GUÍA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

ELECTROPERU S.A.

FECHA	RESPONSABLE	FIRMA
	Elaborado por: Oficial de Seguridad de la Información	
	Revisado por: Comité de Gobierno Digital	
	Aprobado por: Gerencia General	

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
01	Noviembre - 2019	Nuevo

I. FINALIDAD

Definir los componentes para implementar, operar, monitorear, mantener y mejorar el Sistema de Gestión de Seguridad de la Información de ELECTROPERU S.A.

II. ALCANCE

Todas las personas que mantienen un vínculo laboral de forma temporal o permanente y bajo todas las modalidades de contrato; así como las entidades externas y proveedores que tienen acceso a la información de ELECTROPERU S.A. deben cumplir con lo dispuesto en el presente documento.

III. BASE NORMATIVA

- NTP-ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requisitos 2ª Edición.
- Plan Estratégico Institucional.
- Política Nacional de Gobierno Electrónico.
- Ley Nº 27806 "Transparencia y Acceso a la Información Pública, sus modificatorias y reglamento".
- Manual Corporativo "Manual para la documentación de procesos y procedimientos".
- Lineamiento Corporativo "Lineamiento de Gestión Integral de Riesgos para las empresas bajo el ámbito de FONAFE".
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Política de Seguridad de la Información de ELECTROPERU S.A.
- Manual de Gestión Integral de Riesgos (GIR) de ELECTROPERU S.A.

IV. DEFINICIONES

En complemento a las definiciones detalladas en el Manual de Gestión Integral de Riesgos de ELECTROPERU S.A. se señalan las siguientes:

- **Activo:** Bien vinculado a información que tiene valor para la empresa
- **Confidencialidad:** Principio que establece que la información debe ser accesible sólo a aquellos usuarios que se encuentren debidamente autorizados
- **Disponibilidad:** Principio que establece que la información debe estar disponible en forma organizada para los usuarios autorizados cada vez que sea requerida.
- **Evento de seguridad de la información:** Suceso inesperado en el que se trasgrede un determinado control de seguridad de la información pero no se genera un impacto negativo a la empresa.
- **Incidente de seguridad de la información:** Suceso inesperado en el que se trasgrede un determinado control de seguridad de la información y que genera un impacto negativo a la empresa.
- **Integridad:** Principio que establece que la información no sea alterada ni modificada, es decir, debe permanecer completa, exacta y valida.
- **Instalaciones de proceso de información:** Infraestructura (física o lógica) en la que se almacena o procesa información.
- **Política de Seguridad de la Información:** Documento de alto nivel que expresa el compromiso de la Alta Dirección con la seguridad de la información.

- **Sistema de Gestión de Seguridad de la Información - SGSI:** Sistema Integral de gestión que busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Seguridad de la Información:** Consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Tercero:** Personal externo a ELECTROPERU S.A.

V. ENFOQUE

Se utiliza el "Ciclo PDCA" también conocido como "Círculo de Deming":

- **PLAN: Establecimiento y Gestión del SGSI** - Establecer objetivos y procesos para lograr resultados de acuerdo a la Política de Seguridad de la Información de la empresa.
- **DO: Implementación del SGSI** - Implementar los procesos identificados.
- **CHECK: Monitoreo y Revisar el SGSI** - Realizar seguimiento y medición de los procesos respecto a la Política de Seguridad de la Información de la empresa.
- **ACT: Mantener y Mejorar el SGSI** - Tomar acciones para mejorar continuamente el desempeño del sistema.

ELECTROPERU S.A. LUIS HORNA DIAZ Gerente de Administración y Finanzas (e)

VI. COMPONENTES

ELECTROPERU S.A. RENÉ GARAGORRI REYES Subgerente de Imagen Inst. y Resp. Social

El presente documento, desarrolla los siguientes componentes:

- **Componente 01** : Objetivos de la Seguridad de la Información
- **Componente 02** : Organización para la Seguridad de la Información
- **Componente 03** : Alcance del Sistema de Gestión de Seguridad de la Información – SGSI
- **Componente 04** : Declaración de Aplicabilidad – SOA
- **Componente 05** : Metodología para la Gestión de Riesgos de Seguridad de la Información

ELECTROPERU S.A. DENISSE LUYO CAMA Subgerente de Recursos Humanos

ELECTROPERU S.A. MIGUEL SUAREZ MENDOZA Asesor Legal

ELECTROPERU S.A. ADA FUENTES TAPIA Sub Gerente de Planificación y Control (e)

ELECTROPERU S.A. EDWIN SAN ROMAN ZUBIZARRETA Gerente General

ELECTRO PERU S.A. JULIO TAKIMOTO ALDAVE Sub Gerente de Informática

ELECTROPERU S.A. LUIS ALARCÓN TABOADA Analista de Archivo y Trámite Documentario

COMPONENTE 01:
OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

1.1. DESCRIPCIÓN

El presente componente busca identificar y definir en base a la Política de Seguridad de la Información los objetivos a niveles y funciones relevantes en ELECTROPERU S.A.

1.2. DESARROLLO

Los Objetivos de Seguridad de la Información de ELECTROPERU S.A. son:

Objetivo Estratégico	ID	Objetivo de Seguridad de la Información	Indicador
OEI4 OEI5	OSI01	Implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información - SGSI, que permita asegurar la confidencialidad, integridad y disponibilidad de la información.	Procesos incorporados al Sistema de Gestión de Seguridad de la Información (Ejecutado / Planificado)
OEI4 OEI5	OSI02	Proveer los recursos necesarios para el cumplimiento de la Política de la Seguridad de la Información.	Presupuesto aprobado para proyectos vinculados a la Seguridad de la Información (Ejecutado / Planificado)
OEI4 OEI5 OEI7	OSI03	Promover la concientización y capacitación al personal para que contribuyan en el cumplimiento de lo establecido en la Política de la Seguridad de la Información.	Temas de Seguridad de la Información del Plan de capacitación aprobado (Ejecutados / Planificados)
OEI4 OEI5	OSI04	Satisfacer requisitos aplicables relacionados a la seguridad de la información.	Controles de seguridad de la información vinculados a los procesos de la empresa (Implementados / Planificados)

1.3. EVALUACIÓN

Los objetivos de seguridad de la información serán evaluados semestralmente para conocer sobre los avances y resultados respectivos. Cabe indicar que para cumplir cada objetivo identificado se requiere realizar un conjunto de actividades que involucra la participación planificada de diversas áreas de la empresa.

