siguiente escala para su interpretación:

| Nivel | Descripción |
|---|---|
| **Adecuado** | Si el resultado del indicador es >= 70% |
| **En alerta** | Si el resultado del indicador es >=31% y <=69% |
| **Critico** | Si el resultado del indicador es <= 30% |

***Tabla 32.*** *Tabla nivel de indicador AGRSI*

**Periodos de medición:** Este indicador se debe medir en periodos *anuales*.

### 4.2.1. Medidas a tomar frente al cumplimiento de los indicadores

Si se evidencia que los resultados de los indicadores se ubican en niveles *En alerta* o *Critico* se deben seguir las medidas que dispone el OD-IIT-001 Modelo de Seguridad y Privacidad de la Información – DIAN, con el fin de tomar medidas que permitan mejorar los resultados de los indicadores.

## 5. Mejoramiento continuo

Con el fin de garantizar la mejora continua de la gestión de riesgos de seguridad de la información, la UAE-DIAN establece puntos de control cada vez que existan hallazgos, falencias, eventos o incidentes de seguridad de la información, con el objetivo de mitigar el impacto de su existencia, tomar acciones para controlarlos y prevenirlos.

Como parte del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN la gestión de riesgos de seguridad de la información y protección de datos, se alinea a sus definiciones y acata los planes de mejoramiento continuo determinados para su mejora; estos pueden identificarse con mayor detalle en el contenido de este modelo.

## 6. Control de cambios

| Versión | Vigencia | | Descripción de cambios | Tipo de información |
|---|---|---|---|---|
| | Desde | Hasta | | |
| 1 | 09/02/2023 | 06/12/2023 | Versión inicial, elaborada con base en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5 – DAFP-2020” del Departamento Administrativo de la Función Pública y el “Anexo 4-Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas” de MINTIC | Esta versión corresponde a información pública reservada |
| 2 | 07/12/2023 | | Se modifica la estructura del documento para incluir elementos importantes para la gestión metodológica como: | Esta versión corresponde |

| | | | | |
|---|---|---|---|---|
| | | | • Consideración de los riesgos de protección de datos personales en la gestión de riesgos de seguridad de la información.<br>• Análisis del contexto interno/externo<br>• Análisis de las partes interesadas, sus necesidades y expectativas.<br>• Inclusión del alcance para la gestión de riesgos de seguridad de la información.<br>• Alineación con la política de gestión de riesgos de seguridad de la información.<br>• Identificación de roles y responsabilidades.<br>• Identificación de los recursos requeridos para la gestión metodológica.<br>• Análisis de los objetivos de la entidad y los objetivos de los procesos.<br>• Cambio en la agrupación de los activos de información.<br>• Inclusión de los tipos de amenazas relacionadas con datos personales y ciberseguridad.<br>• Ajustes en las fórmulas para las mediciones de la probabilidad y el impacto de los riesgos.<br>• Ajustes en las escalas para la medición del nivel de riesgo.<br>• Inclusión de los criterios para la priorización de los riesgos.<br>• Inclusión de las fórmulas para el cálculo de la medición conjunta de controles.<br>• Inclusión de los seguimientos que debe realizar la gestión de riesgos de seguridad de la información.<br>• Alineación de los indicadores y el mejoramiento continúo dispuesto por el MSPI.<br>• Inclusión de los indicadores de gestión para la medición de la gestión de riesgos de seguridad de la información. | a Información Pública |

| | | | | |
|---|---|---|---|---|
| | | | Adicional se realizaron ajustes generales tomados de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5 – DAFP-2020" e incluir elementos faltantes que se encuentran en el Anexo 4 – "Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas - MNGRSI" de MINTIC | |

***Tabla 33.*** *Tabla de control de cambios*

| | | | |
|---|---|---|---|
| **Elaboró**: | Consultor Externo EY<br>**Elaboración técnica** | Consultor | Oficina de Seguridad de la Información |
| | Tito Alejandro Menjura Murcia<br>**Elaboración metodológica** | Gestor II | Coordinación de Procesos y Riesgos Operacionales |
| | Alfredo Ahumada Ahumada<br>**Elaboración metodológica** | Gestor II | Coordinación de Procesos y Riesgos Operacionales |
| **Revisó**: | Carlos Javier Ibañez Serna | Gestor II | Oficina de Seguridad de la Información |
| **Aprobó**: | Hugo Alcides Pérez Pinilla | Jefe de Oficina (E) | Oficina de Seguridad de la Información |

## 7. Anexos

Anexo 1. Instrumentos de consulta para la gestión de riesgos de seguridad de la información

Anexo 2. Matriz de riesgos de seguridad de la información para proyectos