electroperu la energía de los peruanos	**Instructivo de Trabajo:** **Gestión de riesgos de seguridad de la información, ciberseguridad y protección de privacidad**	
Código: S3.3.3.IT1	**Versión:** 1	**Fecha:** 19/02/2025

Elaborado por:	**Revisado por:**	**Aprobado por:**
Oficial de Seguridad y Confianza Digital	Subgerente de Tecnologías de la Información y Comunicaciones	Gerente General
Firmado digitalmente por: ALARCON TABOADA Luis Manuel FAU 20100027705 hard Motivo: Oficial de Seguridad y Confianza Digital Fecha: 19/02/2025 14:52:28-0500	Firmado digitalmente por: TAKIMOTO ALDAVE Julio Roberto FAU 20100027705 hard Motivo: Subgerente de TIC Fecha: 19/02/2025 17:05:51-0500	Firmado digitalmente por: RODRIGUEZ LUNA Anddy FAU 20100027705 hard Motivo: Gerente General Fecha: 19/02/2025 17:44:56-0500

1. PROCESO / PROCEDIMIENTO

El presente documento corresponde a: S3. Tecnología de Información y Comunicaciones / S3.3. Gestión de la Información / S3.3.3. Seguridad de la Información y Ciberseguridad.

2. ACTIVIDAD

Brindar pautas, orientación y soporte a la gestión de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad. Es aplicable y de cumplimiento para todas las personas que mantienen un vínculo laboral de forma temporal o permanente y bajo las diferentes modalidades de contratación o de formación (practicantes); incluyendo a las organizaciones externas (públicas y privadas) que tienen acceso a la información y activos digitales de ELECTROPERU S.A.

3. RESPONSABLES

- Subgerencia de Tecnologías de la Información
- Oficial de Seguridad y Confianza Digital
- Áreas usuarias

4. DETALLE DEL INSTRUCTIVO

En ELECTROPERU S.A.:

a. La gestión de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad es responsabilidad de todo el personal, así como también es parte de la gestión integral de riesgos y de las actividades de sus procesos.

b. Los riesgos de los activos de información del negocio son gestionados por los dueños y/o responsables de los procesos, los riesgos de los activos de información tecnológicos (IT) son gestionados por la Subgerencia de Tecnologías de la Información y los riesgos de los activos de información operacionales (OT) son gestionados por la Gerencia de Producción.

c. Los dueños y/o responsables de los riesgos tienen la capacidad y autoridad de poder gestionar el riesgo asignado en el proceso de identificación de este.

d. Los dueños y/o responsables de los controles son asignados para asegurar el diseño, implementación, operación y supervisión de las medidas de control.

e. Los principios de confidencialidad, integridad y disponibilidad de la información en base a buenas prácticas internacionales (controles) son enunciados en el Código de seguridad de la información, ciberseguridad y protección de la privacidad según Anexo A de la norma ISO/IEC 27001:2022.

4.1. METODOLOGIA

4.1.1. Análisis del contexto:

Luego de definir el alcance y el contexto donde se va a realizar la evaluación de los riesgos de seguridad de la información es necesario realizar un análisis del contexto interno y externo en base a los factores que pueden afectar al Sistema de Gestión de Seguridad de la Información.

4.1.2. Criterios de evaluación de riesgo:

En base a su impacto a los objetivos de la organización, los criterios pueden ser: De negocio, Jurídicos y normativos, Tecnologías en la Operación (OT), Tecnologías de información (IT), Financieros y/o fraude, Ambientales, seguridad y salud, entre otros. Se asume el apetito del riesgo consignado en el *"Manual de Gestión Integral de Riesgos"* de ELECTROPERU S.A.

4.1.3. Inventario de activos de información:

En coordinación con los dueños y/o responsables de procesos se elabora el inventario de activos de información para su valoración en base a la confidencialidad, integridad y disponibilidad de la información que tratan. Los activos de información deben ser tasados o valorados para priorizar la evaluación de sus riesgos de seguridad de la información, ciberseguridad y protección de la privacidad y en lo posible agruparlos. Para ello se utiliza la siguiente fórmula:

Valor del Activo = (Confidencialidad + Integridad + Disponibilidad) / 3

Confidencialidad:

- **Bajo (1):** La información asociada al activo es pública.
- **Medio (2):** La información asociada al activo es de uso interno, determinado personal puede acceder a ella, su divulgación podría afectar algunos procesos.
- **Alto (3):** La información asociada al activo es restringida. Sólo personal autorizado puede acceder a ella, su divulgación afectaría la imagen de la organización.
- **Extremo (4):** La información asociada al activo es confidencial y solo es accedida por Alta Gerencia, su divulgación sería catastrófica para la organización.