COMPONENTE 02:
ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

2.1. DESCRIPCIÓN

El presente componente busca identificar y asignar la autoridad, los roles y las funciones (responsabilidades) relevantes a la seguridad de la información en ELECTROPERU S.A.

2.2. DESARROLLO

Los roles y las funciones (responsabilidades) para la Seguridad de la Información son:

2.2.1. Rol: Alta Dirección

2.2.1.1. Directorio:

Sus funciones están establecidas según el "Manual de Gestión Integral de Riesgos" de ELECTROPERU S.A.

2.2.1.2. Gerencia General:

Sus funciones están establecidas según el "Manual de Gestión Integral de Riesgos" de ELECTROPERU S.A. Asimismo tiene responsabilidades como:

a. Promover la cultura de gestión de seguridad de la información de ELECTROPERU S.A.
b. Implementar la norma NTP ISO/IEC 27001:2014 en ELECTROPERU S.A.

2.2.1.3. Gerencias:

Denominadas "Responsable de Procesos" según el "Manual de Gestión Integral de Riesgos" de ELECTROPERU S.A.

2.2.2. Rol: Equipo de Gestión Integral de Riesgos

Sus roles y funciones están establecidos en el "Manual de Gestión Integral de Riesgos" de ELECTROPERU S.A.

2.2.3. Rol: Comité de Gobierno Digital

Su conformación y funciones están establecidas en la Resolución Ministerial N° 087-2019-PCM y sus modificaciones.

2.2.4. Rol: Oficial de Seguridad de la Información

Su designación está establecida en la Resolución Ministerial N° 166-2017-PCM y sus modificaciones.Cumple con las siguientes funciones:

a. Coordinar la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.
b. Gestionar la operación y monitoreo del Sistema de Gestión de Seguridad de la Información – SGSI.
c. Gestionar el mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información – SGSI.
d. Comunicar periódicamente al Comité de Gobierno Digital sobre el desempeño del Sistema de Gestión de Seguridad de la Información – SGSI.

2.2.5. Rol: Jefe de área

Comprende Subgerentes o quien haga sus veces. Tiene como funciones:

a. Identificar y reportar incumplimientos a la Política y/o el marco normativo aprobado vigente sobre Seguridad de la Información.
b. Apoyar en la identificación e implementación de controles de seguridad de información.

2.2.6. Rol: Responsable de Proceso (Dueño)

Sus funciones están establecidas según el Manual Corporativo "Manual para la documentación de procesos y procedimientos" de FONAFE y el "Manual de Gestión Integral de Riesgos" de ELECTROPERU S.A.

2.2.7. Rol: Propietario de activo

Designado por el Jefe de área de ELECTROPERU S.A. Tiene como funciones:

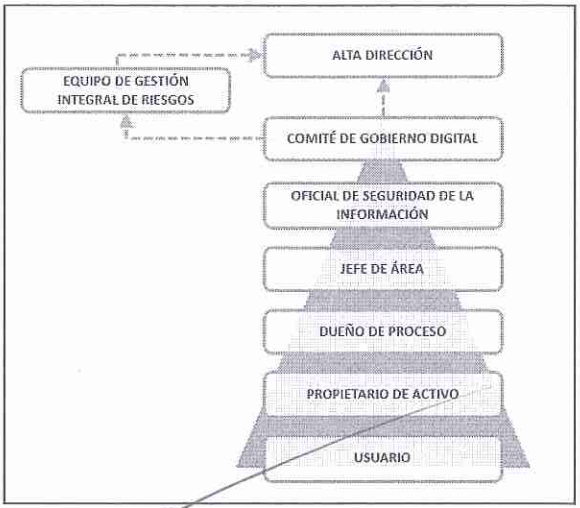
a. Implementar y administrar controles de seguridad de la información a los activos de su responsabilidad.
b. En coordinación con el Oficial de Seguridad de la Información, evaluar los resultados de la implementación de controles en los activos de su responsabilidad.
c. Reportar incidentes y oportunidades de mejora.
d. Cumplir con la política de seguridad de la información, así como identificar y reportar a los niveles correspondientes cualquier incumplimiento a la misma.

2.2.8. Rol: Usuario

Es toda persona que mantiene un vínculo laboral de forma temporal o permanente y bajo todas las modalidades de contrato; así como las entidades externas y proveedores que tienen acceso a la información de ELECTROPERU S.A. Tiene como función:

a. Cumplir con la política de seguridad de la información, así como identificar y reportar a los niveles correspondientes cualquier incumplimiento a la misma.

2.3. AUTORIDAD:



Organización para la Seguridad de la Información

COMPONENTE 03:
ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

3.1. DESCRIPCIÓN

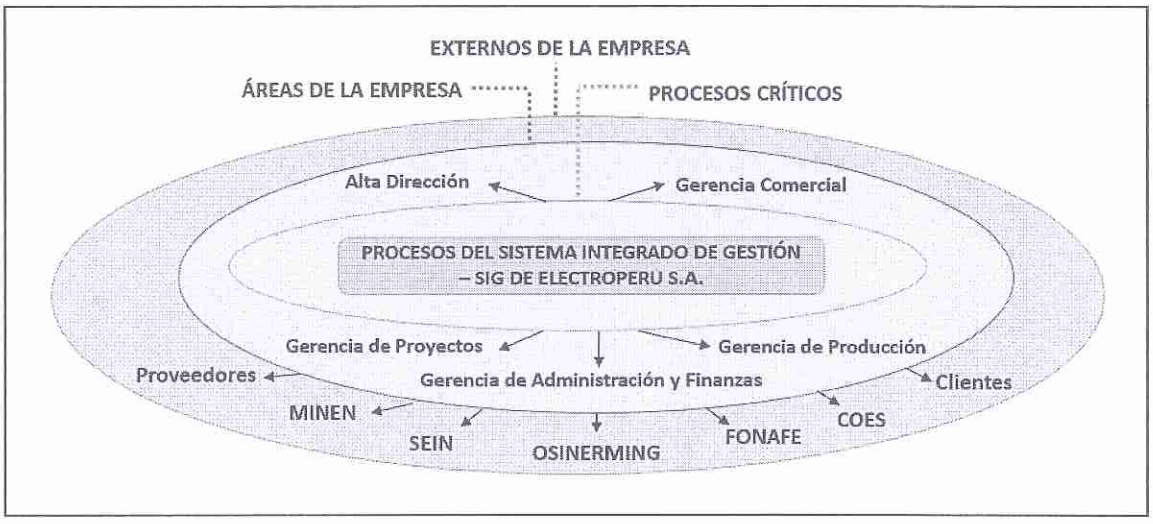
El presente componente busca definir el alcance del Sistema de Gestión de Seguridad de Información - SGSI en ELECTROPERU S.A.

