# METODOLOGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

## SGSI-ME-01

| Elaborado por: | Revisado por: | Aprobado por: |
|---|---|---|
| ..... | ..... | ..... |
| Nombre y Firma | Nombre y Firma | Nombre y Firma |

# ÍNDICE

## 1. OBJETIVO

Establecer el marco metodológico para la ejecución del proceso de gestión de riesgos de Seguridad de la Información de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).

## 2. REFERENCIAS NORMATIVAS

**2.1.** NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.

**2.2.** Resolución de Superintendencia Nº 025 -2018/SUNAT. Aprueban la Política Institucional de Administración de Riesgos y la Metodología de Administración de Riesgos Institucional (MARI)

## 3. DEFINICIONES

**3.1.** Activo de información: Elemento que contiene o administra información, a través del cual la entidad obtiene beneficios para el logro de sus objetivos estratégicos.

**3.2.** Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u entidad.

**3.3.** Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**3.4.** Clasificación de los activos de información: Categorización de los activos que tienen valor para la entidad.

**3.5.** Comité de Gestión de Seguridad de la Información: Es un comité ejecutivo conformado por altos directivos de la entidad, designado para gestionar, supervisar, revisar e informar de manera permanente los aspectos del SGSI.

**3.6.** Confidencialidad: Propiedad que determina que la información no esté disponible, ni sea divulgada a personas o procesos no autorizados.

**3.7.** 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.

**3.8.** Criterio de aceptación del riesgo: Condición, establecida formalmente, que ayuda a determinar el nivel de riesgos con los que puede convivir la entidad.

**3.9.** Custodio del activo: Identifica a la persona o la entidad que tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones definidas por el propietario del activo.

**3.10.** Disponibilidad: Propiedad que asegura que los usuarios autorizados tienen acceso a la información cuando la requieran.

**3.11.** Equipo de gestión de riesgos: Es el conjunto de especialistas en los activos de información del proceso.

**3.12.** Estimación del riesgo: Proceso para asignar valores a la probabilidad y el impacto de un riesgo.

**3.13.** Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables y decidir si corresponde o no tratarlo.

**3.14.** Gestión de riesgos: Actividades coordinadas para dirigir y controlar el riesgo en una entidad.

**3.15.** Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

**3.16.** Impacto: Nivel de afectación en el logro de los objetivos de la organización o el proceso.

**3.17.** Incidente de seguridad de la información: Evento no deseado que tiene probabilidad de comprometer operaciones del negocio y amenazar la seguridad de la información.

**3.18.** Información: Conjunto de datos organizados y con significado, en poder de la entidad que poseen valor para la misma, independientemente de la forma (impresa, oral, escrita, etc.) o de su origen.

**3.19.** Integridad: Propiedad de salvaguardar la exactitud y totalidad de los activos de información.

**3.20.** Inventario de activos: Es un registro conformado por los activos de información que tienen valor para la entidad y que están dentro del alcance del SGSI.

**3.21.** Nivel de exposición al riesgo: Grado de que un riesgo se materialice causando un impacto.

**3.22.** Oficial de Seguridad de la Información: Es el coordinador del Comité de Gestión de Seguridad de la Información y principal responsable operativo de la implementación del SGSI.

**3.23.** Probabilidad: Es la posibilidad de que un evento cualquiera ocurra o no.

**3.24.** Probabilidad de ocurrencia del riesgo: Probabilidad de que una amenaza explote una vulnerabilidad.

**3.25.** Propietario del activo: Identifica a la persona o la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

**3.26.** Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

**3.27.** Respuesta al riesgo: Decisión o estrategia para tratar el riesgo, pudiendo ser: aceptar, evitar, transferir o reducir el riesgo.

**3.28.** Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

**3.29.** Riesgo efectivo: Nivel de riesgos que se posee actualmente.

**3.30.** Riesgo residual: Riesgo remanente después de ser tratado.

**3.31.** Tratamiento de riesgos: Proceso de selección e implementación de controles para minimizar el riesgo.

**3.32.** Usuarios de los activos de información: Personas que usan los activos de información de la entidad en sus actividades diarias.

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

**SIGLAS**

**3.34.** CGSI: Comité de Gestión de Seguridad de la Información.

**3.35.** EGR: Equipo de Gestión de Riesgos.

**3.36.** OFSI: Oficial de Seguridad de la Información.

**3.37.** SGSI: Sistema de Gestión de Seguridad de la Información.

**3.38.** SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria.

## 4. METODOLOGÍA DE GESTION DE RIESGOS

El proceso de gestión de riesgos de seguridad de la información será desarrollado en un ciclo de mejora continua que se repetirá anualmente, de tal forma que se asegure el control continuo de los riesgos de seguridad de la información llevándolos a niveles aceptables. En casos excepcionales, que comprendan cambios significativos en la entidad, en sus procesos o la ocurrencia de algún evento relevante que justifique su ejecución, se podrá iniciar un ciclo de gestión de riesgos no planificado.

El proceso de evaluación de riesgos de seguridad de la información se realizará mediante talleres con el Equipo de Gestión de Riesgos, el Oficial de Seguridad en coordinación con el Propietario del Riesgo planificará la realización del proceso de evaluación de riesgos.

