METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

SGSI-ME-01

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 Nacional Adjunta de Administración y Finanzas N° 000073-2021-SUNAT/800000, que aprueba la Metodología de Administración de Riesgos Institucional (MARI), Versión 3.

3. DEFINICIONES Y ABREVIATURAS

3.1. **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, equipamiento informático, edificios, personas, etc.) que tenga valor para la organización.

3.2. **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

3.3. **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones sobre el tratamiento de riesgos.

3.4. **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.

3.5. **Control:** Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto.

3.6. **Criterio de Aceptación del Riesgo:** Condición, establecida formalmente, que ayuda a determinar el nivel de riesgos con los que puede convivir la entidad.

3.7. **Custodio del Activo de Información:** Persona o entidad que tiene la responsabilidad de mantener un adecuado nivel de protección de los activos

de información en base a las especificaciones coordinadas con el Propietario del Activo de Información.

3.8. **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.

3.9. **Equipo de Gestión de Riesgos:** Es el conjunto multidisciplinario de especialistas de la institución, que se conforma previo al inicio de las actividades de gestión de riesgos y con la finalidad de llevar a cabo dicha gestión. Entre sus miembros se debe considerar al Oficial de Seguridad de la Información, al Custodio del Activo de información, al Propietario del Activo de Información, al Propietario del Riesgo, al personal de la Gerencia de Seguridad de la Información y del proceso del cual se quiere evaluar los riesgos, entre otros que se consideren necesarios. Los miembros indicados pueden designar a sus representantes.

3.10. **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.

3.11. **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

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

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

3.14. **Incidente de Seguridad de la Información:** Un solo evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

3.15. **Información:** Conjunto de datos contenidos en documentos físicos (papel, microfichas, libros, etc.), medios magnéticos (cintas, discos, etc.), medios ópticos (CD, DVD, etc.) y medios electrónicos (USB, disco duro externo, etc.), que poseen valor para la entidad.

3.16. Integridad: Propiedad de la información relativa a su exactitud y completitud.

3.17. Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

3.18. Nivel de Riesgo: Grado de que un riesgo se materialice causando un impacto.

3.19. Oficial de Seguridad de la Información: Es el responsable operativo de la implementación y mantenimiento del SGSI. Es designado mediante resolución de la superintendencia nacional.

3.20. Probabilidad de Ocurrencia del Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad.

3.21. Propietario del Activo de Información: Persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, recepción, desarrollo, mantenimiento, uso y seguridad de los activos. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

3.22. Propietario del Riesgo: Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo.

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

3.24. Riesgo de Seguridad de la Información: Potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, cause daños a una organización.

3.25. Riesgo Efectivo: Es el nivel de riesgo que se posee actualmente.

3.26. Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo.

3.27. Tratamiento de Riesgos: Proceso para modificar el riesgo.

3.28. Usuario de la Información: Persona autorizada a utilizar un sistema de información determinado, bajo un nivel de acceso preestablecido. Para efectos del presente documento, se refiere a los colaboradores, personal de modalidades formativas y terceros vinculados con la SUNAT.

3.29. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

ABREVIATURAS

- **EGR:** Equipo de Gestión de Riesgos.
- **GSI:** Gerencia de Seguridad de la Información.
- **OFSI:** Oficial de Seguridad de la Información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **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 y/o activos de información, se podrá iniciar un ciclo de gestión de riesgos no planificado.

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 1: Capacitación y Consideraciones Previas
	Fase 2: Elaboración del Inventario de Activos
	Fase 3: Análisis de Riesgos
	Fase 4: Evaluación de Riesgos
	Fase 5: Tratamiento de Riesgos

Dichas fases se realizarán mediante sesiones con el EGR, y se llevarán a cabo de acuerdo con lo planificado en el Plan de Trabajo del SGSI.

4.1. Fase 1: Capacitación y Consideraciones Previas

En esta etapa, el OFSI junto con el personal de la GSI realizarán las charlas de capacitación requeridas a todos los involucrados, en caso corresponda.