Integridad:

- **Bajo (1):** El activo puede tolerar una alteración menor de sus componentes, podría afectar una actividad menor del proceso.
- **Medio (2):** El activo puede tolerar una alteración media de sus componentes, podría afectar algunas actividades importantes del proceso.
- **Alto (3):** El activo no puede tolerar una alteración de sus componentes, podría afectar un proceso completo.
- **Extremo (4):** El activo no puede tolerar pérdida o alteración de sus componentes, podría afectar varios procesos completos.

Disponibilidad:

- **Bajo (1):** El activo no puede estar no disponible por mas de una semana, su carencia afectaría una actividad menor del proceso.
- **Medio (2):** El activo no puede estar no disponible por más de un día, su carencia afectaría una o más actividades del proceso.
- **Alto (3):** El activo no puede estar no disponible por más de dos horas, su carencia afectaría en la operación completa de un proceso.
- **Extremo (4):** El activo siempre debe estar disponible, pues su carencia afectaría la operación de varios procesos.

Valor del activo:

	Bajo	Medio	Alto	Extremo
Valores	De 1.0 a 1.49	De 1.50 a 2.49	De 2.50 a 3.49	De 3.50 a 4.00

4.1.4. Identificación de riesgos

Los riesgos y sus controles son identificados y registrados en los formatos respectivos según el nivel de valoración o tasación obtenido.

4.1.5. Análisis de riesgos:

Se define el nivel de riesgo utilizando la siguiente fórmula:

Nivel de Riesgo = Nivel de Probabilidad x Nivel de Impacto

Los niveles de probabilidad son:

a. Baja o rara (1):

- ✓ Probabilidad de ocurrencia baja o casi nula. (Podría ocurrir 1 o 2 veces al año)
- ✓ No existe recuerdo y/o evidencia histórica de haber ocurrido.
- ✓ Podría ocurrir sólo bajo circunstancias muy excepcionales.

b. Media o posible (2):

- ✓ Probabilidad de ocurrencia eventual (Podría ocurrir 3 o 4 veces al año)
- ✓ Eventos similares ocurren de manera esporádica.
- ✓ Podría ocurrir bajo ciertas circunstancias.

c. Alta o probable (3):

- ✓ Probabilidad de ocurrencia media o periódica. (mensual o quincenal)
- ✓ Eventos similares ocurren con regular frecuencia.
- ✓ Probablemente ocurrirá bajo múltiples circunstancias.

d. Extrema o casi seguro (4):

- ✓ Probabilidad de ocurrencia elevada o muy frecuente. (semanal o diaria)
- ✓ Eventos similares ocurren con alta frecuencia.
- ✓ Se espera que ocurra en la mayoría de las circunstancias.

Los niveles de impacto (Negativo) son:

a. Bajo o menor (1):

- ✓ No se impacta la rentabilidad, la operatividad, el cumplimiento legal y/o imagen de la organización.
- ✓ Confidencialidad: La información expuesta no hace daño a la organización.
- ✓ Integridad: La información alterada no hace daño a la organización.

- ✓ Disponibilidad: La falta de acceso a la información no hace daño a la organización.

b. Medio o moderado (2):

- ✓ Se impacta seriamente la rentabilidad, la operatividad, el cumplimiento legal y/o la imagen de la organización.
- ✓ Confidencialidad: La información expuesta hace daño medio a la organización.
- ✓ Integridad: La información alterada hace daño medio a la organización.
- ✓ Disponibilidad: La falta de acceso a la información hace daño medio a la organización.

c. Alto o significativo (3):

- ✓ Se impacta drásticamente la rentabilidad, la operatividad, el cumplimiento, legal y/o la imagen de la organización.
- ✓ Confidencialidad: La información expuesta hace alto daño a la organización.
- ✓ Integridad: La información alterada hace alto daño a la organización.
- ✓ Disponibilidad: La falta de acceso a la información hace alto daño a la organización.

d. Extremo o grave (4):

- ✓ Se impacta irreversiblemente la rentabilidad, la operatividad, el cumplimiento legal y/o la imagen de la organización.
- ✓ Confidencialidad: La información expuesta hace daño extremo a la organización.
- ✓ Integridad: La información alterada hace daño extremo a la organización.
- ✓ Disponibilidad: La falta de acceso a la información hace daño extremo a la organización.