El Oficial de Seguridad de la Información realizará una charla de capacitación al Equipo de Gestión de Riesgos y Propietarios del Riesgo con el fin de explicar la presente metodología y los formatos a utilizar, así como dar a conocer los niveles de riesgo, criterios de aceptación de riesgos, niveles de riesgo aceptables y, los criterios para la realización de las evaluaciones de riesgos de seguridad de la información.

El proceso de gestión de riesgos de la seguridad de la información está conformado por las fases que se muestran en la Tabla N° 1:

**Tabla N° 1:** Fases de la Gestión de Riesgos

| PROCESO | FASES |
|---|---|
| **Gestión de Riesgos** | Fase 0: Criterios Básicos |
| | Fase 1: Inventario de Activos |
| | Fase 2: Análisis de Riesgos |
| | Fase 3: Evaluación de Riesgos |
| | Fase 4: Plan de Tratamiento de Riesgos |

## 5. FASE 0: CRITERIOS BÁSICOS

En esta fase inicial se presentan los distintos criterios básicos que serán utilizados en el proceso de gestión de riesgos. Estos criterios están relacionados a la tasación

de activos, criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo.

### 5.1. Tasación de Activos

Con la finalidad de definir el alcance de los activos de información, se han definido los siguientes niveles de tasación de activos, que van desde bajo, medio hasta alto.

El criterio para determinar el alcance de los activos define que solo aquellos activos con un valor alto formarán parte del alcance de activos que pasan a la siguiente fase de Análisis de Riesgos.

En el numeral 5.3 se definen los criterios establecidos para la valoración de los activos.

### 5.2. Evaluación del Riesgo

La SUNAT reconoce los cinco niveles de riesgos: **Extremo, Alto**, **Medio**, **Bajo y No Significativo**. Asimismo, considera que el nivel de riesgo aceptado corresponde a aquellos clasificados como **Medio**, **Bajo y No Significativo,** es decir, aquellos que no ocasionan un impacto significativo sobre la seguridad de la información.

Los riesgos clasificados con nivel **Extremo y Alto** son considerados para ser tratados de acuerdo con lo descrito en la fase de tratamiento de riesgos, salvo en los casos que se detallan en la siguiente sección de Aceptación del Riesgo.

### 5.3. Criterios de Aceptación del Riesgo

Para los riesgos identificados como **Extremo y Alto** en la fase de Evaluación de riesgos, se ha definido que podrán ser aceptados cumpliendo con los siguientes criterios de aceptación del riesgo:

a) El costo de tratar el riesgo se estima como mayor a la pérdida o impacto económico 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.
d) Cuando la repercusión en las operaciones de otras tareas supera el impacto del riesgo.
e) Cuando la implementación del control implica conflictos contractuales o legales.

# 6. FASE 1: INVENTARIO DE ACTIVOS

El análisis de riesgos se deberá iniciar con la elaboración del inventario de activos de información de los procesos considerados dentro del alcance del SGSI. Los activos de información identificados.

## 6.1. Activos de Información

Se pueden diferenciar dos clases de activos de información: los activos primarios y activos de soporte.

**Los activos primarios de información:**

Los activos primarios de información comprenden principalmente:

- Información vital para la ejecución del proceso y su propósito.
- Información personal que se encuentra amparada por las leyes nacionales relacionadas con la privacidad.
- Información estratégica que se requiere para apoyar el logro de los objetivos estratégicos.
- Información de alto costo: a) cuya recolección, almacenamiento, y procesamiento exigen el uso intensivo de recursos por un largo periodo de tiempo y/o b) requiere una alta inversión para su adquisición.

**Los activos de soporte de información:**

Son activos de los cuales dependen los activos primarios del alcance:

- Software.
- Físicos.
- Servicios.
- Personal.

## 6.2. Identificación de Activos

Para cada proceso del alcance, se deberá preparar la lista de sus activos de información, en el cual se registran datos importantes para caracterizar y valorar al activo. (Ver formato SGSI-ME-01.FO-01 Inventario de Activos de Información):

- Código del activo.
- Nombre único del activo.

- Descripción del activo.
- Categoría y tipo del activo: Indica la naturaleza del activo (ver Tabla N° 2).
- Tipo de ubicación: Física o lógica.
- Ubicación: Descripción de la ubicación del activo.
- Clasificación: Respecto al grado de sensibilidad de la información. (ver Tabla N° 3).
- Frecuencia de uso: Diario, semanal, quincenal, mensual, anual, eventual (ver Tabla N° 4).
- Propietario del activo: Registrar el cargo del propietario del activo.
- Custodio del activo: Registrar el cargo del custodio del activo.
- Requisito legal, reglamentario o contractual: Si el activo está relacionado o sujeto a algún requerimiento, éste se debe indicar.
- Valor del activo: Alto, Medio, Bajo (ver Tabla N° 5).

A continuación, se muestran las Tablas N° 2, N° 3, y N° 4 utilizadas como referencia en la identificación de activos de información.