Asimismo, en el inicio de esta fase el EGR debe verificar el riesgo residual sobre los activos considerando los controles de seguridad definidos e implementados en la gestión de riesgos previa, sin perjuicio de que los propietarios consideren realizar una verificación continua una vez implementados dichos controles.

Se deben tener en cuenta los siguientes criterios básicos que serán utilizados en el proceso de gestión de riesgos:

4.1.1. Criterio de Tasación de Activos

Se han definido tres niveles de activos: **Bajo, Medio y Alto**. Sólo aquellos activos que en la fase 2, Elaboración del Inventario de Activos, hayan sido catalogados con valor alto formarán parte de los activos que pasan a la fase 3, Análisis de Riesgos. En el numeral 4.2.3 se definen los criterios establecidos para la valorización de los activos.

4.1.2. Criterio de Aceptación del Riesgo

La SUNAT reconoce cinco niveles de riesgos: **Extremo, Alto**, **Medio**, **Bajo y No Significativo**. Asimismo, considera que el nivel de riesgo aceptado corresponde a aquellos riesgos 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 5, Tratamiento de Riesgos, salvo en los casos que se detallan a continuación:

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.

4.2. Fase 2: Elaboración del Inventario de Activos

Luego de la Capacitación y Consideraciones Previas (fase 1), el proceso de gestión de riesgos deberá continuar con la elaboración del inventario de activos de información de los procesos considerados dentro del alcance del SGSI. Los activos de información identificados.

4.2.1. 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.

4.2.2. Identificación de Activos

Para cada proceso del alcance, se deberá preparar el inventario 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

CATEGORÍA	TIPO DE ACTIVO
Físicos	Equipo de procesamiento
	Equipo de comunicaciones
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicaciones
	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 subproceso, puede ser soportado por una o más unidades organizacionales.

Tabla N° 4: Frecuencia de Uso

FRECUENCIA DE USO
Diario
Semanal
Quincenal
Mensual
Anual
Eventual

4.2.3. Valorización de Activos

El EGR colocará la valorización del activo de información identificado, la cual se define 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 institución.
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 institución.
Bajo	Activos secundarios que constituyen información para la toma de decisiones de un área específica. No compromete ningún proceso crítico de la SUNAT.

Finalmente, tomando en cuenta, además, lo definido en el numeral 4.1.1, los activos de información valorizados como altos, pasan al análisis de riesgos (fase 3).

4.3. Fase 3: Análisis de Riesgos

Completado el inventario de activos de información (Fase 2), se deberán identificar las posibles amenazas a las que están expuestos los activos valorizados como altos en la etapa anterior, así como también las vulnerabilidades y controles existentes (Ver formato Matriz de Riesgos de Seguridad de la Información/ SGSI-ME-01.FO-02).

4.3.1. Identificar Amenazas

Para cada uno de los activos de información seleccionados, 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°	AMENAZA	TIPO DE ACTIVO
1	Acceso no autorizado a la información	**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 extralaboral 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)	**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	
19	Error humano en los cambios en el software (bugs)	
20	Incompatibilidad en la operación con otro software	
21	Corto circuito	**Activos Físicos (Equipos)**
22	Filtraciones de agua	
23	Filtración de polvo	
24	Corrosión de equipos	

N°	AMENAZA	TIPO DE ACTIVO
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	**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	**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	**Ubicaciones Físicas**
49	Inundación	
50	Hundimiento de suelos	
51	Incendio	
52	Destrucción intencional de los ambientes (protestas)	

4.3.2. Identificar Vulnerabilidades

En la Tabla N° 7 se expone un ejemplo de la tipología de vulnerabilidades genéricas agrupadas por cada tipo de activo de información:

Tabla N° 7: Nivel de Vulnerabilidades

N°	VULNERABILIDAD	TIPO DE ACTIVO
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	
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	

N°	VULNERABILIDAD	TIPO DE ACTIVO
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 áreas susceptibles 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)	
53	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o	
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	

N°	VULNERABILIDAD	TIPO DE ACTIVO
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 "pantallas y escritorios limpios"	
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**

4.3.3. 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 debe definir la descripción del control.

