Resolución Directoral

N° 006-2022-VIVIENDA/OGEI

Lima, 12 de setiembre del 2022

VISTO:

El Informe Nº 066-2022-VIVIENDA/OGEI-GFN del Especialista en Seguridad de la Información;

CONSIDERANDO:

Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, mediante Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial N° 166-2017-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición” en todas las entidades integrantes del Sistema Nacional de Informática, en concordancia con la recomendación efectuada, a través del Memorando N° 152-2015-PCM/ONGEI, por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros;

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el artículo N° 105 del Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N° 029-2021-PCM, establece como parte de las obligaciones de las entidades públicas en seguridad digital, que implementen y mantengan un sistema de Gestión de Seguridad de la Información. Asimismo, el artículo N° 109 del mismo cuerpo

normativo dispone, entre otros, que el diseño, implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) atiende a las necesidades de todas las partes interesadas de la entidad y responde a los objetivos estratégicos, estructura, tamaño, procesos y servicios de la entidad;

Que, el artículo 55 del Reglamento de Organización y Funciones - ROF del Ministerio de Vivienda, Construcción y Saneamiento MVCS, establece que la Oficina General de Estadística e Informática - OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como planificar, desarrollar, implementar y gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, con Resolución Ministerial Nº 356-2018-VIVIENDA, del 23 de octubre de 2018 se constituyó el Comité de Gobierno Digital en el marco de la Resolución Ministerial N° 119-2018-PCM, entre cuyas funciones destaca la de liderar y dirigir el proceso de transformación digital en la entidad;

Que, estando a lo expuesto y conforme a la propuesta remitida por el Especialista en Seguridad de la Información, corresponde expedir la presente Resolución aprobando la Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS, según lo expresado en el documento de visto;

De conformidad con lo dispuesto en la Ley N°29518, Ley Orgánica del Poder Ejecutivo, Ley N° 30156, Ley de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N° 010-2014-VIVIENDA, modificado por Decreto Supremo N° 006-2016-VIVIENDA, la Resolución Ministerial N° 004-2016-PCM que aprueba la Norma Técnica Peruana “NTP ISO/IEC 27001:2014;

SE RESUELVE:

Artículo 1.- Aprobar la Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS, el mismo que forma parte integrante de la presente Resolución.

N°	Documento	Código	Versión
1	Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS	DGSI-07	1.0

Resolución Directoral

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento.

Regístrese y comuníquese.

FIRMA DIGITAL

VIVIENDA

Firmado digitalmente por: ESCAJADILLO CHIMAYCO Walter Fidel FAU 20504743307 hard
Motivo: Soy el autor del documento
Fecha: 2022/09/13 07:49:40-0500

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

INFORME Nº 066-2022-VIVIENDA/OGEI-GFN

A : **ING. WALTER ESCAJADILLO CHIMAYCO**
Director General de la Oficina General de Estadística e Informática

ASUNTO : Metodología de Gestión de Riesgos de Seguridad de la Información en Ministerio de Vivienda, Construcción y Saneamiento.

FECHA : San Isidro, 12 de septiembre de 2022

Tengo el agrado de saludarlo y a través del presente me dirijo a usted, para informar respecto a la Metodología de Gestión de Riesgos de Seguridad de la Información en el Ministerio de Vivienda, Construcción y Saneamiento (MVCS).

1. Antecedentes

1.1 Con informe N° 005-2022-VIVIENDA/OGEI-GFN, concluye que es de necesidad urgente, la contratación del servicio mencionado en el presente informe técnico para garantizar que se cumpla con lo establecido en el Memorando Múltiple N° 097-2021/VIVIENDA-SG logrando efectuar las recomendaciones emitidas y que los servicios que brinda el Ministerio de Vivienda, Construcción y Saneamiento sean realizados de manera segura.

La contratación de este servicio permitirá generar información documentada que permita sustentar la adecuada gestión y diligencia de la organización para la Metodología de Gestión de Riesgos de Seguridad de la Información en el Ministerio de Vivienda, Construcción y Saneamiento.

1.2 Con informe N° 041-2022-VIVIENDA/OGEI-GFN, se evidencia que el proveedor del servicio de gestión de riesgos, ha cumplido con la entrega del tercer entregable de acuerdo a los Términos de Referencia.

2. Análisis

2.1 La metodología en el servicio utilizada en el análisis de gestión de riesgos, fue elaborada, presentada y aprobada por la Oficina General de Estadística e Informática, dicha metodología específica 6 etapas que componen el proceso de gestión de riesgos:

- Inventario de activos de información
- Identificación de riesgos de seguridad de la información
- Análisis de riesgos de seguridad de la información
- Evaluación de riesgos de seguridad de la información
- Tratamiento de riesgos de seguridad de la información
- Estimación del riesgo residual

3. Conclusión

3.1 El Ministerio de Vivienda, Construcción y Saneamiento, no cuenta con Metodología de Gestión de Riesgos de Seguridad de la Información.

3.2 Al respecto, y en base a lo expuesto en el análisis del presente informe, el suscrito alcanza la Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS.

4. Recomendación

Por lo antes expuesto, el suscrito recomienda:

4.1 Se recomienda aprobar la Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS para que sea usado en las áreas o procesos analizado que forma parte del alcance del Sistema de Gestión de Seguridad de la Información.

4.2 Se adjunta la Metodología de Gestión de Riesgos de Seguridad de la Información en el MVCS con sus anexos y el proyecto de Resolución Directoral.

Es todo cuanto cumplo con informar para los fines pertinentes.

Sin otro particular,

FIRMA DIGITAL
VIVIENDA
Firmado digitalmente por: FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft
Motivo: Soy el autor del documento
Fecha: 2022/09/12 16:45:02-0500

Ing. Guillermo Fernández Namuche
Especialista en Seguridad de la Información

PERÚ | Ministerio de Vivienda, Construcción y Saneamiento

METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Oficina General de Estadística e Informática

HOJA DE CONTROL DE DOCUMENTO

DOCUMENTO / ARCHIVO

Título	Metodología de Gestión de Riesgos de Seguridad de la Información
Fecha	12/09/2022
Versión	1.0
Localización	Ministerio de Vivienda, Construcción y Saneamiento (MVCS)

REGISTRO DE CAMBIOS

Versión	Páginas	Fecha Modificación	Motivo del cambio
1.0	27	12/09/2022	Elaboración inicial del documento

CONTROL DEL DOCUMENTO

ROL	NOMBRE	CARGO	VISTO
Elaborado por:	Guillermo Fernández Namuche	Especialista en Seguridad de la Información (OSI)	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2022/09/12 16:08:19-0500
Aprobado por:	Walter Fidel Escajadillo Chimayco	Director General de la Oficina General de Estadística e Informática (OGEI)	FIRMA DIGITAL VIVIENDA Firmado digitalmente por ESCAJADILLO CHIMAYCO Walter Fidel FAU 20504743307 hard Motivo: Soy el autor del documento Fecha: 12.09.2022 16:37:40 -05:00

Contenido

1. OBJETIVOS DE LA METODOLOGIA 4
2. ALCANCE 4
3. BASE LEGAL 4
4. DEFINICIONES Y ABREVIATURAS 5
5. PROCESO METODOLÓGICO 7
5.1. Gestión de riesgos de seguridad de la información 7
5.1.1. Identificación de activos de información 7
5.1.2. Identificación de riesgos de seguridad de la información 10
5.1.3. Análisis de riesgos de seguridad de la información 13
5.1.4. Evaluación de riesgos de seguridad de la información 17
5.1.5. Tratamiento de riesgos de seguridad de la información 18
5.1.6. Estimación del riesgo residual 20
5.2. GESTIÓN DE RIESGOS Y OPORTUNIDADES DEL SGSI 20
5.2.1. Riesgos de SGSI 20
5.2.2. Oportunidades del SGSI 22
6. FORMATOS 27
7. ANEXOS 27

1. OBJETIVOS DE LA METODOLOGIA

Establecer los lineamientos para la gestión única y estándar de los riesgos y oportunidades de seguridad de la información del Ministerio de Vivienda, Construcción y Saneamiento (MVCS).

2. ALCANCE

Las disposiciones contenidas en este procedimiento son de aplicación y obligatorio cumplimiento para los cambios en el área o proceso analizado que forma parte del alcance del Sistema de Gestión de Seguridad de la Información.