3.2. DESARROLLO

El alcance del Sistema de Gestión de Seguridad de la Información – SGSI, comprende los procesos incluidos en el Sistema Integrado de Gestión – SIG de ELECTROPERU S.A.

En consideración a ello, el alcance del SGSI será actualizado cada vez que se presente alguna modificación y/o actualización en el alcance del SIG de ELECTROPERU S.A. Cabe indicar que la implementación del citado alcance en el SGSI se desarrollará de forma progresiva para lo cual se deberá contar con la planificación respectiva.

Las interfaces y dependencias del alcance del Sistema de Gestión de Seguridad de Información - SGSI de ELECTROPERU S.A. se muestran a continuación:



Interfaces y Dependencias del alcance del Sistema de Gestión de Seguridad de Información - SGSI

COMPONENTE 04:
DECLARACIÓN DE APLICABILIDAD - SOA

4.1. DESCRIPCIÓN

El presente componente busca definir los controles de la NTP ISO/IEC 27001:2014 que son aplicables a ELECTROPERU S.A.

4.2. DESARROLLO

La Declaración de aplicabilidad o SOA de ELECTROPERU S.A. a continuación se detalla:

ITEM	DESCRIPCIÓN	¿APLICA?
A.5	**Políticas de seguridad de la Información**	
A.5.1	**Dirección de la Gerencia para la Seguridad de la Información**	
A.5.1.1	Políticas para la seguridad de la información	SI
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI
A.6	**Organización de Seguridad de la Información**	
A.6.1	**Organización interna**	
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI
A.6.1.2	Segregación de funciones	SI
A.6.1.3	Contacto con autoridades	SI
A.6.1.4	Contacto con grupos especiales de interés	SI
A.6.1.5	Seguridad de la Información en los proyectos	SI
A.6.2	**Dispositivo móviles y trabajo a distancia**	
A.6.2.1	Políticas de dispositivos móviles	SI
A.6.2.2	Teletrabajo	NO
A.7	**Seguridad de los recursos humanos**	
A.7.1	**Antes del empleo**	
A.7.1.1	Selección	SI
A.7.2.2	Términos y condiciones del empleo	SI
A.7.2	**Durante el empleo**	
A.7.2.1	Responsabilidades de la gerencia	SI
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	SI
A.7.2.3	Proceso disciplinario	SI
A.7.3	**Término y cambio de empleo**	
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI
A.8	**Gestión de activos**	
A.8.1	**Responsabilidades sobre los activos**	
A.8.1.1	Inventario de activos	SI
A.8.1.2	Propiedad de los activos	SI
A.8.1.3	Uso aceptable de los activos	SI
A.8.1.4	Retorno de los activos	SI
A.8.2	**Clasificación de la información**	
A.8.2.1	Clasificación de la información	SI
A.8.2.2	Etiquetado de la información	SI
A.8.2.3	Manejo de los activos	SI
A.8.3	**Manejo de los medios**	
A.8.3.1	Gestión de los medios removibles	SI
A.8.3.2	Disposición de medios	SI
A.8.3.3	Transferencia de medios físicos	SI
A.9	**Control de acceso**	
A.9.1	**Requisitos de la empresa para el control de acceso**	
A.9.1.1	Política de control de acceso	SI
A.9.1.2	Acceso a redes y servicios de redes	SI
A.9.2	**Gestión de acceso de usuario**	
A.9.2.1	Registro y baja de usuario	SI
A.9.2.2	Aprovisionamiento de acceso a usuario	SI
A.9.2.3	Gestión de derechos de accesos privilegiados	SI

ELECTROPERU S.A. - LUIS HORNA DÍAZ - Gerente de Administración y Finanzas (e)

ELECTROPERU S.A. - RENÉ GAMARRA REYES - Subgerente de Imagen Inst. y Resp. Social

ELECTROPERU S.A. - DENISSE LUYO CAMA - Subgerente de Recursos Humanos

ELECTRO PERU S.A. - JULIO TAKIMOTO ALDAVE - Gerente de Informática

ELECTROPERU S.A. - LUIS MARCÓN TAPIA - Analista de Archivo y Trámite Documentario

ELECTROPERU S.A. - MIGUEL SUAREZ MENDOZA - Asesor Legal

ELECTROPERU S.A. - ADA FUENTES TAPIA - Sub Gerente de Planificación y Control (e)