**Tabla N° 2:** Categorías y Tipos de Activo

| Categoría | Tipo de Activo |
|---|---|
| **Activos Primarios** | |
| **Información** | Información electrónica |
| | Información escrita |
| | Información hablada |
| | Otro tipo de información |
| **Activos de Soporte** | |
| **Software** | Software comercial o herramientas, utilitarios |
| | Software desarrollado por terceros |
| | Software desarrollado internamente |
| | Software de administración de base de datos |
| | Otro software |
| **Físicos** | Equipo de procesamiento |
| | Equipo de comunicaciones |
| | Medio de almacenamiento |
| | Mobiliario y equipamiento |
| | Otros equipos |
| **Servicios** | Procesamiento y comunicaciones |

| Categoría | Tipo de Activo |
|---|---|
| | Servicios generales |
| | Otros servicios |
| **Personal** | Clientes |
| | Empleados |
| | Accionistas |
| | Personal Externo |

**Tabla N° 3:** Clasificación de Sensibilidad

| Clasificación | Detalle |
|---|---|
| **Público** | Son activos que se consideran públicos, y que pueden ser accedidos tanto por miembros de la entidad como por personas externas a ella (público en general), sin estar sujetos a ningún control. |
| **Uso interno** | Son activos que son accedidos exclusivamente por personal interno de la entidad y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso. |
| **Confidencial** | Son activos que pertenecen a un proceso[1] que por su naturaleza son reservados exclusivamente al personal del proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso. Su revelación requiere la aprobación de su dueño o propietario, es de uso exclusivo de la organización, en el caso de terceros se deberá firmar acuerdo de confidencialidad y no divulgación. |
| **Restringida** | Son activos cuyo acceso es restringido a un grupo determinado de individuos, seleccionados a partir de un proyecto específico o que pertenecen a un grupo o nivel específico dentro de la entidad. Estos deben ser gestionados con todas las precauciones y controles posibles determinando exactamente que personas tienen acceso a los mismos y vigilando su uso, transporte y almacenamiento. |

[1] Un proceso o sub-proceso, puede ser soportado por una o más unidades organizacionales.

**Tabla N° 4:** Frecuencia de Uso

| Frecuencia de Uso |
|---|
| Diario |
| Semanal |
| Quincenal |
| Mensual |
| Anual |
| Eventual |

### 6.3. Valorización de Activos

El Equipo de Trabajo colocará la valoración del activo de información identificado, la cual se definen de la siguiente manera:

**Tabla N° 5:** Valor del Activo

| Activo | Detalle |
|---|---|
| **Alto** | Activo importante para la SUNAT. Su disponibilidad es necesaria para los procesos críticos de la SUNAT. |
| **Medio** | Constituye un soporte para los activos importantes de la SUNAT. La información puede estar replicada en varias fuentes o existen medios alternos. No compromete los procesos críticos de la SUNAT. |
| **Bajo** | Activos secundarios, que constituyen información para la toma de decisiones de un área específica. No compromete ningún proceso crítico de la SUNAT. |

## 7. FASE 2: ANÁLISIS DE RIESGOS

Completado el inventario de activos de información (Fase 1), en dónde se seleccionan los activos de información que definen el alcance del análisis de riesgos, se deberán identificar las posibles amenazas a las que están expuestos los mismos, así como también las vulnerabilidades y controles existentes. (Ver formato SGSI-ME-01.FO-02 Matriz de Riesgos de Seguridad de la Información).

### 7.1. Identificar Amenazas

En base a la lista de activos de información del alcance, se realizará la identificación de las amenazas asociadas a cada uno de ellos. En la Tabla N° 6 se expone un ejemplo de tipología de amenazas genéricas agrupadas por cada tipo de activo de información al cual podrían afectar.

**Tabla N° 6:** Tipos de Amenaza

| N° | Tipología de Amenaza | Tipo |
|---|---|---|
| 1 | Acceso no autorizado a la información | **Amenazas a la Información** |
| 2 | Modificación no autorizada de la información | |
| 3 | Eliminación no autorizada de la información | |
| 4 | Robo de activos contenedores de información | |
| 5 | Inadecuada eliminación de activos contenedores de información | |
| 6 | Corrupción de datos por error de procesamiento | |
| 7 | Uso extra laboral de la información | |
| 8 | Ataques de hacking/cracking sobre la información | |
| 9 | Virus informáticos que alteran o eliminan la información | |
| 10 | Fuga de Información | |
| 11 | Adulteración intencional del software (bombas lógicas, sabotaje) | **Amenazas al Software** |
| 12 | Cambios no autorizados sobre el software (mantenimientos) | |
| 13 | Actualizaciones no controladas del software (parches) | |
| 14 | Instalación de software no licenciado o autorizado | |
| 15 | Copia no controlada del código fuente del software | |
| 16 | Saturación de la operación del software | |
| 17 | Hacking/cracking | |
| 18 | Virus informáticos | |