3. BASE LEGAL

La definición de la presente Metodología se encuentra alineado a las directivas y normas, que se soportan en las siguientes normas:

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y su modificatoria.
- Resolución N° 129-2014/CNB-INDECOPI que aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición".
- Resolución Ministerial N° 004-2016-PCM, Resolución Ministerial que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática y sus modificatorias.
- Resolución Ministerial N° 087-2019-PCM, Resolución Ministerial que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Decreto Supremo N° 157-2021-PCM aprobó el Reglamento del Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital como un Sistema Funcional del Poder Ejecutivo, tiene la finalidad de fomentar e impulsar la transformación digital de las entidades públicas, las empresas privadas y la sociedad en su conjunto, fortalecer el uso efectivo de las tecnologías digitales, las redes y los servicios digitales por parte de los ciudadanos y personas en general.
- Resolución Ministerial N° 374-2017-VIVIENDA, que aprueba la Política de seguridad de la Información del Ministerio de Vivienda, Construcción y Saneamiento.
- Resolución Ministerial N° 248-2018-VIVIENDA, que aprueba el Mapa de Procesos y el Manual de Gestión de Procesos y Procedimientos del Ministerio de Vivienda, Construcción y Saneamiento.
- Resolución Ministerial N° 356-2018-VIVIENDA, que aprueba la conformación del Comité de Gobierno Digital en el Ministerio de Vivienda, Construcción y Saneamiento y su modificatoria.
- Decreto Legislativo N° 1412, Ley de Gobierno Digital
- Decreto Supremo Nº 029-2021-PCM que aprueba el Reglamento de la Ley de Gobierno Digital, publicada en febrero de 2021 por Decreto Legislativo N° 1412.
- NTP ISO/IEC 27000:2018 "Tecnología de la Información. técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Visión general y vocabulario".
- NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición.

- NTP ISO/IEC 27002:2017 “Tecnología de la Información. técnicas de seguridad. Código de prácticas para los controles de seguridad de la información”.

- NTP ISO/IEC 27003:2013 “Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información”.

- NTP-ISO 31000:2018 Gestión del Riesgo. Directrices. 2ª Edición, aprobada por Resolución Directoral N° 014-2018-INACAL-DN.

- NTP ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. 2ª Edición.

4. DEFINICIONES Y ABREVIATURAS

- **Activo de información:** Información imprescindible para las organizaciones que se debe proteger frente a riesgos y amenazas. Como, por ejemplo: Servicios y personal, datos/información, equipo informático (hardware), aplicaciones 8software), etc.

- **Aceptación del riesgo:** Decisión informada para tomar un riesgo en particular.
  - Nota 1: La aceptación del riesgo puede ocurrir sin el tratamiento del riesgo o durante el proceso de tratamiento de riesgos.
  - Nota 2: Riesgos aceptados están sujetas a supervisión y revisión.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

- **Análisis de riesgo:** Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.
  - Nota 1: El análisis de riesgos proporciona las bases para la evaluación del riesgo y para tomar las decisiones sobre el tratamiento del riesgo.
  - Nota 2: El análisis de riesgo incluye la estimación del riesgo.

- **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados.

- **Control:** Medida que modifica un riesgo.
  - Nota 1: Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.
  - Nota 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

- **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

- **Evaluación de riesgo:** Proceso de la comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo o su magnitud es aceptable o tolerable.
  - Nota 1: La evaluación de riesgos ayuda a la decisión sobre el tratamiento del riesgo.

- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo que afecten la confidencialidad, integridad y disponibilidad de la información.

- **Identificación del riesgo:** Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.
  - Nota 1: La identificación de riesgos consiste en la identificación de las fuentes de riesgos, eventos/sucesos, sus causas y sus consecuencias potenciales.
  - Nota 2: La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas y de expertos; así como necesidades de las partes interesadas.

- **Integridad:** Propiedad salvaguardar la exactitud y completitud de los activos.

- **Nivel de riesgo:** Magnitud de un riesgo, expresados en términos de la combinación de las consecuencias y de su probabilidad.

- **Probabilidad:** Posibilidad de que algún hecho se produzca.

- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas en salidas.

- **Proceso de gestión de riesgos:** Aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación, consulta, establecidos el contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgo.
  - Nota 1: ISO/IEC 27005 utiliza el término "proceso" para describir la gestión del riesgo global. Los elementos dentro del proceso de gestión de riesgos se denominan "actividades"

- **Propietario del riesgo:** Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.

- **Riesgo:** Efecto de la incertidumbre sobre la consecución de los objetivos.
  - Nota 1: Un efecto es una desviación de lo esperado, positivo o negativo.
  - Nota 2: La incertidumbre es el estado, aunque sea parcial, de la carencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia, o la posibilidad.
  - Nota 3: El riesgo se caracteriza a menudo por referencia a los eventos potenciales y consecuencia, o una combinación de estos.
  - Nota 4: El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad asociada de ocurrencia.
  - Nota 5: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden ser expresados como efecto de la incertidumbre en los objetivos de seguridad de la información.
  - Nota 6: El riesgo para la seguridad de la información se asocia con la posibilidad de que las amenazas explotarán vulnerabilidades de un activo de información o un grupo de activos de información y por lo tanto causan daño a la organización.

- **Riesgo residual:** Riesgo que queda después del tratamiento del riesgo.
  - Nota 1: Riesgo residual puede contener riesgos no identificados.
  - Nota 2: Riesgo residual también puede ser conocido como "riesgo retenido"

- **Sistema de información:** Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo dela información.

- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
  - Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiablidad también pueden estar involucrados.

- **Tratamiento del riesgo:** Proceso para modificar el riesgo.
  - Nota 1: El tratamiento del riesgo puede implicar:
    - ✓ Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
    - ✓ Tomar el aumento del riesgo con el fin de perseguir una oportunidad;
    - ✓ Eliminar la fuente de riesgo;
    - ✓ El cambio de la probabilidad;
    - ✓ El cambio de las consecuencias;
    - ✓ Compartir el riesgo con la otra parte o partes (incluyendo los contratos y la financiación del riesgo);

- ✓ Retener el riesgo por elección informada.

- Nota 2: Tratamientos de riesgos que tienen que ver con las consecuencias negativas se refieren a veces como “riesgos mitigación”, “eliminación de riesgos”, “prevención de riesgos” y “reducción del riesgo”.
- Nota 3: El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

- **Vulnerabilidad:** Debilidad de un activo o de un control que puede ser explotado por una o más amenazas.

- **Abreviaturas:**
  - CID: Confidencialidad, integridad y disponibilidad
  - OSI: Oficial de Seguridad de la Información
  - SGSI: Sistema de Gestión de Seguridad de la Información

5. PROCESO METODOLÓGICO

El proceso de gestión de riesgos y oportunidades de seguridad de la información se realiza una vez al año como mínimo y cada vez que un evento produzca cambios en el área o proceso analizado que forma parte del alcance del SGSI.

Asimismo, en cada revisión por la Dirección y cuando sea necesario en sesión del Comité de Gobierno Digital, se informa el resultado del análisis de evaluación y tratamiento de los riesgos y oportunidades, así como el estado de las acciones consideradas en el plan de tratamiento.

5.1. Gestión de riesgos de seguridad de la información

Para que este proceso sea efectivo, requiere la participación de los propietarios de información y/o custodios de información de distintas direcciones o áreas de responsabilidad dentro de la institución que tengan relación con el proceso a analizar, de esta forma se logra la identificación de amenazas, vulnerabilidades, impactos y probabilidades de ocurrencias en un corto tiempo.

El proceso de gestión de riesgos se compone de 4 etapas:

- Inventario de activos de información
- Análisis de riesgos de seguridad de la información
- Evaluación de riesgos de seguridad de la información y
- Tratamiento de riesgos de seguridad de la información

y se registran en los formatos SGSI.FR.01: Inventario de activos de información y SGSI.FR.02: Matriz de riesgos de seguridad de la información y plan de tratamiento, según corresponda.