ELECTROPERU S.A. - EDWIN SAN ROMAN ZUBIZARRETA - Gerente General

ITEM	DESCRIPCIÓN	¿APLICA?
A.9.2.4	Gestión de información de autenticación secreta de usuarios	NO
A.9.2.5	Revisión de derechos de acceso de usuarios	SI
A.9.2.6	Remoción o ajuste de derechos de acceso	SI
A.9.3	**Gestión de acceso de usuario**	
A.9.3.1	Uso de información de autenticación secreta	NO
A.9.4	**Control de acceso a sistemas y aplicaciones**	
A.9.4.1	Restricción de acceso a la información	SI
A.9.4.2	Procedimientos de ingreso seguro	SI
A.9.4.3	Sistema de gestión de contraseñas	SI
A.9.4.4	Uso de programas utilitarios privilegiados	SI
A.9.4.5	Control del acceso al código fuente de los programas	SI
A.10	**Criptografía**	
A.10.1	**Controles de la Criptografía**	
A.10.1.1	Política del uso de controles criptográficos	NO
A.10.1.2	Gestión de las claves	NO
A.11	**Seguridad física y medioambiental**	
A.11.1	**Áreas seguras**	
A.11.1.1	Perímetro de seguridad física	SI
A.11.1.2	Controles de ingreso físico	SI
A.11.1.3	Asegurar oficinas, áreas e instalaciones	SI
A.11.1.4	Protección contra amenazas externas y ambientales	SI
A.11.1.5	Trabajo en áreas seguras	SI
A.11.1.6	Áreas de despacho y carga	SI
A.11.2	**Equipos**	
A.11.2.1	Emplazamiento y protección de equipos	SI
A.11.2.2	Servicios de suministro	SI
A.11.2.3	Seguridad del cableado	SI
A.11.2.4	Mantenimiento de equipos	SI
A.11.2.5	Remoción de activos	SI
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI
A.11.2.7	Disposición o reutilización segura de equipos	SI
A.11.2.8	Equipos de usuarios desatendidos	SI
A.11.2.9	Política de escritorio y pantalla limpia	SI
A.12	**Seguridad de las operaciones**	
A.12.1	**Procedimientos y responsabilidades operativas**	
A.12.1.1	Procedimientos operativos documentados	SI
A.12.1.2	Gestión del cambio	SI
A.12.1.3	Gestión de la capacidad	SI
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	SI
A.12.2	**Protección contra código malicioso**	
A.12.2.1	Controles contra código malicioso	SI
A.12.3	**Respaldo**	
A.12.3.1	Respaldo de la información	SI
A.12.4	**Registros y monitoreo**	
A.12.4.1	Registro de eventos	SI
A.12.4.2	Protección de la información de registros	SI
A.12.4.3	Registros del administrador y del operador	SI
A.12.4.4	Sincronización de reloj	SI
A.12.5	**Control del software operacional**	
A.12.5.1	Instalación de software en sistemas operacionales	SI
A.12.6	**Gestión de vulnerabilidad técnica**	
A.12.6.1	Gestión de vulnerabilidades técnicas	SI
A.12.6.2	Restricciones sobre la instalación de software	SI
A.12.7	**Consideraciones para la auditoria de los sistemas de información**	
A.12.7.1	Controles de auditoria de sistemas de información	SI
A.13	**Seguridad de las comunicaciones**	
A.13.1	**Gestión de Seguridad de la Red**	
A.13.1.1	Controles de la red	SI

ELECTROPERU S.A. - LUIS HORNA DÍAZ - Gerente de Administración y Finanzas (e)

ELECTROPERU S.A. - RENÉ GARAGORRI REYES - Subgerente de Imagen Insl. y Resp. Social

ELECTROPERU S.A. - DENISSE LUYO CAMA - Subgerente de Recursos Humanos

ELECTRO PERU S.A. - JULIO TAKIMOTO ALDAVE - Gerente de Informática

ELECTROPERU S.A. - LUIS ALARCÓN TARDADA - Analista de Archivo y Trámite Documentario

ELECTROPERU S.A. - MIGUEL SUAREZ MENDOZA - Asesor Legal

ELECTROPERU S.A. - ADA FUENTES TAPIA - Sub Gerente de Planificación y Control (e)

ELECTROPERU S.A. - EDWIN SAN ROMAN ZUBIZARRETA - Gerente General

ITEM	DESCRIPCIÓN	¿APLICA?
A.13.1.2	Seguridad de servicios de red	SI
A.13.1.3	Segregación de redes	SI
A.13.2	**Transferencia de la información**	
A.13.2.1	Políticas y procedimientos de transferencia de la información	SI
A.13.2.2	Acuerdos sobre transferencia de información	SI
A.13.2.3	Mensajes electrónicos	SI
A.13.2.4	Acuerdos de confidencialidad o no divulgación	SI
A.14	**Adquisición, desarrollo y mantenimiento del sistema**	
A.14.1	**Requisitos de seguridad de los sistemas de información**	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI
A.14.1.2	Aseguramiento de servicios sobre redes publicas	SI
A.14.1.3	Protección de transacciones en servicios de aplicación	NO
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	
A.14.2.1	Política de desarrollo seguro	SI
A.14.2.2	Procedimientos de control de cambio del sistemas	SI
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI
A.14.2.4	Restricciones sobre cambio a los paquetes de software	SI
A.14.2.5	Principios de ingeniería de sistemas seguros	SI
A.14.2.6	Ambiente de desarrollo seguro	SI
A.14.2.7	Desarrollo contratado externamente	SI
A.14.2.8	Pruebas de seguridad del sistema	SI
A.14.2.9	Pruebas de aceptación del sistema	SI
A.15	**Relaciones con los proveedores**	
A.15.1	**Seguridad de la información en las relaciones con los proveedores**	
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	SI
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	SI
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI
A.15.2	**Gestión de entrega de servicios del proveedor**	
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	SI
A.15.2.2	Gestión de cambios a los servicios de proveedores	SI
A.16	**Gestión de Incidentes de seguridad de la información**	
A.16.1	**Gestión de Incidentes de seguridad de la información y mejoras**	
A.16.1.1	Responsabilidades y procedimientos	SI
A.16.1.2	Reporte de eventos de seguridad de la información	SI
A.16.1.3	Reporte de debilidades de seguridad de la información	SI
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI
A.16.1.7	Recolección de evidencia	SI
A.17	**Gestión de los aspectos de la seguridad de la información para la continuidad del negocio**	
A.17.1	**Continuidad de la seguridad de la información**	
A.17.1.1	Planificación de continuidad de seguridad de la información	SI
A.17.1.2	Implementación de continuidad de seguridad de la información	SI
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	SI
A.17.2	**Redundancias**	
A.17.2.1	Instalaciones de procesamiento de la información	SI
A.18	**Cumplimiento**	
A.18.1	**Cumplimiento de los requisitos legales y contractuales**	
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	SI
A.18.1.2	Derechos de propiedad intelectual	SI
A.18.1.3	Protección de registros	SI
A.18.1.4	Privacidad y protección de datos personales	SI
A.18.1.5	Regulación de controles criptográficos	NO
A.18.2	**Revisiones de la seguridad de la información**	
A.18.2.1	Revisión independiente de la seguridad de la información	SI
A.18.2.2	Cumplimiento de políticas y normas de seguridad	SI
A.18.2.3	Revisión del cumplimiento técnico	SI

ELECTROPERU S.A. LUIS HORNA DÍAZ Gerente de Administración y Finanzas (e)

ELECTROPERU S.A. RENÉ CARAGORRI REYES Subgerente de Imagen Inst. y Resp. Social

ELECTROPERU S.A. DENISSE LUYO CAMA Subgerente de Recursos Humanos

ELECTRO PERU S.A. JULIO TAKIMOTO ALDAVE Gerente de Informática

ELECTROPERU S.A. LUIS ALARCÓN TABOADA Analista de Archivo y Trámite Documentario

ELECTROPERU S.A. MIGUEL SUAREZ MENDOZA Asesor Legal

ELECTROPERU S.A. ADA FUENTES TAPIA Sub Gerente de Planificación y Control (e)

ELECTROPERU S.A. EDWIN SAN ROMAN ZUBIZARRETA Gerente General

CONTROLES:

En base a la NTP ISO/IEC 27001:2014 se han identificado los siguientes:

A.5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A.5. Dirección de la Gerencia para la Seguridad de la Información

A.5.1.1. Políticas para la Seguridad de la Información

Debe contarse con una Política de Seguridad de la Información aprobada.