4.3.4. Evaluación del Criterio CID

El EGR, para poder determinar como la amenaza y vulnerabilidad afectan la Confidencialidad (C), Integridad (I) y Disponibilidad (D) del activo, evaluará cada uno de dichos criterios tomando en cuenta los valores según las siguientes tablas:

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: - Pérdida de la ventaja competitiva. - Uso malicioso en contra de la SUNAT. - Pérdidas financieras que no pueden ser absorbidas por la SUNAT. - 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: - Uso malicioso en contra de la imagen o situaciones puntuales. - Pérdidas financieras que pueden ser absorbidas por la SUNAT. - No se producen demandas legales.
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.

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.	- Pérdidas económicas (pérdida, incumplimiento de metas). - Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). - Daño de la imagen de la SUNAT (daño a nivel nacional e internacional que no se puede reparar en el corto plazo).

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
			– 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.	– Pérdidas económicas (menor eficiencia, incumplimiento de metas en menor escala). – Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). – Daño de la imagen de la SUNAT (daño a nivel nacional, se puede reparar en el corto plazo). – No se pierde la confianza de los usuarios.
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.	– Pérdidas económicas (no impacta en la eficiencia, se cumplen las metas). – Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo, pero este es manejable). – Daño de la imagen de la SUNAT (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente). – No se pierde la confianza de los usuarios.

Tabla N° 10: Valorización de Disponibilidad

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
3	**Alta**	Es información o activo indispensable para la continuidad de la SUNAT. 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: – Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. – Perjuicios legales que afectan la imagen de la SUNAT.

VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
			– Perjuicios económicos que no pueden ser absorbidos por la SUNAT. – Problemas sindicales.
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. 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: – Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. – Perjuicios legales que no comprometen la imagen de la SUNAT. – Perjuicios económicos que pueden ser absorbidos por la SUNAT. – No hay problemas sindicales.
1	**Baja**	Es información o activos de apoyo o secundarios para la SUNAT. La información se encuentra duplicada en varias fuentes. Si no está disponible no comprometerá procesos operativos importantes.	La falta de disponibilidad produce: – Que los niveles de servicio acordados para los procesos operativos importantes, no se vean afectados. – Problemas administrativos y operativos no significativos. – Perjuicios económicos que no son significativos. – No hay perjuicios legales. – No hay problemas sindicales.

4.3.5. Valor CID

El EGR calcula el valor CID de acuerdo con la siguiente tabla:

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

4.3.6. Impacto

El EGR determinará el impacto de acuerdo con la siguiente tabla:

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.

4.3.7. Estimar la Probabilidad de Ocurrencia del Riesgo

El EGR determinará la probabilidad de ocurrencia de acuerdo con la siguiente tabla:

Tabla N° 13: Probabilidad de Ocurrencia del Riesgo

VALOR	CLASIFICACIÓN	DEFINICIÓN
1	**Muy Baja**	El evento no ha ocurrido o ha ocurrido al menos 1 vez al año.
2	**Baja**	Si bien el evento puede ocurrir, el periodo entre uno y otro 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.

4.4. Fase 4: Evaluación de Riesgos

Luego de completado el análisis de riesgos, se procederá a la evaluación del riesgo.

4.4.1. Nivel de Riesgo

Con el valor obtenido del producto del Impacto por la Probabilidad, el EGR obtendrá el Nivel de Riesgo de acuerdo con la siguiente tabla:

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 con niveles, según su grado de exposición, lo cual realizará el EGR según la siguiente tabla:

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.

4.4.2. Nombre del Riesgo

El OFSI, o su representante, 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.

Tabla N° 16: Nombre del 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.*

4.4.3. Código del Riesgo

El OFSI, o su representante, asignará un código para el riesgo que sirva para identificarlo respecto de otros.