Los niveles de impacto (Positivo) son:

a. Bajo o poco beneficioso (1): La oportunidad tiene poco impacto positivo a la rentabilidad, la operatividad, el cumplimiento legal y/o imagen de la organización.

b. Medio o medianamente beneficioso (2): La oportunidad tiene moderado impacto positivo a la rentabilidad, la operatividad, el cumplimiento legal y/o imagen de la organización.

c. Alto o beneficioso (3): La oportunidad tiene alto impacto positivo a la rentabilidad, la operatividad, el cumplimiento legal y/o imagen de la organización.

d. **Extremo o muy beneficioso (4):** La oportunidad tiene muy alto impacto positivo a la rentabilidad, la operatividad, el cumplimiento legal y/o imagen de la organización.

El Nivel de riesgo puede ser:

	Bajo o raro	Moderado o posible	Alto o probable	Extremo o casi seguro
Valores	De 1 a 2.99	De 3 a 5.99	De 6 a 11.99	De 12 a 16

4.1.6. Valoración de riesgos:

Para riesgos con impacto negativo:

a. **Bajo o raro (1 a 2.99):** Se administra con procedimientos rutinarios y se controla con seguimiento. No requiere aprobación de presupuesto específico.
b. **Moderado o posible (3 a 5.99):** Se administrada con procedimientos de control con atención periódica y seguimiento programado.
c. **Alto o probable (6 a 11.99):** Requiere atención prioritaria y planes de tratamiento.
d. **Extremo o casi seguro (12 a 16):** Se requiere acción inmediata y planes de tratamiento con un presupuesto aprobado.

Para riesgos con impacto positivo:

e. **Bajo o raro (1 a 2.99):** No es necesario tratar la oportunidad, solo se monitorea.
f. **Moderado o posible (3 a 5.99):** Evaluar si se necesita tratar la oportunidad o aplicar acciones en base al beneficio a obtener.
g. **Alto o probable (6 a 11.99):** Se requiere atención prioritaria a través de planes de tratamiento.
h. **Extremo o casi seguro (12 a 16):** Se requiere acción inmediata y planes de tratamiento con un presupuesto aprobado.

4.1.7. Tratamiento de riesgos:

El nivel de riesgo obtenido define la prioridad de atención de este, tomando en cuenta la disponibilidad de recursos de la empresa:

NIVEL DE RIESGO	PRIORIDAD DE ATENCIÓN
Bajo o raro	Se acepta el riesgo
Moderado o posible	Se acepta el riesgo
Alto o probable	Mediano o corto plazo
Extremo o casi seguro	Corto plazo o inmediato

Luego de determinar alguna de las siguientes estrategias de tratamiento para el riesgo se establece las acciones para su implementación:

a. **Evitar:** Comprende dejar de realizar la actividad ligada al riesgo pues el beneficio de implementar un control es menor al costo del riesgo inherente y sus posibles consecuencias.
b. **Reducir o mitigar:** Comprende establecer controles para disminuir la probabilidad y el impacto, pues el beneficio de implementar un control es mayor al costo del riesgo inherente y la empresa se encuentra en la capacidad de realizar el tratamiento del riesgo. (Considerar el Anexo A del estándar internacional ISO/IEC 27001:2022 y la matriz de la Declaración de Aplicabilidad - SoA).
c. **Transferir o compartir:** Comprende compartir a un tercero la administración del riesgo o enfrentar los impactos originados, pues el beneficio de implementar un control es mayor al costo del riesgo inherente y un tercero tiene mejores condiciones o capacidad para realizar el tratamiento del riesgo.
d. **Explotar:** Comprende obtener beneficio de la situación (oportunidad).
e. **Aceptar o asumir:** Comprende conservar el riesgo, pues no se tiene la necesidad o capacidad de tratarlo y llevarlo a un nivel aceptable o el costo de tratar el riesgo se estima como mayor a la pérdida o impacto económico generado por su ocurrencia.

5. CONTROL DE MODIFICACIONES

Versión	Descripción del(los) Cambio(s)
1.0	Creación del documento