A.5.1.2. Revisión de las políticas para la seguridad de la información

Debe revisarse la Política para la Seguridad de la Información periódicamente.

A.6. ORGANIZACÍON DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1. Organización Interna

A.6.1.1. Roles y responsabilidades para la seguridad de la información

Debe definirse y asignarse roles y responsabilidades para la seguridad de la información en la empresa.

A.6.1.2. Segregación de Funciones

Debe diseñarse y aplicarse una estructura organizacional con funciones segregadas.

A.6.1.3. Contacto con autoridades

Debe diseñarse y aplicarse mecanismos para la comunicación con stakeholders relevantes.

A.6.1.4. Contactos con grupos especiales de interés

Debe diseñarse y aplicarse mecanismos para la comunicación con stakeholders relevantes.

A.6.1.5. Seguridad de la información en los proyectos

Debe tratarse la seguridad de la información en la gestión de proyectos.

A.6.2. Dispositivos móviles y trabajo a distancia

A.6.2.1. Políticas de dispositivos móviles

Debe diseñarse y aplicarse mecanismos de seguridad de soporte para el manejo de los riesgos derivados del uso de equipos móviles.

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1. Antes de empleo

A.7.1.1. Selección

Debe verificarse la información de candidatos a ser empleados en concordancia con las leyes, regulaciones y ética relevantes y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.

A.7.1.2. Términos y condiciones del empleo

Debe estipularse en los acuerdos contractuales las responsabilidades de los empleados, contratistas y/o proveedores respecto a la seguridad de la información.

A.7.2. Durante el empleo

A.7.2.1. Responsabilidad de la Gerencia

Debe contarse con el compromiso de la Alta Gerencia para la difusión y aplicación de la política y los mecanismos establecidos para la seguridad de la información.

A.7.2.2. Conciencia, educación y capacitación sobre la seguridad de la información

Debe concientizarse y capacitarse sobre seguridad de la información a las personas que mantienen un vínculo laboral de forma temporal o permanente y bajo todas las modalidades de contrato; así como las entidades externas y proveedores que tienen acceso a la información de la empresa, según sea relevante para sus funciones.

A.7.2.3. Proceso disciplinario

Debe diseñarse y aplicarse mecanismos para la gestión de las infracciones cometidas a la seguridad de la información.

A.7.3. Término y cambio de empleo

A.7.3.1. Terminación o cambio de responsabilidades de empleo

Debe definirse y comunicarse a las personas que mantienen un vínculo laboral de forma temporal o permanente y bajo todas las modalidades de contrato, las responsabilidades de seguridad de la información que permanecerán válidos después del término o cambio de empleo.

A.8. GESTIÓN DE ACTIVOS

A.8.1. Responsabilidades sobre los activos

A.8.1.1. Inventario de activos de información

Debe elaborarse y mantenerse actualizado el inventario de activos de información de los procesos de la empresa.

A.8.1.2. Propiedad de los activos

Debe asignarse propietarios a los activos registrados en el inventario de activos de información.

A.8.1.3. Uso aceptable de los activos

Debe diseñarse y aplicarse mecanismos para el uso aceptable de la información, los activos relacionados a la información y las instalaciones de procesamiento de la misma según los procesos de la empresa.

A.8.1.4. Retorno de los activos

Debe asegurarse que una vez terminado su empleo, contrato o acuerdo, todo personal devuelva los activos que le fueron asignados y que estén en su posesión.

A.8.2. Clasificación de la información

A.8.2.1. Clasificación de la información

Debe clasificarse la información de la empresa.

A.8.2.2. Etiquetado de la información

Debe diseñarse y aplicarse mecanismos para el etiquetado de la información, de acuerdo al esquema de clasificación adoptado por la empresa.

A.8.2.3. Manejo de los activos

Debe diseñarse y aplicarse mecanismos para el manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la empresa.

A.8.3. Manejo de los medios

A.8.3.1. Gestión de los medios removibles

Debe diseñarse y aplicarse mecanismos para la gestión de los medios removibles de acuerdo al esquema de clasificación adoptado por la empresa.

A.8.3.2. Disposición de medios

Debe diseñarse y aplicarse mecanismos para desechar y/o eliminar medios removibles de manera segura.

A.8.3.3. Transferencia de medios físicos

Debe diseñarse y aplicarse mecanismos para proteger los medios removibles que contienen información del acceso no autorizado, mal uso o alteración.

A.9. CONTROL DE ACCESO

A.9.1. Requisitos de la empresa para el control de acceso

A.9.1.1. Política de control de acceso

Debe diseñarse y aplicarse mecanismos para el acceso del personal interno (contratados y/o practicantes) y externo (visitantes y/o terceros que prestan servicios) a las instalaciones de ELECTROPERU S.A.

A.9.1.2. Acceso a redes y servicio de redes

Debe asegurarse que los usuarios tengan acceso solo a la red y a los servicios de red que hayan sido autorizados a usar.

A.9.2. Gestión de acceso de usuario

A.9.2.1. Registro y baja de usuario

Debe diseñarse y aplicarse mecanismos para el registro de altas y bajas de usuarios que tienen acceso a los sistemas y/o servicios.

A.9.2.2. Aprovisionamiento de acceso a usuario

Debe diseñarse y aplicarse mecanismos para asignar o revocar los derechos de acceso a los usuarios de los sistemas y servicios.

A.9.2.3. Gestión de derechos de accesos privilegiados

Debe restringirse y controlarse la asignación de accesos privilegiados.

A.9.2.5. Revisión de derechos de acceso de usuario

Debe realizarse la revisión a los derechos de acceso de usuarios a los activos.