| N° | Tipología de Amenaza | Tipo |
|---|---|---|
| 19 | Error humano en los cambios en el software (bugs) | |
| 20 | Incompatibilidad en la operación con otros software | |
| 21 | Corto circuito | **Amenazas a Activos Físicos (Equipos)** |
| 22 | Filtraciones de agua | |
| 23 | Filtración de polvo | |
| 24 | Corrosión de equipos | |
| 25 | Congelación de equipos | |
| 26 | Desconexión de equipos | |
| 27 | Saturación de humedad en ambientes | |
| 28 | Fallas del sistema de aire acondicionado | |
| 29 | Radiación electromagnética | |
| 30 | Robo de equipos o de sus componentes | |
| 31 | Incumplimiento del plan de mantenimiento | |
| 32 | Uso inadecuado de los equipos | |
| 33 | Desconfiguración del equipo | |
| 34 | Obsolescencia de los componentes del equipo | |
| 35 | Falla de servicios para las telecomunicaciones | **Amenazas a Servicios** |
| 36 | Degradación de servicios para las telecomunicaciones | |
| 37 | Falla de la provisión de energía eléctrica | |
| 38 | Incumplimiento de fechas por parte de proveedores | |
| 39 | Provisión de servicios defectuosos (personal) | |
| 40 | Provisión de recursos defectuosos (materiales) | |
| 41 | Falla en servicios de información provistos por clientes | |
| 42 | Contaminación del ambiente por gases | **Amenazas a Personal** |
| 43 | Uso de credenciales falsificadas | |
| 44 | Bloqueo del acceso al centro de trabajo | |
| 45 | Dificultad en el desplazamiento hacia el centro de trabajo | |
| 46 | Asaltos/secuestros | |
| 47 | Enfermedad | |
| 48 | Sismo | **Amenazas a Ubicaciones Físicas** |
| 49 | Inundación | |
| 50 | Hundimiento de suelos | |
| 51 | Incendio | |

| N° | Tipología de Amenaza | Tipo |
|---|---|---|
| 52 | Destrucción intencional de los ambientes (protestas) | |

### 7.2. Identificar Vulnerabilidades

En la Tabla N° 7 se expone un ejemplo de tipología de amenazas genéricas agrupadas por cada tipo de activo de información al cual podrían afectar.

**Tabla N° 7**: Nivel de Vulnerabilidades

| N° | Vulnerabilidad | Categoría |
|---|---|---|
| 1 | Mantenimiento insuficiente | **Hardware** |
| 2 | Falta de esquemas de reemplazo periódicos | |
| 3 | Susceptibilidad a la humedad, al polvo y a la suciedad | |
| 4 | Falta de control eficiente del cambio de configuración | |
| 5 | Susceptibilidad a variación de voltaje | |
| 6 | Susceptibilidad a variaciones de temperatura | |
| 7 | Almacenamiento no protegido | |
| 8 | Falta de cuidado al descartarlo | |
| 9 | Equipo desfasado por vigencia tecnológica | |
| 10 | Pruebas al software inexistentes o insuficientes | **Software** |
| 11 | Errores conocidos en el software | |
| 12 | No hacer "logout" cuando se sale de la estación de trabajo | |
| 13 | Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente | |
| 14 | Falta de evidencia de auditoria | |
| 15 | Asignación equivocada de derechos de acceso | |
| 16 | Software ampliamente distribuido | |
| 17 | Interfaz de usuario complicada | |
| 18 | Falta de documentación | |
| 19 | Seteo incorrecto de parámetros | |
| 20 | Fechas incorrectas | |
| 21 | Falta de mecanismos de identificación y autentificación como la autentificación de usuarios | |
| 22 | Tablas de claves no protegidas | |
| 23 | Mala administración de claves | |

| N° | Vulnerabilidad | Categoría |
|---|---|---|
| 24 | Habilitación de servicios innecesarios | |
| 25 | Software inmaduro o nuevo | |
| 26 | Especificaciones no claras o incompletas para los desarrolladores | |
| 27 | Falta de control de cambios eficaz | |
| 28 | Descarga y uso incontrolado de software | |
| 29 | Falta de copias de respaldo | |
| 30 | Falta de pruebas de envió o recepción de mensaje | **Red** |
| 31 | Líneas de comunicación no protegidas | |
| 32 | Tráfico delicado no protegido | |
| 33 | Mala estructura del cableado | |
| 34 | Falta de identificación y autentificación del destinatario | |
| 35 | Arquitectura de red insegura | |
| 36 | Transferencia de claves en claro | |
| 37 | Gestión inadecuada de la red (capacidad de recuperación del ruteo) | |
| 38 | Conexiones no protegidas de la red pública | |
| 39 | Ausencia del personal | **Personal** |
| 40 | Procedimientos inadecuados del reclutamiento | |
| 41 | Capacitación de seguridad insuficiente | |
| 42 | Uso incorrecto del software y hardware | |
| 43 | Falta de conciencia de seguridad | |
| 44 | Falta de mecanismos de monitoreo | |
| 45 | Trabajo no supervisado del personal externo o de limpieza | |
| 46 | Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería | |
| 47 | Uso inadecuado o negligente del control de acceso físico a edificios y ambientes | **Sitio** |
| 48 | Ubicaciones en una área susceptible a las inundaciones | |
| 49 | Red inestable de energía eléctrica | |
| 50 | Falta de protección física del edificio, puertas y ventanas | |
| 51 | Falta de un procedimiento formal para el registro y baja de usuarios | **Institución** |
| 52 | Falta de proceso formal para revisar el derecho de acceso (supervisión) | |

| N° | Vulnerabilidad | Categoría |
|---|---|---|
| 53 | Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros | |
| 54 | Falta de auditorías regulares (supervisión) | |
| 55 | Falta de informes de fallas registradas en los registros del administrador y del operador | |
| 56 | Respuesta inadecuada del mantenimiento del servicio | |
| 57 | Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio | |
| 58 | Falta de procedimiento de control de cambios | |
| 59 | Falta de procedimiento formal para el control de la documentación de la institución | |
| 60 | Falta de proceso formal para autorización de información pública disponible | |
| 61 | Falta de asignación apropiada de responsabilidades de seguridad en la información | |
| 62 | Falta de planes de continuidad | |
| 63 | Falta de una política de uso de correos electrónicos | |
| 64 | Falta de procedimientos para introducir software en sistemas operativos | |
| 65 | Faltas de registro en los historiales del administrador y del operador | |
| 66 | Falta de procedimientos para manejo de la información clasificada | |
| 67 | Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos | |
| 68 | Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados) | |
| 69 | Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información | |
| 70 | Falta de política formal sobre el uso de computadoras portátiles | |
| 71 | Falta de control de activos que se encuentran fuera del local | |
| 72 | Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada" | |
| 73 | Falta de autorización al acceso a las instalaciones de procesamiento de la información | |
| 74 | Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad | |
| 75 | Falta de revisiones regulares de la gestión | |
| 76 | Falta de procedimientos para reportar debilidades en la seguridad | |
| 77 | Otras vulnerabilidades que se indiquen en los talleres | **Otros** |

### 7.3. Identificar Controles

En esta etapa se deberá realizar la identificación de los controles existentes, su estado de implementación y utilización. Asimismo, si es posible también se deberán identificar los controles planificados.

Para cada uno de los controles se deben definir la descripción del control.

### 7.4. Evaluación del Criterio CID

El Equipo de Trabajo, para poder determinar como la amenaza y vulnerabilidad afecta la Confidencialidad (C), Integridad (I) y Disponibilidad (D) del activo, evaluará cada uno de los criterios CID. Se tomarán los valores según las siguientes tablas:

#### a) Tabla de Valorización de Confidencialidad

**Tabla N° 8:** Valorización de Confidencialidad

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **3** | **Alta** | Es la información o recurso que deberá ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas. | La divulgación no autorizada produce:<br>- Pérdida de la ventaja competitiva.<br>- Uso malicioso en contra de la SUNAT.<br>- Pérdidas financieras que no pueden ser absorbidas por la SUNAT.<br>- Demandas legales que dañan la imagen y confianza pública de la SUNAT. |
| **2** | **Media** | Es la información que deberá ser divulgada sólo al personal de las áreas que la manejan y modificada sólo por personas autorizadas e individualizadas. | La divulgación no autorizada produce:<br>- Uso malicioso en contra de la imagen o situaciones puntuales.<br>- Pérdidas financieras que pueden ser absorbidas por la SUNAT.<br>- No se producen demandas legales. |

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **1** | **Baja** | Es la información que podrá ser divulgada a público general, pero que sólo puede ser modificada por personas autorizadas. | La divulgación no autorizada no representa perjuicio para la SUNAT. |

### b) Tabla de Valorización de Integridad

**Tabla N° 9:** Valorización de Integridad

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **3** | **Alta** | Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de gran magnitud. | La falta de integridad produce daños de gran magnitud los que se pueden expresar como:<br>- Pérdidas económicas (pérdida, incumplimiento de metas).<br>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable).<br>- Daño de la imagen de la SUNAT (daño a nivel nacional e internacional que no se puede reparar en el corto plazo).<br>- Pérdida de la confianza de los usuarios. |
| **2** | **Media** | Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de mediana magnitud. | La falta de integridad produce daños de mediana magnitud los que se pueden expresar como:<br>- Pérdidas económicas (menor eficiencia, incumplimiento de metas en menor escala).<br>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable).<br>- Daño de la imagen de la SUNAT (daño a nivel nacional, se puede reparar en el corto plazo).<br>- No se pierde la confianza de los usuarios. |

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **1** | **Baja** | Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provocará daños de pequeña magnitud. | La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como:<br>- Pérdidas económicas (no impacta en la eficiencia, se cumplen las metas).<br>- Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable).<br>- Daño de la imagen de la SUNAT (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente).<br>- No se pierde la confianza de los usuarios. |

### c) Tabla de Valorización de Disponibilidad

**Tabla N° 10:** Valorización de Disponibilidad

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **3** | **Alta** | Es información o activo indispensable para la continuidad de la SUNAT.<br>El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos. | La falta de disponibilidad por períodos prolongados produce:<br>- Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio.<br>- Perjuicios legales que afectan la imagen de la SUNAT.<br>- Perjuicios económicos que no pueden ser absorbidos por la SUNAT.<br>- Problemas sindicales. |

| Valor | Clasificación | Definición | Consecuencia |
|---|---|---|---|
| **2** | **Media** | La disponibilidad de la información es necesaria para la continuidad de la SUNAT, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable.<br>El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos. | La falta de disponibilidad produce:<br>- Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo.<br>- Perjuicios legales que no comprometen la imagen de la SUNAT.<br>- Perjuicios económicos que pueden ser absorbidos por la SUNAT.<br>- No hay problemas sindicales. |
| **1** | **Baja** | Es información o activos de apoyo o secundarios para la SUNAT.<br>La información se encuentra duplicada en varias fuentes.<br>Si no está disponible no comprometerá procesos operativos importantes. | La falta de disponibilidad produce:<br>- Que los niveles de servicio acordados para los procesos operativos importantes, no se vean afectados.<br>- Problemas administrativos y operativos no significativos.<br>- Perjuicios económicos que no son significativos.<br>- No hay perjuicios legales.<br>- No hay problemas sindicales. |

### 7.5. Valor CID

El Equipo de Trabajo calcula el valor CID de acuerdo a la siguiente tabla:

#### a) Tabla de Valorización

**Tabla N° 11:** Valor CID

| ASPECTO DE SEGURIDAD AFECTADO POR EL RIESGO | | | VALOR CID |
|---|---|---|---|
| C | I | D | |
| 1 | 1 | 1 | No Significativo |
| 1 | 1 | 2 | Bajo |
| 1 | 1 | 3 | Alto |
| 1 | 2 | 1 | Bajo |

| | | | |
|---|---|---|---|
| 1 | 2 | 2 | Mediano |
| 1 | 2 | 3 | Alto |
| 1 | 3 | 1 | Alto |
| 1 | 3 | 2 | Alto |
| 1 | 3 | 3 | Extremo |
| 2 | 1 | 1 | Bajo |
| 2 | 1 | 2 | Mediano |
| 2 | 1 | 3 | Alto |
| 2 | 2 | 1 | Mediano |
| 2 | 2 | 2 | Mediano |
| 2 | 2 | 3 | Alto |
| 2 | 3 | 1 | Alto |
| 2 | 3 | 2 | Alto |
| 2 | 3 | 3 | Extremo |
| 3 | 1 | 1 | Alto |
| 3 | 1 | 2 | Alto |
| 3 | 1 | 3 | Extremo |
| 3 | 2 | 1 | Alto |
| 3 | 2 | 2 | Alto |
| 3 | 2 | 3 | Extremo |
| 3 | 3 | 1 | Extremo |
| 3 | 3 | 2 | Extremo |
| 3 | 3 | 3 | Extremo |

## 7.6. Impacto

El Equipo de Trabajo determinará el impacto de acuerdo a la siguiente tabla.

### a) Tabla de Valorización del Impacto del Riesgo

**Tabla N° 12:** Valorización del Impacto del Riesgo

| Nivel | Descripción | Impacto |
|---|---|---|
| **5** | **Extremo** | Impacta en forma severa en la SUNAT al punto de comprometer la confidencialidad o integridad de información crítica y/o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la SUNAT y su efecto repercute en todo el personal involucrado. |
| **4** | **Alto** | Impacta en forma grave a un área o servicio específico de la SUNAT, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro de la SUNAT. |
| **3** | **Mediano** | El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo. |
| **2** | **Bajo** | El impacto es leve y se puede prescindir del mismo en un tiempo limitado. |
| **1** | **No Significativo** | No representa un impacto importante para la SUNAT. |

### 7.7. Estimar la Probabilidad de Ocurrencia del Riesgo

El Equipo de Trabajo determinará la probabilidad de ocurrencia de acuerdo a la siguiente tabla:

**Tabla N° 13:** Probabilidad de Ocurrencia del Riesgo

| Valor | Clasificación | Definición |
|---|---|---|
| **1** | **Muy Baja** | El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año. |
| **2** | **Baja** | Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año. |

| | | |
|---|---|---|
| **3** | **Moderada** | Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año. |
| **4** | **Alta** | Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes. |
| **5** | **Muy Alta** | El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más. |

## 8. FASE 3: EVALUACIÓN DEL RIESGO

Luego de completado el análisis de riesgos, se procederá a la evaluación del riesgo, que utilizará como información de entrada, la probabilidad de ocurrencia del riesgo. Se comparará los resultados del análisis de riesgo con los criterios de riesgos establecidos. (Ver formato SGSI-ME-01.FO-02 Matriz de Riesgos de Seguridad de la Información).

### 8.1. Nivel de Riesgo

El riesgo efectivo es la medida del daño probable causado por una amenaza, que se materializa en un activo. Con el valor obtenido del producto del Impacto por la Probabilidad el Equipo de Trabajo obtendrá el Nivel de Riesgo de acuerdo a la siguiente tabla:

#### a) Tabla de Valorización del Riesgo

**Tabla N° 14:** Valorización de Riesgos

| TABLA DE VALORIZACIÓN DE RIESGOS | | | | | |
|---|---|---|---|---|---|
| **Impacto** | | **Probabilidad** | | **Nivel de Riesgo** | |
| Extremo | 5 | Muy Alta | 5 | Extremo | 25 |
| Alto | 4 | Muy Alta | 5 | Extremo | 20 |
| Mediano | 3 | Muy Alta | 5 | Extremo | 15 |
| Bajo | 2 | Muy Alta | 5 | Alto | 10 |
| No Significativo | 1 | Muy Alta | 5 | Mediano | 5 |
| Extremo | 5 | Alta | 4 | Extremo | 20 |
| Alto | 4 | Alta | 4 | Extremo | 16 |

| | | | | | |
|---|---|---|---|---|---|
| Mediano | 3 | Alta | 4 | Alto | 12 |
| Bajo | 2 | Alta | 4 | Mediano | 8 |
| No Significativo | 1 | Alta | 4 | Bajo | 4 |
| Extremo | 5 | Moderada | 3 | Extremo | 15 |
| Alto | 4 | Moderada | 3 | Alto | 12 |
| Mediano | 3 | Moderada | 3 | Alto | 9 |
| Bajo | 2 | Moderada | 3 | Mediano | 6 |
| No Significativo | 1 | Moderada | 3 | Bajo | 3 |
| Extremo | 5 | Baja | 2 | Alto | 10 |
| Alto | 4 | Baja | 2 | Mediano | 8 |
| Mediano | 3 | Baja | 2 | Mediano | 6 |
| Bajo | 2 | Baja | 2 | Bajo | 4 |
| No Significativo | 1 | Baja | 2 | No Significativo | 2 |
| Extremo | 5 | Muy Baja | 1 | Mediano | 5 |
| Alto | 4 | Muy Baja | 1 | Bajo | 4 |
| Mediano | 3 | Muy Baja | 1 | Bajo | 3 |
| Bajo | 2 | Muy Baja | 1 | No significativo | 2 |
| No Significativo | 1 | Muy Baja | 1 | No significativo | 1 |

Los riesgos serán clasificados de acuerdo a niveles, según su grado de exposición, lo cual realizará el Equipo de Trabajo según la siguiente tabla:

**b) Tabla de Nivel de Riesgo**

**Tabla N° 15:** Nivel de Riesgo

| Rango de Riesgo | Nivel de Riesgo | Descripción de las Consecuencias |
|---|---|---|
| **De 15 a 25** | **Extremo** | Puede afectar seriamente a la SUNAT, en términos de paralización de las operaciones. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable. |
| **De 9 a 12** | **Alto** | Puede afectar los niveles de operación y servicio de la SUNAT, incumplimiento de metas, y divulgación no autorizada de información fuera de la SUNAT. Requiere una acción correctiva sujeta a la discreción de los Propietarios del Riesgo en términos de plazos y compromisos. |

| | | |
|---|---|---|
| **De 5 a 8** | **Mediano** | Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas de la SUNAT. La divulgación no autorizada no representa perjuicio importante para la SUNAT. Su aceptación está sujeta a la revisión de los Propietarios del Riesgo. |
| **De 3 a 4** | **Bajo** | No causa un efecto considerable en la SUNAT. Usualmente son aceptados sin revisión. |
| **De 1 a 2** | **No Significativo** | El efecto para la SUNAT es insignificante. Usualmente no se les considera para la gestión de riesgos. |

### 8.2. Nombre del Riesgo

El Oficial de Seguridad de la Información asignará un nombre para el riesgo que sirva para identificarlo respecto de otros.

A continuación, se muestra un ejemplo de cómo se construye la narración del riesgo o escenario de riesgo.

| Elemento | Ejemplo de narración |
|---|---|
| Activo de Información | *Archivos de configuración lógica de switches y router* |
| Amenaza a la Confidencialidad | *Acceso no autorizado a los archivos de configuración lógica de switches y router, por parte de atacantes internos y/o atacantes externos.* |
| Vulnerabilidad | *No se guardan los archivos de configuración lógica de switches y router con algún de software de encriptación en los discos duros de los administradores.* |
| Impacto | *Impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques.* |
| Escenario de Riesgo | ***Si** ocurre un acceso no autorizado a los archivos de configuración lógica de switches y router, **entonces** puede causar un impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques **debido** a que no se guardan los archivos de configuración lógica de switches y router con algún de software de encriptación en los discos duros de los administradores.* |

### 8.3. Código del Riesgo

El Oficial de Seguridad de la Información asignará un código para el riesgo que sirva para identificarlo respecto de otros.

## 9. FASE 4: TRATAMIENTO DEL RIESGO

En esta etapa de tratamiento del riesgo, se deberán considerar las mejoras a implementar, ya sea mediante la inclusión de controles adicionales o a través de la mejora de controles existentes. La implementación de estas mejoras se realizará sobre los riesgos seleccionados en la fase anterior.

### 9.1. Propuesta de Tratamiento del Riesgo

Una vez efectuado el análisis y la evaluación del riesgo, se debe decidir qué acciones se han de tomar con los activos que están sujetos a riesgos reales y significativos para la entidad. Para ello se puede aplicar una de las siguientes estrategias (ver formato SGSI-ME-01.FO-03 Plan de Tratamiento de Riesgos).

**Tabla N° 16**: Opciones de Tratamiento del Riesgo

| Medida Frente al Riesgo | |
|---|---|
| Aceptar | Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas. |
| Reducir | Reducir la probabilidad o el impacto de ocurrencia mediante la implementación de controles de seguridad de la información. Se utiliza cuando al implementar el control trae beneficios mayores a la inversión de su implementación. |
| Evitar | Eliminar la fuente del proceso que genera la amenaza. Se utiliza cuando el nivel de riesgo es alto y la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la entidad, de modo que puede ser retirada funcionalmente. |
| Transferir | Transferir el impacto del riesgo a terceros (empresas aseguradoras o proveedores de servicio). Se utiliza cuando no se puede reducir la probabilidad de ocurrencia de un riesgo pero el impacto es inminente. |

### 9.2. Plan de Tratamiento del Riesgo

Producto de esta selección se genera el SGSI-ME-01.FO-03 Plan de Tratamiento de Riesgos. En el cual se deben colocar los siguientes ítems:

Código del Riesgo, Nombre del Riesgo, Nivel de Riesgo, Nombre del Activo, Amenaza, Vulnerabilidad, los cuales se obtienen de la Matriz de Riesgos de Seguridad de la Información SGSI-ME-01.FO-02.

Los siguientes ítems, se llenarán de la siguiente manera:

a) **Tratamiento del Riesgo**: El Oficial de Seguridad de la Información colocará la opción del tratamiento de riesgos que corresponda de acuerdo a la Tabla 16: Opciones de Tratamiento del Riesgo, descritas en el punto 8.1.
b) **El Control Referencia ISO 27001:** El Oficial de Seguridad de la Información selecciona los controles que se implementarán, los mismos que se encuentran en el anexo A de la norma.
c) **Actividad a Realizar para la Implementación del Control:** Se define las actividades específicas que se realizarán para implementar el control.
d) **Riesgo Residual:** Es el nivel de riesgo que se espera obtener luego de la aplicación de controles, de acuerdo al nivel de aceptación de riesgo que se ha definido dentro de la SUNAT, los cuales son: **Medio**, **Bajo y No Significativo,** es decir, aquellos que no ocasionan un impacto significativo sobre la seguridad de la información.

   El Oficial de Seguridad de la Información incluirá el riesgo luego de aplicar controles, teniendo en cuenta lo siguiente:

   - **Impacto**

     El Oficial de Seguridad de la Información incluirá el impacto identificado (columna “IMPACTO”) de la Matriz de Riesgos de Seguridad de la Información SGSI-PR-02.FO-02
   - **P (X)**

     El Oficial de Seguridad de la Información incluirá la probabilidad de ocurrencia esperada luego de aplicar controles, de acuerdo a la Tabla de Valorización de la Probabilidad de Ocurrencia (la probabilidad esperada permite que el nivel de riesgo este dentro del nivel de

aceptación de riesgos definidos por la institución, el cual como mínimo deber ser medio.

e) **Responsable de la Implementación:** El Oficial de Seguridad de la Información en coordinación con el Propietario del Riesgo colocará el nombre y apellido del responsable de la implementación del control.

f) **Área del Responsable de la Implementación**: El Oficial de Seguridad de la Información colocará el Área a la que pertenece el responsable de la implementación.

g) **Fecha de Inicio de la Implementación:** El Responsable de la Implementación colocará la fecha comprometida para el inicio de la implementación.

h) **Fecha Fin de la Implementación:** El Responsable de la Implementación colocará la fecha comprometida para la finalización de la implementación.

i) **Estado:** El Oficial de Seguridad de la Información deberá especificar el estado de la implementación del plan de acuerdo a la Tabla de Estado de Implementación.

**Tabla N° 17**: Estado de Implementación

| Estado |
|---|
| Pendiente |
| En Proceso |
| Concluida |

Los riesgos y la efectividad de las medidas de control serán revisadas por el Propietario del Riesgo para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos, ya que pocos riesgos permanecen estáticos, esto se realizará en forma anual, para tal efecto será asistido por el Oficial de la Seguridad de la Información.

Para el caso del tratamiento que busca reducir el riesgo usado en el Plan de Tratamiento del Riesgo, los propietarios de los riesgos aceptan los controles propuestos y los riesgos residuales (riesgos que surgen después de la aplicación de los controles planificados) mediante la firma del formato SGSI-

ME-01.FO-05 Acta de Aprobación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

### 9.3. Declaración de Aplicabilidad

El Oficial de Seguridad de la Información deberá desarrollar la Declaración de Aplicabilidad (SoA), la cual se plasmará en el formato SGSI-ME-01.FO-04 Declaración de Aplicabilidad (SoA).

## 10. REGISTROS Y ANEXOS

a) SGSI-ME-01.FO-01 Inventario de Activos de Información
b) SGSI-ME-01.FO-02 Matriz de Riesgos de Seguridad de la Información
c) SGSI-ME-01.FO-03 Plan de Tratamiento de Riesgos
d) SGSI-ME-01.FO-04 Declaración de Aplicabilidad (SoA)
e) SGSI-ME-01.FO-05 Acta de Aprobación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

## 11. CONTROL DE CAMBIOS

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 01 | 25/01/2019 | Oficial de Seguridad de Información |