5.1.1. Identificación de activos de información

Para la identificación y valoración de los activos de información se realizan entrevistas con personal clave de cada proceso definido en el alcance del SGSI y se completa el formato SGSI.FR.01: Inventario de activos de información que contiene los siguientes atributos:

- **Fecha de inicio:** indica la fecha de inicio de ejecución del inventario de activos de información.
- **Proceso:** indica el nombre del proceso relacionado al activo de información.
- **Subproceso:** indica el nombre del subproceso relacionado al activo de información.
- **Código:** identificador o nomenclatura del activo de información, indica la asignación de un código según la siguiente estructura:

AI.año.númerocorrelativo

i. AI: mnemónico relativo a “activo de información”.

ii. Año: se refiere al año de identificación del activo.
iii. Número correlativo: número correlativo comenzando en el 1.

- **Nombre:** indica el nombre del activo de información identificado.
- **Descripción:** indica una breve descripción del activo de información identificado.
- **Categoría y tipo:** indica la categoría y tipo de activo.

Tabla 1: Clasificación de activos de información

Categoría	Tipo
Primario	Proceso y actividades del negocio
	Información física
	Información digital
Soporte	Hardware
	Software
	Personal
	Contenedor
	Sitio
	Servicio

- **Ubicación física o lógica del activo:** indica la ubicación especifica del activo de información. En el caso de ubicación física, detallar el sitio donde se encuentra y en el caso de la ubicación lógica, detallar el nombre del archivo o del servidor donde se encuentra alojado.
- **Propietario:** indica el nombre de la persona y/o área que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Custodio:** indica el nombre de la persona y/o área que tiene responsabilidad de cuidar o guardar un activo de información.
- **Requerimiento:** indica si la existencia de un activo se debe al cumplimiento de requisitos legales, regulatorios o contractuales.
- **Clasificación según el tipo de uso:** indica el tipo de clasificación según el grado de confidencialidad guardando relación con la tabla 2.

Tabla 2: clasificación según el tipo de uso

Clasificación	Detalle
Confidencial	Activos de información que pertenecen a un proceso o dirección y que por su naturaleza son **reservados exclusivamente al personal del área o proceso especifico**, incluye también aquellos activos de información que incluyen datos sensibles.
Uso interno	Activos de información que son **accedidos exclusivamente por personal interno de la institución.**
Público	Activos de información que no son clasificados como confidenciales o de uso interno que presumen públicos.

- **Clasificación CID:**

  - **Confidencialidad (C):** indica el grado de confidencialidad requerido por el activo de información. (ver tabla 3)
  - **Integridad (I):** indica el grado de integridad requerido por el activo de información. (ver tabla 3)
  - **Disponibilidad (D):** indica el grado de disponibilidad requerido por el activo de información. (ver tabla 3)

Tabla 3: Niveles de valorización de los activos según CID

Nivel / Valor	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)
Bajo (1)	La información asociada al activo es de uso general y cualquiera puede acceder a ella, pues no impacta a la organización	El activo puede tolerar una alteración alta de sus componentes, ya que la alteración de integridad afectaría una actividad menor del proceso.	El activo no puede estar indisponible por más de una semana, su carencia afectaría una actividad menor del proceso
Medio (2)	La información asociada al activo es interna y solo personal de algunas áreas internas pueden acceder a ella, su divulgación afectaría los procesos de las áreas involucradas.	El activo no puede tolerar más que una alteración media de sus componentes, ya que la alteración de su integridad afectaría una o más actividades del proceso.	El activo no puede estar indisponible por más de dos días, su carencia afectaría una o más actividades del proceso
Alto (3)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, divulgación comprometería la reputación e imagen de la organización.	El activo no puede tolerar más que una alteración baja de sus componentes, ya que la alteración de su integridad afectaría una o más actividades importantes del proceso.	El activo no puede estar indisponible por más de cinco horas, su carencia afectarla en la operación del proceso.
Extremo (4)	La información asociada al activo confidencial solo es accedida por Directores, su divulgación sería catastrófica para la organización.	El activo no puede tolerar pérdida o alteración de sus componentes, ya que la alteración de su integridad comprometería varios procesos de la organización.	El activo siempre debe estar disponible, pues su carencia afectaría el flujo de producción de varios procesos de la organización.

- **Valor del activo:** indica el promedio de los valores de calificación respecto a la confidencialidad, integridad y disponibilidad utilizando la siguiente formula:

$$Valor\ del\ Activo = \frac{Confidencialidad + Integridad + Disponibilidad}{3}$$

- **Tasación del activo:** indica el rango de tasación de los activos de información según el valor de activo (ver tabla 4).

Tabla 4: tasación de los activos

Tasación	Rango
Extremo	3.50 – 4.00
Alto	2.50 – 3.49
Medio	1.50 – 2.49
Bajo	1.01 – 1.49

5.1.2. Identificación de riesgos de seguridad de la información

Una vez completo el inventario de activos de información se selecciona solo los activos de información cuyo rango de tasación es “Extremo” y “Alto”.

Para continuar con la etapa de análisis de riesgos, se identifica amenazas y vulnerabilidades y se registran en la matriz SGSI.FR.02: Matriz de riesgos de seguridad de la información y plan de tratamiento considerando los siguientes atributos:

- **Vulnerabilidad:** Indica la vulnerabilidad a la que se encuentra expuesto el activo ed información (ver tabla 5). Estas vulnerabilidades pueden estar orientadas al lado cibernetico y se puede utilizar otros tipos de input como informes de Ethical Hacking, reportes de herramientas automatizadas de escaneo de vulnerabilidades, informes de revisión de código, evaluaciones de otras metodologías como NIST-CSF, entre otros.

Tabla 5: Guía de vulnerabilidades de seguridad de la información

Categoría	Vulnerabilidad
Archivos	Información sin digitalizar
	Ubicación fisica sin medidas de seguridad
	Información sin etiquetado
	Posibilidad de accesos no autirizados
	No cuenta con encriptación o cifrado
	Falta de copias de respaldo
Hardware	Mantenimiento insuficiente
	Susceptibilidad a la humedad, al polvo y a la suciedad
	Almacenamiento no protegido
	Falta de cuidado al descartarlo
	Equipo obsoleto
	Debilidad de configuración
	No existe control de bloqueo automatico de los equipos desatendidos
	Equipos sin procesos de gestión de capacidad
	No cuenta con equipo de contingencia
Software	Pruebas al software inexistentes o insuficientes
	Falta de pruebas de culnerabilidades
	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente
	Falta de control de accesos
	Interfaz de usuario complicada
	Falta de documentación
	Errorres de configuración
	Fechas incorrectas
	Tablas de claves no protegidas
	Habilitación de servicios innecesarios
	Software inmaduro o nuevo
	Falta de control de cambios eficaz
	Falta de copias de respaldo
	Faltas de logs de auditoria en los historiales del administrador y del operador
	Software desfasado por vigencia tecnologica y sis soporte por parte del fabricante
	Falta de licenciamiento
	Falta de procesos de actualziaciones
	Uso inadeecuado o negligente del control de acceso fisico a edificios y ambientes

Patrimonial	Ubicación fisica de ambientes de almacenamiento o procesamiento de datos en areas susceptibles de desastres naturales o inundaciones
	Red inestable de energía eléctrica
	Falta de procedimeintos de monitoreo de instalaciones de procesamiento de la información
	Ambiente fisico reducido y/o saturado (espacio inadecuado)
	Existencia de material inflamable (cajas, papel, etc.)
Personal	Ausencia del personal
	Procedimientos inadecuados del reclutamiento
	Capacitación de seguridad insuficiente
	Uso incorrecto del software y hardware
	Falta de conciencia de seguridad
	Falta de mecanismos de monitoreo
	Trabajo no supervisado
	Falta de un proceso disciplinario formal
	Rotación excesiva o no planificada de personal
Servicios	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros
	Respuesta inadecuada del proveedor del servicio o fabricante
	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio
	Incumplimiento de acuerdo sobre el nivel de servicio
Otros	Falta de procedimieintos
	Falta de politicas
	Falta de un proceso de gestión de incidencias de seguridad de la información
	Falta de acuerdos de confidencialidad
	Ausencia de segregación de funciones
	Falta de mapa de procesos
	Falta de documentación formal del proceso
	Falta de auditorias regulares (supervisión)
	Falta de planes de continuidad (Plan de recuperación de desastres y plan de contingencias)
	Falta de asignación apropiada de responsabilidades de seguridad en la información

- **Amenazas:** Indica la amenaza a la que se encuentra expuesto el activo de información (ver tabla 6). Estas amenazas pueden estar orientadas al lado cibernetico y se puede utilizar otros tipos de *input* como fuentes de amenazas externas, evaluaciones de otras metodologías como NIST-CSF, grupos de interés, foros especializados, entre otros.