A.9.2.6. Remoción o ajuste de derechos de acceso

Debe retirarse los derechos de acceso a la información e instalaciones de procesamientos de información a todos los usuarios al término del empleo, contrato o acuerdo o ajustarse según el cambio.

A.9.4. Control de acceso a sistemas y aplicaciones

A.9.4.1. Restricción de acceso a la información

Debe restringirse el acceso a la información y a las funciones de los sistemas de acuerdo al mecanismo de control de acceso.

A.9.4.2. Procedimientos de ingreso seguro

Debe controlarse el acceso a los sistemas según el marco normativo vigente.

A.9.4.3. Sistema de gestión de contraseñas

Debe diseñarse y aplicarse mecanismos para la gestión de contraseñas.

A.9.4.4. Uso de programas utilitarios privilegiados

Debe restringirse y controlarse el uso de programas utilitarios y/o software (freeware, shareware, etc.).

A.9.4.5. Control de accesos al código fuente de los programas

Debe restringirse el acceso al código fuente de los programas.

A.11. SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

A.11.1. Áreas Seguras

A.11.1.1. Perímetro de seguridad física

Debe definirse las áreas restringidas en la empresa (contienen información sensible o crítica e instalaciones de procesamiento de la información).

A.11.1.2. Controles de ingreso físico

- Debe diseñarse y aplicarse mecanismos para el acceso sólo a personal autorizado a las áreas restringidas de ELECTROPERU S.A.
- Debe definirse y aprobarse mecanismos para el ingreso y/o salida de bienes de las áreas restringidas de ELECTROPERU S.A.

A.11.1.3. Asegurar oficinas, áreas e instalaciones

Debe diseñarse y aplicarse mecanismos de seguridad física para las áreas restringidas de ELECTROPERU S.A.

A.11.1.4. Protección contra amenazas externas y ambientales

Debe diseñarse y aplicarse mecanismos para la protección física contra desastres naturales, ataques maliciosos o accidentes.

A.11.1.5. Trabajo en áreas seguras

Debe diseñarse y aplicarse mecanismos para el trabajo en áreas restringidas.

A.11.1.6. Áreas de despacho y carga

Debe diseñarse y aplicarse mecanismos para controlar los puntos de acceso, espacios de despacho, carga y descarga en las instalaciones de la empresa.

A.11.2. Equipos

A.11.2.1. Emplazamiento y protección de equipos

Debe ubicarse y protegerse los activos para reducir los riesgos físicos y ambientales.

A.11.2.2. Servicio de suministro

Debe protegerse los activos contra las fallas de energía eléctrica y/o alteraciones causadas por fallas en otros suministros.

A.11.2.3. Seguridad del cableado

Debe protegerse de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.

A.11.2.4. Mantenimiento de equipos

Debe mantenerse de manera correcta los activos de los procesos de la empresa.

A.11.2.5. Remoción de activos

Debe diseñarse y aplicarse mecanismos para el retiro de activos de su lugar.

A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones

Debe aplicarse seguridad a los activos fuera de las instalaciones de la empresa.

A.11.2.7. Disposición o reutilización segura de equipos

Debe garantizarse que se haya eliminado, extraído o recuperado la información y/o licencias del software antes de disponer o reutilizar el activo.

A.11.2.8. Equipos de usuarios desatendidos

Debe asegurarse que los activos desatendidos tengan la protección apropiada.

A.11.2.9. Política de escritorio y pantalla limpia

Debe diseñarse y aplicarse mecanismos para la gestión de la configuración de los escritorios (PC y laptops)

A.12. SEGURIDAD DE LAS OPERACIONES

A.12.1. Procedimientos y responsabilidades operativas

A.12.1.1. Procedimientos operativos documentados

Debe documentarse los procesos operativos y ponerse a disposición de los usuarios.

A.12.1.2. Gestión del cambio

Debe controlarse los cambios en la empresa, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información.

A.12.1.3. Gestión de la capacidad

Debe realizarse el monitoreo y optimización del uso de recursos además de la planificación de los requisitos de capacidad.

A.12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones

Debe contarse con ambientes de desarrollo, prueba y producción configurados para reducir los riesgos de acceso o cambios no autorizados.

A.12.2. Protección contra código malicioso

A.12.2.1. Controles contra código malicioso

Debe diseñarse y aplicarse mecanismos para la detección, prevención, recuperación y protección de la información contra códigos maliciosos.

A.12.3. Respaldo

A.12.3.1. Respaldo de la información

Debe diseñarse y aplicarse mecanismos para la generación y pruebas de las copias de respaldo de la información.

A.12.4. Registros y monitoreo

A.12.4.1. Registro de eventos

Debe producirse, mantenerse y revisarse los registros de los eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información.

A.12.4.2. Protección de la información de registros

Debe protegerse la información de los registros de posibles eventos de adulteración y/o acceso no autorizado.

A.12.4.3. Registros del administrador y del operador

Deben ser protegidos y revisados los registros de las actividades del administrador y del operador del sistema.

A.12.4.4. Sincronización del reloj

Debe sincronizarse a una fuente de tiempo de referencia única los relojes de todos los sistemas de procesamiento de la información en la empresa.

A.12.5. Control de software operacional

A.12.5.1. Instalación de software en sistemas operacionales

Debe diseñarse y aplicarse mecanismos para controlar la instalación de sistemas operacionales en la empresa.

A.12.6. Gestión de vulnerabilidad técnica

A.12.6.1. Gestión de vulnerabilidades técnicas

Debe diseñarse y aplicarse mecanismos para obtener información sobre las vulnerabilidades técnicas presentes en los sistemas de la información utilizados en la empresa.

A.12.6.2. Restricciones sobre la instalación de software

Debe diseñarse y aplicarse mecanismos para controlar la instalación de software por parte de los usuarios.

A.12.7. Consideraciones para la auditoría de los sistemas de información

A.12.7.1. Controles de auditoría de sistemas de información

Debe planificarse las auditorías y actividades que involucran la verificación de sistemas informáticos.

A.13. SEGURIDAD DE LAS COMUNICACIONES

A.13.1. Gestión de seguridad de la red

A.13.1.1. Controles de la red

Debe gestionarse y controlarse las redes de la empresa.