4.4.4. Identificación del Propietario del Riesgo

El EGR identificará, para cada riesgo evaluado, al Propietario del Riesgo.

4.5. Fase 5: Tratamiento de Riesgos

En esta etapa de tratamiento del riesgo, el EGR deberá 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.

4.5.1. 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:

Tabla N° 17: Opciones de Respuesta al 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.

4.5.2. Plan de Tratamiento del Riesgo

Producto de esta selección se registra el Plan de Tratamiento de Riesgos (SGSI-ME-01.FO-03), el cual contiene los siguientes ítems:

a) **Código del Riesgo:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
b) **Nombre del Riesgo:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
c) **Nivel de Riesgo:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
d) **Nombre del Activo:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
e) **Amenaza:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
f) **Vulnerabilidad:** Obtener el dato de la Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).
g) **Tratamiento del Riesgo**: Colocar la opción de tratamiento del riesgo escogida de acuerdo con la Tabla N° 17, Opciones de Respuesta al Riesgo, del punto 4.5.1.

h) **Control Referencia ISO 27001:** Seleccionar los controles que se implementarán, los mismos que se encuentran en el anexo A de la norma ISO 27001.

i) **Actividad a Realizar para la Implementación del Control:** Definir las actividades específicas que se realizarán para implementar el control.

j) **Riesgo Residual:** Incluir el riesgo que se espera obtener luego de aplicar controles, el cual tendría que estar en las categorías **Medio**, **Bajo y No Significativo**, es decir, aquellos que no ocasionan un impacto significativo sobre la seguridad de la información (ver Tabla N° 14, Valorización de Riesgos, numeral 4.4.1). Para calcular el riesgo residual se debe tener en cuenta lo siguiente:

- **Impacto:** Incluir el impacto identificado luego de aplicar controles, de acuerdo con la Tabla N° 12, Valorización del Impacto del Riesgo, del numeral 4.3.6.
- **P (X):** Incluir la probabilidad de ocurrencia esperada luego de aplicar controles, de acuerdo con la Tabla N° 13, Probabilidad de Ocurrencia del Riesgo, del numeral 4.3.7.

k) **Responsable de la Implementación:** Colocar el nombre y apellido del responsable de la implementación del control.

l) **Área del Responsable de la Implementación**: Colocar el área a la que pertenece el responsable de la implementación.

m) **Fecha de Inicio de la Implementación:** Colocar la fecha comprometida para el inicio de la implementación.

n) **Fecha Fin de la Implementación:** Colocar la fecha comprometida para la finalización de la implementación.

o) **Estado:** Especificar el estado de la implementación del plan de acuerdo con la Tabla de Estado de Implementación.

Tabla N° 18: 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 Acta de Aprobación del Plan de Tratamiento de Riesgos y los Riesgos Residuales (SGSI-ME-01.FO-05).

4.5.3. Declaración de Aplicabilidad

Finalmente, el OFSI junto con personal de la GSI, deberá desarrollar la Declaración de Aplicabilidad (SoA), la cual se plasmará en el formato Declaración de Aplicabilidad (SoA) (SGSI-ME-01.FO-04).

5. OPORTUNIDADES DE MEJORA

De forma paralela al proceso de gestión de riesgos, en cualquiera de sus fases, los miembros del EGR pueden identificar posibles oportunidades de mejora que permitan afinar, corregir y perfeccionar procesos evaluados, así como los procesos del SGSI con la finalidad de alcanzar o lograr los objetivos de la entidad en seguridad de la información, para lo cual, se seguirá lo definido en el Procedimiento de Mejora Continua del SGSI (SGSI-PR-05).

6. 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.

7. CONTROL DE CAMBIOS

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial del documento	01	25/01/2019	Oficial de Seguridad de Información
Inclusión de revisión de riesgo residual previo a la gestión de riesgos. Actualización de definiciones, fases y otros. Inclusión de la Gerencia de Seguridad de la Información	02	22/03/2023	Oficial de Seguridad de Información