Tabla 6. Guía de amenazas

Tipo	Descripción	Amenazas
Daño fisico	Se puede generar por un accidente dentro de la institución, o por un accidente en los centros de trabajo contiguos al nuestro.	Fuego
		Daño por agua
		Contaminación
		Accidente importante
		Destrucción del equipo o los medios
		Polvo, corrosión, congelamiento
		Roturas o averías
Eventos naturales	Dependiendo la localización de las sedes que albergan los activos de	Fenomenos climaticos
		Fenomenos sismicos
		Fenomenos volcanicos

	información, estos pueden estar expuestos eventos naturales.	Fenomenos metereologicos
		Inundación
Perdida de los servicios esenciales	La perdida de los servicios esenciales puede suponer la caída de las operaciones de la institución.	Falla en el sistema de suministro de agua o de aire acondicionado
		Perdida de suministro de energía
		Falla en el equipo de telecomunicaciones
Fallas técnicas	Pueden presentarse fallas en un momento determinado, por ataques externos o la información que gestionan suele mostrar un crecimeinto en muchos casos exponencial, que puede llevarlos al colapso.	Falla del equipo Saturación del sistema de información Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información Agotamiento de los recursos informáticos Fallo de la climatización
Acciones no autorizadas	El uso no previsto de determinada información, pueden suponer una amenaza grave.	Acceso no autorizado
		Uso no autorizado del equipo
		Copia fraudulenta del software
		Uso de software falso o copiado
		Corrupción de los datos
		Procesamiento ilegal de los datos
Compromiso de las funciones	Amenazas graves relacionadas con los roles y funciones estandarizados en la institución.	Error en el uso
		Error del usuario
		Abuso de derechos
		Falsificación de derechos
		Negación de acciones
		Incumplimiento en la disponibilidad del personal
		Rotación personal
Compromiso de la información	Puede provocar graves consecuencias en la información de la institución a nivel de perdida, modificación o robo.	Interceptación de señales de interferencia comprometedoras
		Robo de medios o documentos
		Robo de equipo
		Recuperación de medios reciclados o desenchados
		Datos provenientes de fuertes no confiables
		Manipulación con hardware
		Intercepción de señales de interferencia comprometedoras
Humanas	Amenazas relacionadas a las acciones humanas provocada intencionalmente.	Piratas informático
		Persona malintecionada
		Codigo malintencionado (por ejemplo, virus, malware, caballo troyano)
		Espionaje insdustrial
		Ingenieria social
		Suplantación de identidad
		Denegación de servicios (Ataques DoS)
		Sabotaje del sistema
		Errores (bugs) en el sistema

		Extorsión
		Soborno

- **Código del riesgo:** indica la asignación de un código al riesgo según la siguinete estructura:

  RI.año.númerocorrelativo

  i. RI: mnemónico relativo a “riesgo de información”.
  ii. Año: relacionado al ítem a. Año.
  iii. Número correlativo: número correlativo comenzando en el 1.

- **Riesgo:** indica el detalle del riesgo identificado que puede afectar a uno o varios activos de información y que sirva para identificarlo respecto de otros.

- **Propietario del riesgo:** indica el nombre de una persona, una institución u otra paret interesada con la responsabilidad y autoridad para administrar el riesgo.

5.1.3. Análisis de riesgos de seguridad de la información

5.1.3.1 Riesgos inherente

- Aspecto de seguridad afectados: indica si el riesgo afecta la confidencialidad, integridad y disponibilidad del activo de información (ver tabla 7).

Tabla 7: Aspecto de seguridad afectado por el riesgo

Calificación	Confidecnialidad (C)	Integridad (I)	Disponibilidad (D)
Baja (1)	Cuando la pérdida o falla de un determinado activo afecta la divulgación o revelamiento no autorizado de la información, **no impactando** la operatividad, competividad, el cumplimiento legal, rentabilidad o imagen de la institución.	Cuando la perdida o falla de un determinado activo afecta la exactitud y completitud de la información, **no impactando** la operatividad, competitividad, el cumplimeinto legal, rentabilidad o imagen de la institución.	Cuando la pérdida o falla de un determinado activo afecta la accesibilidad y disposición de la información, **no impactando** la operatividad, competitividad, el cumplimeinto legal, rentabilidad o imgen d ela institución.
Media (2)	Cuando la perdida o falla de un determinado activo afecta la divulgación o revelamiento no autorizado de la información, **impactando parcialmente** la operatividad, competitividad, el cumplimieinto legal,	Cuando la pérdida o falla de un determinado activo afecta la exactitud y completitud de la información, **impactando parcialmente** la operatividad, competitividad, el cumplimiento legal,	Cuando la perdida o falla de un determinado activo afecta la accesibilidad y disposición de la información, **impactando parcialmente** la operatividad, competitividad, el cumplimiento legal,

	rentabilidad o imagen de la istitución.	rentabilidad o imagen de la institución.	rentabilidad o imagen de la isntitución.
Alta (3)	Cuando la pérdida o falla de un determinado activo afecta la divulgación o revelamiento no autorizado de la información, **impactando gravemente** la operatividad, competitividad, el cumplimiento legal, rentabilidad o imagen de la institución.	Cuando la perdida o falla de un determinado activo afecta la exactitud y completitud de la información, **impactando gravemente** la operatividad, competitividad, el cumplimiento legal, rentabilidad o imagen de la isntitución.	Cuando la perdida o falla de un determinado activo afecta la accesibilidad y disposición de la información, **impactando gravemente** la operatividad, competitividad, el cumplimiento legal, rentabilidad o imagen de la institución.

- **Valor y nivel del impacto:** considerando a qué aspecto de seguridad afecta al riesgo (ver tabla 7) indica el nivel del imapcto del riesgo (ver tabla 8).

Tabla 8: Escala del nivel del impacto según el aspecto de seguridad (CID) afectado

Aspecto de seguridad afectado por el riesgo			Nivel del impacto
C	I	D	
1	1	1	Insignificante
1	1	2	Menor
1	1	3	Mayor
1	2	1	Menor
1	2	2	Moderado
1	2	3	Mayor
1	3	1	Mayor
1	3	2	Mayor
1	3	3	Muy significativo
2	1	1	Menor
2	1	2	Moderado
2	1	3	Mayor
2	2	1	Moderado
2	2	2	Moderado
2	2	3	Mayor
2	3	1	Mayor
2	3	2	Mayor
2	3	3	Muy significativo
3	1	1	Mayor
3	1	2	Mayor
3	1	3	Muy significativo
3	2	1	Mayor
3	2	2	Mayor
3	2	3	Muy significativo
3	3	1	Muy significativo
3	3	2	Muy significativo
3	3	3	Muy significativo

- *Insignificante* es cuando en el (aspecto de seguridad afectado por el riesgo) CID los valores son todos 1.
- *Menor* es cuando en el (aspecto de seguridad afectado por el riesgo) CID al menos tiene un valor 2.
- *Moderado* es cuando en el (aspecto de seguridad afectado por el riesgo) CID tiene dos valores 2.
- *Mayor* es cuando en el (aspecto de seguridad afectado por el riesgo) CID al menos tiene un valor 3.
- *Muy significativo* es cuando en el (aspecto de seguridad afectado por el riesgo) CID tiene dos o tres valores 3.

Tabla 9: Escala del impacto del riesgo

ESCALA DE IMPACTO		
Valor	**Nivel**	**Descripción**
1	Insignificante	No afectaría actividades ni procesos de la institución o terceros.
2	Menor	Afectaría una actividad o proceso no críticos de la institución o terceros.
3	Moderado	Podría ocasionar un perjuicio en una o más de una actividad o proceso crítico de la institución o terceros.
4	Mayor	Podría ocasionar un perjuicio significativo para la institución o terceros y que podría impedir la ejecución de las actividades de la institución.
5	Muy significativo	Podría ocasionar un perjuicio muy significativo para la institución o terceros y que podría impedir la ejecución de las actividades, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones.

- **Valor y nivel de la robabilidad de ocurrencia**: indica la probabilidad de ocurrencia de la explotación de la vulnerabilidad por la amenza considerando los controles actuales (ver tabla 10).

Tabla 10: Escala de la probabilidad de ocurrencia del riesgo

ESCALA DE PROBABILIDAD			
Valor	**Nivel**	**Descripción**	
1	**Raro**	Puede ocurrir en circunstancias excepcionales.	No se ha presentado en el último año.
2	**Improbable**	No esperado, pero podría ocurrir algunas veces.	Se ha presentado al menos una vez en el trimestre.
3	**Posible**	Es posible que ocurra el evento con una frecuencia media.	Se ha presentado al menos una vez en el trimestre.
4	**Probable**	Existen antecedentes de que el evento ocurrirá dentro de un plazo de tiempo.	Se ha presentado una o más de una vez al mes.
5	**Casi seguro**	Se sabe que ocurre con cierto grado de certeza y	Se ha presentado una o más de una vez a la semana.

		que la frecuencia es muy alta o casi cierta.	

- **Valor del riesgo inherente:** se estima el valor del riesgo como la multiplicación de los valores de calificación respecto a la probabilidad e impacto siguiendo la siguiente formula:

$$Valor\ del\ riesgo\ inherente = Probabilidad \times Impacto$$

- **Nivel del riesgo inherente:** indica el nivel del riesgo según el valor de riesgo identificado previamente (ver tabla 9).

Tabla 11: Escala del riesgo de seguridad de la información

Valor	Nivel
1 – 2	Muy bajo
3 – 4	Bajo
5 – 10	Medio
12 – 16	Alto
20 - 25	Muy alto

La dupla impacto-Probabilidad de un riesgo se grafican en una tabla de doble entrada y de esta forma se obtiene graficamente los riesgos de seguridad de la información que tienen más probabilidad de ocurrencia y que causan más daño al cumplimiento de los objetivos de seguridad de la información (ver anexo 1)

5.1.3.2 Identificación de controles

- Controles actuales: en el contexto de los riesgos, un control desalienta la ocurrencia de una amenaza (reduce la probabilidad de ocurrencia) o mitiga el impacto de una amenaza (mitiga el impacto del daño).

5.1.3.3 Riesgo

En esta sección se analiza el riesgo considernado los controles actuales previamente identificados.

- **Aspecto de seguridad afectado:** Indica si el riesgo afecta la confidencialidad, integridad y disponibilidad del activo de información (ver tabla 7).
- **Valor y nivel del impacto:** Considerando a qué aspecto de seguridad afecta el riesgo (ver tabla 7) indica el nivel del impacto del riesgo (ver tabla 8).
- **Valor y nivel de la probabilidad de ocurrencia:** Indica la probabilidad de ocurrencia de la explotación de la vulnerabilidad por la amenaza considernado los controles actuales (ver tabla 10).
- **Valor del riesgo:** Se estima el valor del riesgo como la multiplicación de los valores de calificación respecto a la probabilidad e impacto siguiendo la siguente formula:

$$Valor\ del\ riesgo = Probabilidad \times Impacto$$

- Nivel del riesgo: Indica el nivel del riesgo según el valor de riesgo identificado previamente (ver tabla 11).

5.1.4. Evaluación de riesgos de seguridad de la información

La Alta Dirección establece como criterio de aceptación del riesgo el nivel **MEDIO**, lo que implica no tratar los riesgos categorizados como “Muy bajo” y “Bajo” y tratar los riesgos categorizados como “Alto” y “Muy alto”.

- **Comparación con el criterio de aceptación del riesgo:** Se compara el valor de riesgo obtenido con el criterio de aceptación del riesgo de la institución. En caso resulte superior al criterio de aceptación del riesgo se debe colcoar en el formato “Tratar”, lo que significa que este riesgo pasará al plan de tratamiento de riesgos y se decidirá una opción de tratamiento.
- **Factores de priorización:** Indica los criterios para realizar valoraciones de riesgo de seguridad de la información en base a los factores relevantes (ver tabla 12).

Tabla 12: Calificación de los factores de priorización

Calificación	Legal	Economico	Operacional	Imagen
Bajo (1)	No hay afectación.	Pérdidas mínimas, reducción de la utilidad en menos del 5%	Se opera parcialmente y no afecta las operaciones.	Afectación mínima de la imagen del personal regular.
Medio (2)	Se afecta al personal regular de la institución.	Pérdidas medias, reducción de la utilidad entre 5% y 10%	Las operaciones tardan días en reanudarse.	Deterioro de la imagen de un área de la institución.
Alto (3)	Se afecta a uno de los Directores o algún personal especializado de la institución.	Pérdidas altas, reducción de la utilidad entre 10% y 15%.	Las operaciones tardan semanas en reanudarse o simplemente no se pueden recuperar.	Deterioro de la imagen de varias áreas de la institución
Extremo (4)	Se afecta la permanencia de una de las áreas o de toda la institución.	Perdidas mayores, reducción de utilidad mayor a 15%	No se pueden recuperar las operaciones.	Deterioro de la imagen de toda la institución.

- **Valor de priorización:** Indica el valor de priorización considerando la calificación de los factores utilizando la siguinete formula:

$$Valor\ de\ priorización\ = \frac{Legal + Económico + Operacional + Imagen}{4}$$

- **Priorización del riesgo:** indica el nivel de priorización del riesgo para el tratamiento de riesgos.

Tabla 13: Escala de priorización

Valor	Nivel
1	Bajada prioridad
2	Prioridad media
3	Alta prioridad
4	Muy alta prioridad

5.1.5. Tratamiento de riesgos de seguridad de la información

Para continuar con la estapa de tratamiento de riesgos, se utiliza el formato SGSI.FR.02: Matriz de riesgos de seguridad de la información y plan de tratamiento considerando los siguientes atributos:

5.1.5.1 Establecimiento de la estrategia de tratamiento

- **Opción de tratamiento:** una vez efectuado la identificación, analisis y evaluación del riesgo, se decide qué medidas se utilizarán para tratar el riesgo (ver tabla 14 y 15).

Tabla 14: Opciones de tratamiento para los riesgos

Opción	Descripción
Evitar	Dejar de realizar la actividad que genera el riesgo debido a que el nivel de riesgo es inaceptable.
Reducir (mitigar)	Establecer controles para disminuir la probabilidad de ocurrencia del riesgo.
Transferir	Trasferir a un tercero con la capacidad o especialización necesaria para administrar adecuadamente el riesgo, o enfrentar las pérdidas originadas ante la ocurrencia de la adversidad. Los seguros transfieren el riesgo de pérdida financiera del asegurado al asegurador. Las transferencia parciales consisten en compartir los riesgos, dando la responsabilidad a un tercero.
Retener (aceptar)	Aceptar el riesgo en su presente nivel realizando una adecuada administración y monitoreo. Para lo cual se debe verificar que cumpla con los criterios de aceptación de risgos definidos.

Tabla 15: Sustentos para seleccionar un tipo de tratamiento de risgos

Opción	¿Cuándo seleccioanarlo?
Evitar	Se seleccionará esta alternativa, cuando el beneficio de implementar un control sea menor al costo del riesgo inherente y sus consecuencias.
Reducir (mitigar)	Se seleccionará esta alternativa, cuando el beneficio de implementar un control sea mayor al costo del riesgo inherente y la institución se encuentre en la capacidad de realizar el tratamiento del riesgo.
Transferir	Se seleccionará esta alternativa, cuando el benefico de implementar un control sea mayor al costo de riesgo inherente y un tercero tenga una mayor capacidad para realizar el tratamiento del riesgo, debido a su especialización, infraestructura entre otros factores.
Retener (aceptar)	Se seleccionará esta alternativa, cuando cumpla con alguno de los criterios de aceptación de riesgos (ejemplo): a) El costo de tratar el riego se estima como mayor a la perdida o impacto economico generado por la ocurrencia del mismo. b) El costo de implementar el control o controles está fuera de presupuesto del año en curso.

	c) No se dispone de recursos o se sufre recortes de presupuesto por decisión de la Alta Dirección de la Institución.

- Los riesgos que, al ser evaluados, se encuentren dentro de la opción de tratamiento de "Retener (aceptar)", deben ser formalmente aprobados por el propietario del riesgo con el formato SGSI.FR.003: Aceptación de reisgos de seguridad de la información.

- El plan de tratamiento de riesgos es aprobado por los propietarios de los riesgos con el formato SGSI.FR.04: Aceptación del plan de tratamiento de riesgos de seguridad de la información y riesgos residuales, en señal de haber aceptado los riesgos residuales estimados de la seguridad de la información.

5.1.5.2 Plan de acción

En los casos en los cuales se requiera de la implemenetación de un control, se sugiere realizar lo siguiente:

- ✓ Utilizar el anexo A de la NTP ISO/IEC 27001:2014, el cual incluye 14 dominios, 35 objetivos de control y 114 controles.
- ✓ Diseñar y planificar la implementación de control, documentándolo mediante el registro de los siguientes datos:
  - Descripción del control
  - Relación con el Anexo A de la ISO/IEC 27001 (en caso de aplicar)
  - Responsable de la implementación
  - Costo de implementación (en caso de aplicar)
  - Tiempo de la implementación, fecha de inicio y fecha de fin

5.1.5.3 Estimación del riesgo residual estimado

El riesgo residual sirve como indicador para medir la efectividad de los controles, es por eso que, al momento de planificar los controles de seguridad, se debe medir la probabilidad e impacto estimado para obtener el nivel de riesgo residual que se espera obtener.

5.1.5.4 Seguimiento

El OSI debe realizar el seguimiento de la implementación del control de manera continua considerando el estado del mismo (ver tabla 16).

Tabla 16: Estado de ejecución

Estado de ejecución	Descripción
Pendiente	Sin implementar. Se establecerá este estado una vez establecido los plazos que tomará la implementación del control.
En proceso	En proceso de implementación. Se establecerá este estado cuando ya se empezó con la implemenetación de acciones o control establecidos.
Implementado y en operación	Se consignará este estado cuando ya se concluyó la implementación de las acciones de tratamiento.
Suspendido	Se considera a aquellas acciones desestimadas. Se deberá justificar esta deceisión y actualziar la estartegia de tratamiento, de corresponder.

5.1.6. Estimación del riesgo residual

El riesgo residual sirve como indicador para medir la efectividad de los controles, es por eso que luego de implementar los controles de seguridad de acuerdo al plan de tratamiento de riesgos de seguridad de la información, se debe medir la probabilidad, impacto para obtener el nivel de riesgo residual.

Si el riesgo residual no es aceptable para la institución, entonces se reevaluarán los riesgos, y de ser el caso, se establecen nuevos controles o actividades que logren mantener el riesgo residual en un nivel aceptable.

5.2. GESTIÓN DE RIESGOS Y OPORTUNIDADES DEL SGSI

A partir del analisis de contexto interno y externo y de comprender las necesidades y expectativas de las partes interesadas, se identifican riesgos y oprotunidades del SGSI que permitan:

- Asegurar que el sistema de gestión pueda lograr los resultados esperados
- Prevenir o reducir efectos indeseados
- Lograr la mejora continua

El proceso de gestión y oportunidaes del SGSI comprende:

- Identificación de riesgos y oportunidades
- Analisís de riesgos y oportunidades
- Evaluación de riesgos y oportunidades
- Definición de acciones para tratar dichos riesgos y oportunidades
- Analisis de riesgos y oportunidades residuales

Este proceso se registra en el formato SGSI.FR.05: Matriz de riesgos y oportunidades dek SGSI y plan de tratamiento.

5.2.1. Riesgos de SGSI

5.2.1.1 Identificación de riesgos

En esta estapa se busca identificar los riesgos que se van a gestionar, es esencial incluir todos los riesgos, sea que estén o no bajo el control de la institución, debido a que un riesgo potencial no identificado durante esta etapa será excluido del análisi posterior.

El OSI gestiona y brinda la asistencia técnica para que las direcciones o áreas involucradas en el alcance del SGSI, identifiquen y actualicen los riesgos considerando el analisis del contexto de la organizacipon y las partes interesadas relevantes al SGSI.

El OSI centraliza el registro de los riesgos en el formato SGSI.FR.05: Matriz de riesgos y oportunidades del SGSI y plan de tratamiento, considerando los siguientes atributos:

- Código: indica la asignación de un codigo al riesgo según la siguiete estructura:

  RI.año.númerocorrelativo

  i. RI: mnemónico relativo a “riesgo de información”.
  ii. Año: relacionado al ítem a.Año.
  iii. Número correlativo: nímero correlativo comenzando en el 1.

- Descripción: indica el detalle del riesgo identificado.
- Propietario del riesgo: indica el nombre de una persona, una institución u otra parte interesada con la responsabilidad y autoridad para administrar el riesgo.

5.2.1.2 Identificación de riesgos

- **Valor y nivel del impacto:** indica el nivel del impacto que la oportunidad se materialice (ver tabala 17).

Tabla 17: Escala del impacto del riesgo

ESCALA DE IMPACTO		
Valor	**Nivel**	**Descripción**
1	**Insignificante**	No afectaria actividades ni procesos de la institución o terceros.
2	**Menor**	Afectaría una actividad o proceso no criticos de la institución o terceros.
3	**Moderado**	Podróia ocasionar un perjuicio en una o más de una actividade o proceso crítico de la institución o terceros.
4	**Mayor**	Podría ocasionar un perjuicio significativo para la institución o terceros y que podría impedir la ejecución de las actividades de la institución.
5	**Muy significativo**	Podría ocasionar un perjuicio muy significativo para la institución o terceros y que podría impedir la ejecucicón de las actividades, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones.

- **Valor y nivel de la probabilidad de ocurrencia:** indica la probabilidad de ocurrencia de la explotación de la vulnerabilidad por la amenaza (ver tabla 18).

Tabla 18: Escala de la probabilidad de ocurrencia del riesgo

ESCALA DE PROBABILIDAD			
Valor	**Nivel**	**Descripción**	
1	**Raro**	Puede ocurrir en circustancias excepcinales.	No se ha presentado en el último año.
2	**Improbable**	No esperado, pero podría ocurrir algunas veces.	Se ha presentado al menos 2 veces al año.
3	**Posible**	Es posible que ocurra el evento con una frecuencia media.	Se ha presentado al menos una vez en el trimestre.
4	**Probable**	Existen antecedentes de que el evento ocurrirá dentro de un plazo de tiempo.	Se ha presentado una o más de una vez al mes.
5	**Casi seguro**	Se sabe que ocurre con cierto grado de certeza y que la frecuencia es muy alta o casi cierta.	Se ha presentado una o más de una vez a la semana.

- Valor del riesgo: se estima el valor del riesgo como la multiplicación de los valores de calificación respescto a la probabilidad e impacto siguiendo la siguiente fórmula:

$$Valor\ del\ riesgo = Probabilidad \times Impacto$$

- Nivel del riesgo: indica el nivel del riesgo según el valor de riesgo identificado previamente (ver tabla 19).

Tabla 19: Escala del riesgo

Valor	Nivel
1 – 2	Muy bajo
3 – 4	Bajo
5 – 10	Medio
12 – 16	Alto
20 - 25	Muy alto

La dupla Impacto-Probabilidad de un riesgo se grafican en una tabla de doble entrada y de esta forma se obtiene graficamente los riegos que tienen más probabilidad de ocurrencia y que causan más daño al cumplimiento de los objetivos de seguridad de la información (ver anexo 1).

5.2.1.3 Evaluación de riesgos

Se utiliza las mismas calificaciones del punto 4.1.4.

5.2.1.4 Plan de tratamiento de riesgos

Se utiliza las mismas calificaciones del punto 4.1.5.

5.2.2. Oportunidades del SGSI

5.2.2.1 Identificación de oportunidades

Se debe identificar las posibles fuentes de oportunidades que permitan mejorar el funcionamiento del SGSI y seguridad de la información en la institución, además identificar el propietario de dicha oportunidad.

El OSI gestiona y brinda la asistencia técnica para que las direcciones o áreas involucradas en el alcance del SGSI identificación y actualicen las oportunidades considerando el analisis del contexto de la organización y las partes interesadas relevantes al SGSI.

El OSI centraliza el registro de las oportunidades en el formato SGSI.FR.05: Matriz de riesgos y oportunidades del SGSI y plan de tratamiento, considerando los siguientes criterios:

- **Código:** indica la asignación de un código a la oportunidad según la siguiente estructura:

  OP.año.númerocorrelativo

  i. OP: mnemónico relativo a “oportunidad”.
  ii. Año: relacionado al ítem a. Año.
  iii. Número correlativo: número correlativo comenzando en el 1.
- **Descripción:** indica el detalle de la oportunidad identificado que puede afectar a uno o varios activos de información y que sirva para identificarlo respecto de otros.

- **Propietario de la oportunidad:** indica el nombre de una persona, una institución u otra parte interesada con la responsabilidad y autoridad para administrar la oportunidad.

5.2.2.2 Analisis de oportunidades

- **Nivel del impacto:** considerando los beneficios en base a los criterios definidos por la institución que afectan la operatividad del negocio (ver tabla 20).

Tabla 20: Escala de impacto de la oportunidad

ESCALA DE IMPACTO		
Valor	Nivel	Descripción
1	**Insignificante**	Al presentarse, su aprovechamiento no afecta sustancialmente los objetivos institucionales.
2	**Menor**	Al presentarse genera oportunidades en la prestación del servicio de la institución, los cuales no impacta sustancialmente en los requisitos de las partes interesadas.
3	**Moderado**	Al presentarse potenciará los procesos de soporte, se debe analizar el costo del aprovechamiento y el beneficio que daría a la institución aprovecharlo.
4	**Mayor**	Al presentarse potenciará los procesos de negocio, se debe analizar el costo del aprovechamiento y el beneficio que daría a la institución aprovecharlo.
5	**Muy significativo**	Al presentarse puede generar beneficios para la institución para el cumplimiento de los objetivos estratégicos.

- **Valor y nivel de la probabilidad de ocurrencia**: indica la probabilidad de ocurrencia que la oportunidad se materialice considerando el contexto actual (ver tabla 21).

Tabla 11: Escala de probabilidad de la oportunidad

ESCALA DE PROBABILIDAD			
Valor	Nivel	Descripción	
1	**Raro**	Puede ocurrir en circunstancias excepcionales.	No se ha presentado en el último año.
2	**Improbable**	No esperado, pero podría ocurrir algunas veces.	Se ha presentado al menos 2 veces al año.
3	**Posible**	Es posible que ocurra el evento con una frecuencia media.	Se ha presentado al menos una vez en el trimestre.
4	**Probable**	Existen antecedentes de que el evento ocurrirá	Se ha presentado una o más de una vez al mes.

		dentro de un plazo de tiempo.	
5	**Casi seguro**	Se sabe que ocurre con cierto grado de certeza y que la frecuencia es muy alta o casi cierta.	Se ha presentado una o más de una vez a la semana.

- **Valor de la oportunidad:** se estima el valor de la oportunidad como la multiplicación de los valores de calificación respecto a la probabilidad e impacto siguiendo la siguiente fórmula:

$$Valor\ de\ la\ oportunidad = Probabilidad \times Impacto$$

- **Nivel de la oportunidad:** indica el nivel de la oportunidad según el valor de la oportunidad identificado previamente (ver tabla 22).

Tabla 22: Escala de la oportunidad

Valor	Nivel
1 – 2	Muy bajo
3 – 4	Bajo
5 – 10	Medio
12 – 16	Alto
20 – 25	Muy alto

La dupla Impacto-Probabilidad de un riesgo se grafican en una tabla de doble entrada y de esta forma se obtiene gráficamente las oportunidades que tienen más probabilidad de ocurrencia y que pueden ayudar al cumplimiento de los objetivos de seguridad de la información (ver anexo 1).

5.2.2.3 Evaluación de riesgos de seguridad de la información

La Alta Dirección establece como criterio de aceptación de la oportunidad el nivel **MEDIO**, lo que implica no tratar las oportunidades categorizadas como “Muy bajo” y “Bajo” y tratar las oportunidades categorizadas como “Alto” y “Muy alto”.

- **Comparación con el criterio de aceptación de la oportunidad:** se compara el valor de la oportunidad obtenido con el criterio de aceptación de oportunidades de la institución. En caso resulte superior al criterio de aceptación de la oportunidad se debe colocar en el formato “Tratar”, lo que significa que esta oportunidad pasará al plan de tratamiento y se decidirá una opción de tratamiento.
- **Priorización de la oportunidad**: indica el nivel de priorización de la oportunidad para su tratamiento (ver tabla 23).

Tabla 23: Calificación de los factores de priorización de la oportunidad

Calificación	Legal	Económico	Operacional	Imagen
Bajo 1	No hay beneficios de cumplimiento.	Ganancias mínimas, aumento de la utilidad en menos del 5%.	Se mejora parcialmente las operaciones.	Aumenta mínimamente la imagen del personal regular.
Medio 2	Hay beneficios medios de cumplimiento.	Aumento de la utilidad entre 5% y 10%.	Se mejora medianamente las operaciones.	Aumento de la imagen de un área de la institución.
Alto 3	No hay beneficios altos de cumplimiento.	Aumento de la utilidad entre 10% y 15%.	Se mejora altamente las operaciones.	Aumento de la imagen de varias áreas de la institución
Extremo 4	No hay beneficios muy altos de cumplimiento.	Aumento de la utilidad mayor a 15%.	Se mejora extremadamente las operaciones.	Aumento de la imagen de toda la institución.

- **Valor de priorización:** indica el valor de priorización considerando la calificación de los factores utilizando la siguiente fórmula:

$$Valor\ de\ priorización = \frac{Legal + Económico + Operacional + Imagen}{4}$$

- **Priorización del riesgo:** indica el nivel de priorización del riesgo para el tratamiento de riesgos (ver tabla 24).

Tabla 24: Escala de priorización

Valor	Nivel
1	Baja prioridad
2	Prioridad media
3	Alta prioridad
4	Muy Alta prioridad

5.2.2.4 Tratamiento de oportunidades

Para continuar con la etapa de tratamiento de oportunidades, se utiliza el formato SGSI.FR.05: Matriz de riesgos y oportunidades del SGSI y plan de tratamiento considerando los siguientes atributos:

A. Establecimiento de la estrategia de tratamiento

- **Opción de tratamiento de la oportunidad**: una vez efectuado la identificación, análisis y evaluación de la oportunidad, se debe decidir qué medidas se deben de utilizar para tratar la oportunidad (ver tabla 25).

Tabla 25: Opción de tratamiento de oportunidades

Opción de tratamiento de oportunidades	
Explotar	Tratar de hacer que la oportunidad definitivamente suceda. Se deben tomar medidas para asegurar que los beneficios de la oportunidad se realicen.
Ignorar	No tomar la oportunidad identificada.

B. Plan de acción

En los casos en los cuales se requiera de la implementación de un control, se debe diseñar y planificar la implementación del control, documentándolo mediante el registro de los siguientes datos:

- Descripción del control
- Relación con el Anexo A de la ISO/IEC 27001 (en caso de aplicar)
- Responsable de la implementación
- Costo de implementación (en caso de aplicar)
- Tiempo de la implementación, fecha de inicio y fecha de fin

C. Estimación del nuevo nivel de la oportunidad estimada

El nuevo nivel de la oportunidad sirve como indicador para medir la efectividad de los controles, es por eso que, al momento de planificar los controles de seguridad, se debe medir la probabilidad e impacto estimado para obtener el nivel de la oportunidad que se espera obtener.

D. Seguimiento

El OSI debe realizar el seguimiento de la implementación del control de manera continua considerando el estado del mismo (ver tabla 26).

Tabla 26: Estado de ejecución

Estado de ejecución	Descripción
Pendiente	Sin implementar. Se establecerá este estado una vez establecido los plazos que tomará la implementación del control.
En proceso	En proceso de implementación. Se establecerá este estado cuando ya se empezó con la implementación de acciones o controles establecidos.
Implementado y en operación	Se consignará este estado cuando ya se concluyó la implementación de las acciones de tratamiento.
Suspendido	Se considera a aquellas acciones desestimadas. Se deberá justificar esta decisión y actualizar la estrategia de tratamiento, de corresponder.

5.2.2.5 Estimación del nuevo nivel de la oportunidad

El nuevo nivel de la oportunidad sirve como indicador para medir la efectividad de las acciones implementadas para materializar la oportunidad identificada, es por eso por lo que se debe medir otra vez la probabilidad e impacto para obtener el nuevo nivel de la oportunidad.

Si el nuevo nivel de la oportunidad no es aceptable para la institución, entonces se considerará reevaluar la oportunidad, y de ser el caso, se establecen nuevos controles o actividades para lograr que se materialice.

6. FORMATOS

- DGSI-07.FR.01 Inventario de activos de información
- DGSI-07.FR.02 Matriz de riesgos de seguridad de la información y plan de tratamiento
- DGSI-07.FR.03 Aceptación de riesgos de seguridad de la información
- DGSI-07.FR.04 Aceptación del plan de tratamiento de riesgos de seguridad de la información y riesgos residuales
- DGSI-07.FR.05 Matriz de riesgos y oportunidades del SGSI y plan de tratamiento

7. ANEXOS

- **Anexo 1**

Tabla 27: Mapa de calor del riesgo

MAPA DE CALOR					
PROBABILIDAD					
5 Casi seguro	**Medio 5**	**Medio 10**	**Alto 15**	**Muy alto 20**	**Muy alto 25**
4 Probable	**Bajo 4**	**Medio 8**	**Alto 12**	**Alto 16**	**Muy alto 20**
3 Posible	**Bajo 3**	**Medio 6**	**Medio 9**	**Alto 12**	**Alto 15**
2 Improbable	**Muy Bajo 2**	**Bajo 4**	**Medio 6**	**Medio 8**	**Medio 10**
1 Raro	**Muy Bajo 1**	**Muy Bajo 2**	**Bajo 3**	**Bajo 4**	**Medio 5**
	1 Insignificante	**2 Menor**	**3 Moderado**	**4 Mayor**	**5 Muy significativo**
	IMPACTO				

	FORMATO 01	Código:	DGSI-07.FR.01
PERÚ Ministerio de Vivienda, Construcción y Saneamiento		Versión:	1.0
	INVENTARIO DE ACTIVOS DE INFORMACIÓN	Clasificación:	Uso Interno
		Página:	1 de 1

Fecha de actualización de matriz:		Responsable de actualización de matriz:	

Fecha de inicio	Proceso	Subproceso	Código	Nombre	Descripción	Categoría	Tipo	Ubicación (física o lógica)	Propietario	Custodio	Requerimiento (legal, reglamentario, contractual)	Clasificación según el tipo de uso	Calificación (CID)						Tasación	
													C	Confidencialidad	I	Integridad	D	Disponibilidad	Valor del activo	Nivel del activo
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-
													-		-		-		0.00	-

	FORMATO 02	Código:	DGSI-07.FR.02
		Versión	1.0
	MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PLAN DE TRATAMIENTO	Clasificación:	Uso Interno
		Página:	1 de 1

Fecha de actualización de matriz:		Responsable de actualización de matriz:	

ACTIVO DE INFORMACIÓN			IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN																		
								Aspecto de seguridad afectado			Escala de impacto		Escala de probabilidad		Escala de riesgo inherente			Aspecto de seguridad afectado			Escala de impacto		Escala de probabilidad		Escala de riesgo	
Código	Nombre del activo de información	Nivel del activo de información	Vulnerabilidad	Amenaza	Código del riesgo	Riesgo	Propietario del riesgo	C	I	D	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor de riesgo inherente	Nivel de riesgo inherente	Controles actuales	C	I	D	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor de riesgo	Nivel de riesgo
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-
											0	-		-	0	-					0	-		-	0	-

EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN										
	Factores de priorización									
Comparación con el criterio de aceptación del riesgo	Legal		Económico		Operacional		Imagen		Valor de priorización del riesgo	Nivel de priorización del riesgo
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!
-		-		-		-		-	#¡DIV/0!	#¡DIV/0!

PLAN DE TRATAMIENTO															RIESGO RESIDUAL					
	Plan de acción						Escala de impacto estimado		Escala de probabilidad estimada		Escala de riesgo residual		Seguimiento		Escala de impacto		Escala de probabilidad		Escala de riesgo residual	
Opción de tratamiento	Descripción del control	Relación con el Anexo A de la ISO/IEC 27001 (en caso de aplicar)	Responsable de implementación	Costo de implementación (en caso de aplicar)	Fecha de inicio	Fecha de fin	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor de riesgo	Nivel de riesgo	Estado de ejecución	Responsable de seguimiento	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor de riesgo	Nivel de riesgo
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-
							0	-		-	0	-			0	-		-	0	-

ACEPTACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como Propietario del Riesgo, declaro:

- Entender que la seguridad de la información es importante para el funcionamiento de los sistemas de información, comunicaciones y procesos de negocio de la institución**.**
- Entender que el análisis de riesgos es un proceso continuo y que los riesgos que hoy no representan un riesgo a tratar, en el futuro podrían pasar a ser necesarios de tratar.
- Entender que la aceptación de riesgos es una decisión tomada con responsabilidad.
- Entender que un riesgo aceptado, debe ser monitoreado en los sucesivos análisis de riesgo que se realicen, para evitar que cause daños a futuro en la institución; sin embargo, como Propietario del riesgo, asumo la responsabilidad de aceptar el (los) riesgo(s) aquí descritos.
- Entender que la responsabilidad asumida significa que la aceptación de estos riesgos puede comprometer los sistemas y/o los procesos de negocio.
- La aceptación actual de estos riesgos no significa que partir de la fecha de firma de este documento, debido a un cambio de las condiciones actuales, se decida implementar controles para mitigarlo(s).
- Haber leído la declaración y estar de acuerdo en aceptar los siguientes riesgos:

N°	Código del activo	Nombre del activo	Código del riesgo	Nombre del riesgo	Valor / Nivel de riesgo
1					
2					
3					
4					
5					

Nombre y apellidos	Cargo	Fecha	Firma

ACEPTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y LOS RIESGOS RESIDUALES

Como Propietario del Riesgo, declaro:

- Comprender y aprobar el plan de tratamiento de riesgos de seguridad de la información que me involucre como propietario, por tanto, me comprometo a la implementación de los controles y/ o acciones indicadas en este documento.
- Reconozco que la implementación de controles para el tratamiento de riesgos es un proceso que reducirá la probabilidad o el impacto de los riesgos, por lo que su ejecución no hace que la institución sea invulnerable frente a los riesgos residuales.
- Acepto los riesgos residuales estimados, producto de la implementación de los controles, decisión tomada con entera responsabilidad y en forma voluntaria.
- Declaro que la aceptación de estos riesgos residuales estimados puede variar, dado que los riesgos identificados tendrán que ser evaluados en una nueva gestión de riesgos, cuando ocurran cambios relevantes al SGSI o en el próximo ciclo de SGSI.

N°	Código del activo afectado	Código del riesgo	Controles a implementar	Valor / Nivel de riesgo residual estimado
1				
2				
3				
4				
5				

Nombre del propietario del riesgo	Cargo	Fecha	Firma

Ministerio de Vivienda, Construcción y Saneamiento	FORMATO 05	Código:	DGSI-07.FR.05
		Versión:	1.0
	MATRIZ DE RIESGOS Y OPORTUNIDADES DEL SGSI Y PLAN DE TRATAMIENTO	Clasificación:	Uso Interno
		Página:	1 de 1

Fecha de actualización de matriz:		Responsable de actualización de matriz:	

	IDENTIFICACION DE RIESGOS/OPORTUNIDADES DEL SGSI			ANÁLISIS DE RIESGOS/OPORTUNIDADES DEL SGSI						EVALUACIÓN DE RIESGOS/OPORTUNIDADES DEL SGSI							PLAN DE TRATAMIENTO															RIESGO/OPORTUNIDAD RESIDUAL					
Tipo	Código	Descripción	Propietario	Escala de impacto		Escala de probabilidad		Escala de riesgo / oportunidad		Comparación con el criterio de aceptación	Criterios de priorización				Valor de priorización	Nivel de priorización	Opción de tratamiento	Plan de acción						Escala de impacto estimado		Escala de probabilidad		Escala de riesgo / oportunidad residual estimado		Seguimiento		Escala de probabilidad		Escala de impacto		Escala de riesgo/oportunidad residual	
				Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor	Nivel		Legal	Económico	Operacional	Imagen				Descripción del control	Relación con el Anexo A de la ISO/IEC 27001 (en caso	Responsable de implementación	Costo de implementación (en caso de aplicar)	Fecha de inicio	Fecha de fin	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor	Nivel	Estado de ejecución	Responsable de seguimiento	Valor de impacto	Nivel de impacto	Valor de probabilidad	Nivel de probabilidad	Valor de riesgo/oportunidad	Nivel de riesgo/oportunidad
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-
					-		-	0	-	-					0	-									-		-	0	-				-		-	0	-