A.13.1.2. Seguridad de servicios de red

Debe diseñarse y aplicarse mecanismos para garantizar el cumplimiento de los niveles de servicios de red.

A.13.1.3. Segregación de redes

Debe segregarse por redes los servicios de información, usuarios y sistemas informáticos.

A.13.2. Transferencia de la información

A.13.2.1. Políticas y procedimientos de transferencia de la información

Debe diseñarse y aplicarse mecanismos para proteger la transferencia de información.

A.13.2.2. Acuerdos sobre transferencia de información

Debe diseñarse y aplicarse mecanismos para la protección de la transferencia de información del negocio entre la empresa y terceros.

A.13.2.3. Mensajes electrónicos

Debe protegerse la información enviada mediante mensajes electrónicos (al interno y externo).

A.13.2.4. Acuerdos de confidencialidad o no divulgación

Debe diseñarse y aplicarse mecanismos de confidencialidad que reflejen las necesidades de la empresa sobre la protección de la información.

A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA

A.14.1. Requisitos de seguridad de los sistemas de información

A.14.1.1. Análisis y especificación de requisitos de seguridad de la información

Debe incluirse requisitos de seguridad de la información en los requerimientos de nuevos sistemas de información o en el mejoramiento de los existentes.

A.14.1.2. Aseguramiento de servicios sobre redes públicas

Debe protegerse la información de las actividades fraudulentas, divulgación y modificaciones no autorizadas.

A.14.2. Seguridad en los procesos de desarrollo y soporte

A.14.2.1. Política de desarrollo seguro

Debe diseñarse y aplicarse mecanismos para el desarrollo de software.

A.14.2.2. Procedimientos de control de cambios del sistema

Debe diseñarse y aplicarse mecanismos para el control de los cambios requeridos vinculados a software.

A.14.2.3. Revisión técnica de aplicaciones después de cambios a la plataforma operativa

Debe revisarse las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo.

A.14.2.4. Restricciones sobre cambio de los paquetes de software

Debe controlarse los cambios requeridos a los paquetes de software.

A.14.2.5. Principios de ingeniería de sistemas seguros

Debe diseñarse y aplicarse mecanismos para el desarrollo de software en la empresa.

A.14.2.6. Ambiente de desarrollo seguro

Debe diseñarse y aplicarse mecanismos para proteger los ambientes de desarrollo de software.

A.14.2.7. Desarrollo contratado externamente

Debe supervisarse y monitorearse las actividades de desarrollo de sistemas contratado externamente.

A.14.2.8. Pruebas de seguridad del sistema

Debe ejecutarse pruebas de funcionalidad de seguridad en el desarrollo del sistema.

A.14.2.9. Pruebas de aceptación del sistema

Debe diseñarse y aplicarse mecanismos para las pruebas de aceptación de los nuevos sistemas de información, renovaciones y nuevas versiones.

A.15. RELACIONES CON LOS PROVEEDORES

A.15.1. Seguridad de la información en las relaciones con los proveedores

A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores

Debe diseñarse y aplicarse mecanismos para mitigar los riesgos asociados al acceso de los proveedores a los activos de la empresa.

A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores

Debe diseñarse y aplicarse mecanismos para que los proveedores accedan, procesen, almacenen, comuniquen o provean información de la empresa.

A.15.1.3. Cadena de suministro de tecnología de información y comunicación

Debe incluir los requisitos para el manejo de los riesgos de seguridad de la información asociados a servicios y productos de tecnología de información.

A.15.2. Gestión de entrega de servicios del proveedor

A.15.2.1. Monitoreo y revisión de servicios de los proveedores

Debe monitorearse, revisarse y auditarse la prestación de servicios de proveedores.

A.15.2.2. Gestión de cambios a los servicios de proveedores

Debe diseñarse y aplicarse mecanismos para gestionar los cambios en la prestación de servicios de los proveedores.

A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A.16.1. Gestión de incidencias de seguridad de la información y mejoras

A.16.1.1. Responsabilidades y procedimientos

Debe diseñarse y aplicarse mecanismos para garantizar respuesta a los incidentes de seguridad de la información.

A.16.1.2. Reporte de eventos de seguridad de la información

Debe diseñarse y aplicarse mecanismos para reportar los eventos de seguridad de la información a través de canales definidos.

A.16.1.3. Reporte de debilidades de seguridad de la información

Debe diseñarse y aplicarse mecanismos para advertir y/o reportar cualquier debilidad de seguridad de la información identificada en los sistemas o servicios.

A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información

Debe diseñarse y aplicarse mecanismos para evaluar los eventos de seguridad de la información; y su clasificación como incidentes.

A.16.1.5. Respuesta a incidentes de seguridad de la información

Debe diseñarse y aplicarse mecanismos para atender los incidentes de seguridad de la información.

A.16.1.6. Aprendizaje de los incidentes de seguridad de la información

Debe gestionarse el conocimiento obtenido del análisis y resolución de incidentes de seguridad de la información (reducir probabilidad o impacto de incidentes futuros).

A.16.1.7. Recolección de evidencia

Debe diseñarse y aplicarse mecanismos para registrar todas las evidencias sobre las amenazas, eventos, incidentes o riesgos para la empresa.

A.17. GESTIÓN DE LOS ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA CONTINUIDAD DEL NEGOCIO

A.17.1. Continuidad de la seguridad de la información

A.17.1.1. Planificación de continuidad de seguridad de la información

Debe determinarse los controles para la seguridad de la información y su continuidad en situaciones adversas (crisis o desastre).

A.17.1.2. Implementación de continuidad de seguridad de la información

Debe planificarse la ejecución de pruebas para la actualización del plan de continuidad de seguridad de la información.

A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información

Debe verificarse periódicamente los controles de la continuidad de la seguridad de la información establecidos e implementados.

A.17.2. Redundancias

A.17.2.1. Instalaciones de procesamiento de la información

Debe contarse con instalaciones de procesamiento de la información con redundancia suficiente para cumplir con los requisitos de disponibilidad.

A.18. CUMPLIMIENTO

A.18.1. Cumplimiento de los requisitos legales y contractuales

A.18.1.1. Identificación de requisitos contractuales y de legislación aplicables

Debe identificarse, documentarse y mantenerse actualizados todos los requisitos legislativos, regulatorios y contractuales que la empresa debe cumplir.

A.18.1.2. Derechos de propiedad intelectual

Debe diseñarse y aplicarse mecanismos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a la propiedad intelectual y al uso de software licenciado.

ELECTROPERU S.A. - LUIS HORNA DÍAZ - Gerente de Administración y Finanzas (e)

A.18.1.3. Protección de registros

Debe protegerse los registros contra la pérdida, destrucción, falsificación, acceso y/o divulgación no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.

A.18.1.4. Privacidad y protección de datos personales

Debe garantizarse la privacidad y la protección de datos personales según lo requiera la legislación y regulación y en la medida que sea aplicable.

ELECTROPERU S.A. - RENÉ GARAYCOCHEA REYES - Subgerente de Imagen Inst. y Resp. Social

A.18.2. Revisiones de la seguridad de la información

A.18.2.1. Revisión independiente de la seguridad de la información

Debe diseñarse y aplicarse mecanismos adecuados para revisar de forma independiente el enfoque de la empresa para gestionar la seguridad de la información y su implementación.

A.18.2.2. Cumplimiento de políticas y normas de seguridad

Debe evaluarse el cumplimiento al marco normativo referido a la Seguridad de la Información.

ELECTROPERU S.A. - DENISSE LUYO CAMA - Subgerente de Recursos Humanos

A.18.2.3. Revisión del cumplimiento técnico

Debe evaluarse los sistemas de la información con respecto al cumplimiento del marco normativo referido a la Seguridad de la Información de la empresa.

ELECTRO PERU S.A. - JULIO TAKIMOTO ALDAVE

ELECTROPERU S.A. - LUIS ALARCÓN TABOADA - Analista de Archivo y Trámite Documentario

ELECTROPERU S.A. - MIGUEL SUÁREZ MENDOZA - Asesor Legal

ELECTROPERU S.A. - ADA FUENTES TAPIA - Sub Gerente de Planificación y Control (e)

ELECTROPERU S.A. - EDWIN SAN ROMAN ZUBIZARRETA - Gerente General

COMPONENTE 05:
METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

5.1. DESCRIPCIÓN

El presente componente busca definir la metodología para gestionar los riesgos vinculados a la seguridad de la información en ELECTROPERU S.A.

5.2. DESARROLLO

5.2.1. Identificación de activos del proceso: (Formato 01)

a. Identificar los activos del proceso
b. Clasificar de los activos del proceso:

TIPO	CATEGORIA	CÓD.	DESCRIPCIÓN
Información	Información electrónica - digital	AI1	Información contenida en medios electrónicos
	Información escrita	AI2	Información contenida en papel
Software	Software licenciado	AS1	Requiere de licencias
	Software no licenciado	AS2	No requiere de licencias
Físico	Equipo de procesamiento	AF1	Servidores, PC, laptops y otros
	Equipo de comunicación	AF2	Router, Switch, cableado, telefonía y otros
	Almacenamiento externo	AF3	USB, discos duros externos, CD y otros
	Mobiliario y equipamiento	AF4	Estantes, cajas fuertes, archivadores y otros
	Equipamiento auxiliar	AF5	Fuentes de alimentación, UPS, equipos de climatización y otros
	Instalaciones	AF6	Sedes, oficinas, almacenes y otros
	Otros equipos	AF7	Impresoras, scaners y otros
Servicio	Servicios específicos	SE1	Impresión, fotocopiado, mensajería y otros
	Servicios generales	SE2	Energía eléctrica, seguridad, limpieza y otros
Personal	Interno	PE1	Incluye personal de planilla y practicantes
	Externo	PE2	Incluye proveedores, supervisores y otros

c. Definir la frecuencia de uso de los activos del proceso.
d. Definir al propietario del activo del proceso (propietario de riesgos vinculados a dicho activo). Este reportará al Responsable del proceso el estado del mismo.

5.2.2. Análisis de activos del proceso: (Formato 01)

a. Analizar los criterios de seguridad de la información de los activos del proceso:

CRITERIOS	DESCRIPCIÓN
Confidencialidad	Autorización a la información vinculada al activo
Integridad	Exactitud de la información vinculada al activo
Disponibilidad	Accesibilidad a la información vinculada al activo

IMPACTO		
Alto (3)	Medio (2)	Bajo (1)
Afectación de proceso (s) o información clasificada como de criticidad alta.	Afectación de proceso (s) o información clasificada como de criticidad media	Afectación de proceso (s) o información clasificada como de criticidad baja

b. Estimar el valor del activo del proceso, mediante la siguiente fórmula:
Valor del Activo = (Confidencialidad + Integridad + Disponibilidad) /3

c. Determinar la tasación del activo del proceso, en base a la siguiente tabla:

Valor del Activo	Nivel de Criticidad
2,67 - 3	Alto
2 - 2,66	Medio
1 - 1,99	Bajo

5.2.3. Identificación de riesgos de los activos del proceso

Esta actividad se lleva a cabo según lo definido en el Manual de Gestión Integral de Riesgos.

5.2.4. Análisis de riesgos de los activos del proceso:

Comprende el desarrollo de las actividades siguientes:

a. Analizar la probabilidad y el Impacto de los riesgos del activo.
b. Determinar el nivel o criticidad del riesgo (Probabilidad por Impacto) del activo.

Estas actividades se llevan a cabo considerando los valores establecidos en el Manual de Gestión Integral de Riesgos.

5.2.5. Evaluación de riesgos de los activos del proceso:

Comprende el desarrollo de las actividades siguientes:

a. Evaluar el nivel o criticidad del riesgo y priorizarlos.
b. Representar los resultados de la evaluación en un Mapa de Riesgos.

Estas actividades se llevan a cabo considerando los valores establecidos en el Manual de Gestión Integral de Riesgos.

5.2.6. Tratamiento de riesgos de los activos del proceso

Se deberá realizar el tratamiento de riesgos considerando lo definido en el Manual de Gestión Integral de Riesgos.

5.2.7. Seguimiento y monitoreo continuo

Se deberá realizar el seguimiento y monitoreo continuo considerando lo definido en el Manual de Gestión Integral de Riesgos.

5.3. FORMATO

FORMATO 01: ACTIVOS DE PROCESOS – SEGURIDAD DE INFORMACIÓN														
PROCESO		ACTIVO								ANÁLISIS			TASACIÓN	
Código	Nombre	Código	Nombre	Descripción	Tipo	Categoría	Ubicación	Propietario	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel