REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de Electricidad

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE REGULACIÓN Y CONTROL DE ELECTRICIDAD

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

INFORME Nro. OSI-2025-001

Octubre 2025

CONTENIDO

1. Antecedentes

La seguridad de la información es un componente fundamental en la gestión moderna de las instituciones públicas, especialmente en un entorno digital interconectado. La creciente digitalización de los servicios y la información en el sector público ha puesto de manifiesto la importancia de proteger los activos de información frente a riesgos cibernéticos y amenazas externas, así como asegurar la continuidad de los servicios que se brindan a los ciudadanos.

En este sentido, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), en su rol como ente rector en la implementación de políticas de seguridad, emitió el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, publicado en el Tercer Suplemento del Registro Oficial Nro. 509 de 01 de marzo de 2024. Este acuerdo establece el Esquema Gubernamental de Seguridad de la Información (EGSI), que constituye un marco normativo para la protección de la información dentro de las instituciones del sector público. El EGSI establece un sistema estructurado para gestionar los riesgos asociados a la seguridad de la información, alineando a todas las entidades del sector público con prácticas internacionales en ciberseguridad y protección de datos.

Este esquema requiere que las instituciones del sector público implementen políticas y procedimientos claros para identificar, evaluar y mitigar los riesgos de seguridad de la información, asegurando así la protección de los datos sensibles que gestionan. De igual manera, subraya la necesidad de realizar un proceso continuo de mejora, donde las políticas de seguridad de la información jueguen un rol crucial en la adaptabilidad y fortaleza de las instituciones frente a nuevas amenazas.

Es por esto que, como respuesta a la necesidad de cumplir con los lineamientos establecidos por el Acuerdo Ministerial y con el propósito de proteger la integridad y disponibilidad de la información, esta institución ha decidido formalizar la Política de Seguridad de la Información, la cual se enmarca dentro de los requisitos del Esquema Gubernamental de Seguridad de la Información (EGSI) y que permitirá garantizar la seguridad y la confianza en la información gestionada a través de sus procesos y sistemas.

Base Normativa:

Constitución de la República del Ecuador

La Constitución de la República del Ecuador establece, en su artículo 226, que las entidades públicas tienen el deber de garantizar los derechos de los ciudadanos, entre los cuales se incluye el acceso a la información de forma segura y transparente. Además, la Constitución reconoce la importancia de una administración pública eficiente y eficaz, que se basa en la correcta gestión de los recursos, incluyendo la información.

Ley Orgánica de Telecomunicaciones

La Ley Orgánica de Telecomunicaciones en su artículo 140 confiere al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) la responsabilidad de establecer políticas, directrices y planes en áreas clave, incluyendo la seguridad de la información en el sector público. Esta ley también establece la obligación del MINTEL de supervisar y garantizar la implementación de estándares y prácticas de seguridad en las instituciones gubernamentales.

Ley Orgánica para la Transformación Digital y Audiovisual

La Ley Orgánica para la Transformación Digital y Audiovisual, promulgada con el fin de fomentar la digitalización del sector público, refuerza la necesidad de establecer un Marco de Seguridad Digital, el cual debe ser cumplido por todas las entidades de la administración pública. En su artículo 19, esta ley establece

que las instituciones públicas deben mantener un Sistema de Gestión de Seguridad de la Información para proteger los datos sensibles y garantizar la operatividad en el entorno digital.

Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales establece que las instituciones públicas y privadas tienen la obligación de adoptar medidas de seguridad para la protección de datos personales. Esta ley establece los principios de protección, los cuales incluyen la confidencialidad, el acceso restringido y la integridad de los datos, y su cumplimiento es esencial para asegurar la privacidad de los ciudadanos en todas las interacciones con las entidades del sector público.

Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003

El Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, publicado en el Tercer Suplemento del Registro Oficial Nro. 509 de 01 de marzo de 2024, establece el Esquema Gubernamental de Seguridad de la Información (EGSI). Este acuerdo es el instrumento normativo clave que orienta la implementación de un Sistema de Gestión de Seguridad de la Información en las instituciones del sector público, estableciendo directrices claras sobre la evaluación de riesgos, la implementación de controles de seguridad y la responsabilidad de las máximas autoridades en la materia.

Normas Internacionales de Seguridad de la Información

La ISO/IEC 27001 y la ISO/IEC 27002 son normas internacionales que proporcionan un marco para el diseño, implementación y gestión de un Sistema de Gestión de Seguridad de la Información (SGSI). La ISO/IEC 27001 establece los requisitos para implementar un SGSI eficaz, mientras que la ISO/IEC 27002 ofrece directrices sobre las mejores prácticas para la gestión de la seguridad de la información. Estas normas sirven de referencia para el Esquema Gubernamental de Seguridad de la Información (EGSI) y son adoptadas por las instituciones del sector público para garantizar la protección de los activos de información.

Normas y Directrices del Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT)

El Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT) del sector público es una entidad que proporciona apoyo ante incidentes de seguridad cibernética y ayuda a gestionar la respuesta ante amenazas. Sus directrices y protocolos de actuación son fundamentales para la implementación de medidas de seguridad en las instituciones públicas, así como para coordinar la respuesta ante ciberataques o brechas de seguridad.

Implementación en la ARCONEL:

La Política de Seguridad de la Información de la ARCONEL será implementada conforme los lineamientos establecidos por el Esquema Gubernamental de Seguridad de la Información (EGSI), en cumplimiento con el Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003. La implementación se llevará a cabo mediante un enfoque gradual que incluirá la evaluación de riesgos en los activos de información críticos, la capacitación continua del personal, y la adopción de controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos institucionales.

La ARCONEL conformará un Comité de Seguridad de la Información, integrado por representantes de diversas áreas clave, y designará un Oficial de Seguridad de la Información encargado de coordinar y supervisar el cumplimiento de la política. Se establecerán procedimientos de monitoreo y mejora continua para garantizar que las medidas de seguridad se mantengan actualizadas y efectivas frente a las amenazas emergentes.

2. Política de Seguridad de la Información

2.1. Descripción de la Política

El Comité de Seguridad de la Información de la Agencia de Regulación y Control de Electricidad (ARCONEL), en cumplimiento con la normativa legal vigente y el Esquema Gubernamental de Seguridad de la Información (EGSI) establecido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), reconoce la importancia crítica de una gestión segura y eficiente de la información. La ARCONEL se compromete plenamente con la implementación del EGSI, asegurando que se adopten los estándares y procedimientos necesarios para la protección de los activos de información dentro de la institución.

La Política de Seguridad de la Información tiene como objetivo principal minimizar, mitigar o eliminar los riesgos asociados a la pérdida, fuga o manipulación no autorizada de la información. Este compromiso con la seguridad de la información se basa en los principios de confidencialidad, integridad y disponibilidad, considerando las necesidades de los grupos de interés tanto internos como externos a la institución.

En consecuencia, esta política será de aplicación obligatoria para todos los funcionarios de la ARCONEL, así como para los terceros, proveedores y cualquier entidad o persona que interactúe con la Agencia en términos de gestión de información. Su cumplimiento será monitoreado de manera continua para garantizar la eficacia y adecuación de las medidas adoptadas, con el fin de asegurar que los datos e información institucional sean tratados con el más alto nivel de seguridad y respeto a la privacidad.

2.2. Objetivo

Establecer un marco integral de gestión de la seguridad de la información, que garantice la protección, confidencialidad, integridad y disponibilidad de los datos e información institucional. Este objetivo busca mitigar los riesgos asociados con la gestión de la información, asegurar el cumplimiento de la normativa legal y regulatoria vigente, promover una cultura organizacional de seguridad a través de la concienciación y formación continua del personal; y, proteger los derechos de la ciudadanía respecto al manejo de sus datos personales, con el fin de asegurar la continuidad de los servicios y la confianza en la institución.

2.3. Objetivos Específicos

- Garantizar la protección de la información institucional mediante la implementación de controles de seguridad adecuados que salvaguarden la confidencialidad, integridad y disponibilidad de los datos gestionados por la ARCONEL.
- Identificar, evaluar y gestionar los riesgos de seguridad de la información mediante la realización de auditorías y evaluaciones periódicas, con el fin de mitigar posibles amenazas y vulnerabilidades en los sistemas y procesos.
- Cumplir con las normativas legales y regulatorias vigentes en materia de seguridad de la información, incluyendo el Esquema Gubernamental de Seguridad de la Información (EGSI), así como las normativas nacionales e internacionales aplicables en protección de datos y

ciberseguridad.

- Promover una cultura de seguridad de la información dentro de la ARCONEL, mediante programas de concienciación, capacitación y sensibilización continua para todo el personal sobre la importancia de la protección de datos y las mejores prácticas en ciberseguridad.
- Asegurar la privacidad y protección de los datos personales de los ciudadanos y usuarios que interactúan con la ARCONEL, garantizando su manejo conforme la Ley Orgánica de Protección de Datos Personales y otras regulaciones relacionadas.
- Establecer y mantener un sistema de gestión de incidentes de seguridad de la información, que permita detectar, reportar, analizar y responder de manera eficiente ante cualquier incidente de seguridad, minimizando su impacto en las operaciones de la institución.
- Garantizar la continuidad de los servicios institucionales mediante la implementación de un Plan de Recuperación ante Desastres (DRP), que permita asegurar la operación de la ARCONEL ante eventos que puedan afectar la infraestructura tecnológica y la disponibilidad de la información crítica.

2.4. Roles y Responsabilidades

2.4.1 Máxima Autoridad

La Máxima Autoridad (Director Ejecutivo) de la ARCONEL , tiene las siguientes responsabilidades:

a) Disponer la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la ARCONEL, asegurando que todas las políticas, procedimientos y controles necesarios sean adoptados para garantizar la protección adecuada de los activos de información institucionales.
b) La Máxima Autoridad de la ARCONEL, a través del Comité de Seguridad de la Información (CSI), será responsable de asegurar que la gestión de la seguridad de la información sea realizada de manera efectiva, alineada con las normativas vigentes y con los objetivos estratégicos de la institución. Esta responsabilidad incluye la supervisión continua de los procesos de seguridad y la toma de decisiones sobre acciones correctivas o de mejora.

2.4.2 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, de acuerdo con lo detallado en el Esquema Gubernamental de Seguridad de la Información, tiene las siguientes responsabilidades:

- Establecer los objetivos de seguridad de la información: Definir los objetivos de seguridad de la información alineados con los objetivos estratégicos de la ARCONEL, asegurando que todos los procesos de la institución consideren la protección de los datos como una prioridad.
- Gestionar la implementación y seguimiento de iniciativas de seguridad: Asegurar la ejecución efectiva de las iniciativas de seguridad de la información, supervisando la implementación de medidas preventivas y correctivas para mitigar riesgos.
- Aprobar y revisar la política de seguridad de la información institucional: Supervisar la aprobación de la Política de Seguridad de la Información por parte de la Máxima Autoridad de la ARCONEL y realizar revisiones periódicas para adaptarla a nuevos desafíos y regulaciones.
- Realizar el seguimiento del comportamiento de los riesgos: Monitorear y evaluar el

comportamiento de los riesgos que afectan a los activos de información, tomando decisiones sobre las medidas que deben adoptarse para mitigar o controlar dichos riesgos.

- Supervisar la gestión de incidentes de seguridad de la información: Conocer y supervisar la investigación y resolución de incidentes relacionados con la seguridad de la información, especialmente aquellos de alto impacto, según los protocolos establecidos en el Plan de Respuesta ante Incidentes.
- Coordinar la implementación de controles específicos de seguridad: Asegurar la implementación de controles específicos de seguridad en los sistemas y servicios de la ARCONEL, siguiendo las directrices del Esquema Gubernamental de Seguridad de la Información (EGSI) y otros marcos normativos aplicables.
- Promover la difusión de la seguridad de la información dentro de la ARCONEL: Fomentar una cultura de seguridad de la información dentro de la institución, mediante programas de sensibilización y capacitación para todo el personal, asegurando que cada funcionario esté comprometido con la protección de los datos.
- Gestionar la continuidad de las operaciones frente a incidentes de seguridad: Coordinar las actividades necesarias para garantizar la continuidad de los servicios y sistemas de información de la ARCONEL en caso de incidentes de seguridad, incluyendo la ejecución del Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP).
- Coordinar la realización de auditorías y evaluaciones internas: Asegurar la realización de auditorías internas y evaluaciones de seguridad periódicas para verificar el cumplimiento de la política de seguridad y las medidas adoptadas, identificando áreas de mejora para implementar nuevas estrategias de seguridad.

2.4.3 Oficial de Seguridad de la Información

Las responsabilidades del Oficial de Seguridad de la Información (OSI) están detalladas en el Artículo 9 del Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003. Este artículo establece de manera clara las funciones y responsabilidades del OSI en relación con la gestión de la seguridad de la información dentro de las instituciones del sector público, incluyendo las responsabilidades dentro de la ARCONEL.

- Identificar y conocer la estructura organizacional de la institución: El OSI debe conocer y entender la estructura organizacional de la institución, así como las interacciones entre los distintos procesos y áreas que manejan la información.
- Identificar las personas o instituciones públicas o privadas que de alguna forma influyen o impactan en la implementación del EGSI: El OSI debe identificar a las personas o instituciones clave, tanto públicas como privadas, que influyen en la implementación del EGSI para asegurar una colaboración efectiva y una integración adecuada del sistema de seguridad.
- Implementar y actualizar el EGSI en su institución: El OSI debe llevar a cabo la implementación inicial del EGSI y asegurar su actualización continua para adaptarse a los cambios tecnológicos, normativos y organizacionales de la institución.
- Elaborar y coordinar con las áreas respectivas las propuestas para la elaboración de la documentación esencial del EGSI: El OSI debe trabajar en conjunto con las áreas pertinentes para desarrollar y coordinar la documentación clave del EGSI, asegurando que esta refleje las políticas, procedimientos y controles necesarios para la seguridad de la información.
- Elaborar, asesorar y coordinar con los funcionarios la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas: El OSI debe desarrollar y proporcionar asesoramiento para la realización de un Estudio de Gestión de Riesgos en

Seguridad de la Información, colaborando con las áreas involucradas para identificar y mitigar riesgos relevantes para la institución.

- Elaborar y coordinar el Plan de concienciación en Seguridad de la Información basado en el EGSI: El OSI debe diseñar y coordinar un plan integral de concienciación sobre seguridad de la información, en línea con el EGSI, trabajando en conjunto con las áreas involucradas y el área de comunicación institucional.
- Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas: El OSI debe promover la cultura de seguridad de la información dentro de la institución, realizando actividades y campañas para sensibilizar a todos los niveles de la organización sobre la importancia de proteger la información.
- Elaborar el plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas, y coordinar su ejecución con las áreas responsables: El OSI debe desarrollar un plan detallado para dar seguimiento a la implementación de medidas correctivas o mejoras, trabajando estrechamente con las áreas responsables para asegurar su ejecución efectiva.
- Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con el área de TI y las áreas clave involucradas, para garantizar la continuidad de las operaciones institucionales ante una interrupción: El OSI debe coordinar la creación y actualización de un Plan de Recuperación de Desastres (DRP), asegurando que el plan involucre a las áreas de TI y otras áreas clave para proteger la continuidad operativa ante cualquier eventualidad.
- Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución: El OSI debe desarrollar procedimientos claros y efectivos para la gestión de incidentes de seguridad de la información, asegurando que los mismos sean manejados de manera oportuna y adecuada.
- Coordinar la gestión de incidentes de seguridad de la información con nivel de impacto alto y que no pudieran ser resueltos en la institución, a través del Centro de Respuestas a Incidentes Informáticos (CSIRT) sectorial y/o nacional: El OSI debe gestionar los incidentes de seguridad de alto impacto que no puedan ser resueltos internamente, coordinando con el CSIRT sectorial o nacional para su pronta resolución.
- Coordinar la realización periódica de revisiones internas al EGSI, así como dar seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión: El OSI debe coordinar revisiones internas periódicas del EGSI, garantizando que se tomen las medidas necesarias para implementar las recomendaciones que surjan de dichas evaluaciones.
- Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada: El OSI debe gestionar y organizar toda la documentación generada durante el proceso de implementación, seguimiento y mejora continua del EGSI, incluyendo políticas, controles, registros y otros documentos relevantes.
- Coordinar con las diferentes áreas que forman parte de la implementación del EGSI, la verificación, monitoreo y el control del cumplimiento de las normas, procedimientos, políticas y controles de seguridad institucionales establecidos de acuerdo a las responsabilidades de cada área: El OSI debe coordinar con las áreas relevantes para asegurar la correcta verificación y monitoreo del cumplimiento de las políticas y controles de seguridad establecidos, garantizando que cada área cumpla con sus responsabilidades en el marco del EGSI.

- Informar al Comité de Seguridad de la Información sobre el avance de la implementación del EGSI y mejora continua, así como las alertas que impidan su implementación: El OSI debe mantener informado al Comité de Seguridad de la Información sobre el progreso del EGSI y las acciones de mejora continua, señalando cualquier alerta o barrera que impida la efectiva implementación del sistema.
- Previa la terminación de sus funciones, el OSI realizará la entrega-recepción de la documentación generada al nuevo Oficial de Seguridad de la Información y la transferencia de conocimientos al Comité de Seguridad de la Información: El OSI debe garantizar una adecuada transferencia de conocimiento y documentación al nuevo oficial o al Comité de Seguridad de la Información antes de su salida, asegurando la continuidad del proceso de seguridad de la información.
- Administrar y mantener el EGSI mediante la definición de estrategias, políticas, normas y controles de seguridad, siendo responsable del cumplimiento el propietario de la información del proceso: El OSI debe gestionar y actualizar el EGSI, desarrollando estrategias, políticas y controles de seguridad, asegurando que cada propietario de la información cumpla con las normativas y procedimientos establecidos.
- Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información: El OSI debe ser el contacto principal con el Ministerio de Telecomunicaciones y de la Sociedad de la Información, facilitando la comunicación y el cumplimiento de las normativas en materia de seguridad de la información.

2.4.4 Servidores de la ARCONEL

Conforme las directrices establecidas en el Esquema Gubernamental de Seguridad de la Información (EGSI) y el Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003, los servidores de la ARCONEL tienen las siguientes responsabilidades:

a) Cumplir con todas las normas legales, políticas, procedimientos e instructivos internos y externos emitidos por la ARCONEL, que se encuentren vigentes, en especial aquellos relacionados con la protección de la información y la seguridad de los sistemas.

b) Mantener la confidencialidad de la información relacionada con sus actividades y funciones dentro de la ARCONEL, y garantizar que no se divulgue sin la debida autorización escrita.

c) No revelar, divulgar, ni facilitar la información generada en el desempeño de sus funciones, ni utilizarla para beneficio propio o de terceros, respetando los principios de confidencialidad, integridad y disponibilidad de la información de la ARCONEL.

d) No reproducir, modificar, hacer pública ni divulgar la información de la ARCONEL sin la autorización expresa de la autoridad competente, siguiendo estrictamente los lineamientos del EGSI.

e) Reconocer que toda la información generada durante el cumplimiento de sus funciones es propiedad exclusiva de la ARCONEL y deberá ser gestionada conforme las políticas y normativas internas.

f) Respetar los derechos de propiedad intelectual sobre la información generada y asegurar que dicha información no sea transmitida o distribuida sin la debida autorización.

g) Utilizar los equipos y recursos tecnológicos de la ARCONEL únicamente para fines relacionados con sus actividades oficiales, restringiendo su uso a otros fines no autorizados.

h) Garantizar que toda la información no pública relacionada con las personas y entidades públicas es confidencial, y solo será utilizada para fines establecidos dentro del marco de sus

funciones dentro de la ARCONEL.

i) Ser responsable de no poner en riesgo la integridad, disponibilidad y confidencialidad de la información manejada, y comprometerse a cumplir con los procedimientos de seguridad aplicables a su función.

j) Entender que cualquier incumplimiento, ya sea intencional o por negligencia, podría implicar sanciones disciplinarias de acuerdo con las normativas vigentes.

k) No utilizar la información de la ARCONEL para fines contrarios a los intereses institucionales.

l) No intentar acceder a recursos que no estén asignados a su persona, ya que esto podrá considerarse como un intento de violación a la seguridad de la institución, con las consecuencias pertinentes.

m) No divulgar bajo ninguna forma, verbal, escrita o electrónica, la información obtenida de los sistemas informáticos de la ARCONEL.

n) Cambiar inmediatamente la contraseña asignada por los responsables del área de Tecnologías de la Información y Comunicación (TIC), y mantener la confidencialidad de la misma.

o) Modificar la contraseña si se sospecha que ha sido comprometida o utilizada por otra persona sin autorización.

p) No permitir que otras personas utilicen su cuenta de usuario.

q) Aceptar la responsabilidad por el uso de su cuenta de usuario, garantizando que se cumplan las políticas de seguridad establecidas.

r) Utilizar los sistemas informáticos de la ARCONEL solo para fines aprobados, cumpliendo con la normativa interna y regulaciones externas.

s) No instalar software no homologado ni autorizado por la Dirección de Tecnologías de la Información y Comunicación.

t) Reconocer que toda la información almacenada en los equipos informáticos de la ARCONEL es propiedad institucional y está sujeta a administración y monitoreo de acuerdo con las pautas de seguridad definidas.

u) Eliminar cualquier mensaje o archivo de origen desconocido o con contenido dudoso, y notificar de inmediato al Oficial de Seguridad de la Información para la debida investigación.

v) Cerrar la sesión o bloquear el equipo de trabajo asignado al finalizar sus tareas, para evitar el uso no autorizado.

w) Mantener un comportamiento ético y profesional en el manejo de la información y en la utilización de los mecanismos de seguridad implementados por la ARCONEL.

x) Aceptar que el incumplimiento de cualquiera de estas normas podría resultar en la revocación del acceso a los sistemas de información y la imposición de sanciones administrativas y penales.

2.4.5 Dirección de Administración del Talento Humano

La Dirección de Administración del Talento Humano, tiene las siguientes responsabilidades:

a) Promover la Capacitación en Seguridad de la Información:

   Garantizar que todo el personal de la ARCONEL reciba formación continua sobre la importancia de la seguridad de la información, las políticas institucionales en este ámbito, y las mejores prácticas para la protección de los datos institucionales.

b) Incorporar el Cumplimiento de la Seguridad de la Información en los Procesos de Selección:

   Asegurar que los nuevos empleados comprendan y se comprometan con la Política de Seguridad de la Información desde el momento de su contratación, incorporando en los

procesos de selección preguntas y evaluaciones sobre seguridad de la información.

c) Sensibilización sobre la Confidencialidad de la Información:

Desarrollar programas de sensibilización sobre la confidencialidad de la información, resaltando la importancia de proteger los datos e información a la que se tiene acceso en el desempeño de las funciones laborales.

d) Colaboración en la Definición de Roles de Seguridad:

Colaborar con el Comité de Seguridad de la Información (CSI) para identificar y designar los roles clave de seguridad de la información dentro de la institución, y asegurar que cada miembro del personal tenga claro su papel en la protección de la información.

e) Gestión del Cumplimiento de Políticas de Seguridad:

Asegurar que todos los funcionarios de la ARCONEL reciban formación y se adhieran a las políticas y procedimientos establecidos para el manejo de la información, siguiendo las directrices del EGSI.

f) Evaluación de la Competencia en Seguridad de la Información:

Evaluar periódicamente las competencias del personal en relación con la seguridad de la información, realizando pruebas o evaluaciones para medir la comprensión de las políticas de seguridad y la capacidad para gestionarlas adecuadamente.

g) Apoyo en la Implementación de la Política de Seguridad de la Información:

Colaborar en la ejecución de la Política de Seguridad de la Información, asegurándose de que el personal de la ARCONEL esté alineado con las prácticas, controles y procedimientos establecidos por la institución para proteger la información.

h) Soporte en la Gestión de Incidentes de Seguridad:

En casos de incidentes relacionados con la seguridad de la información, la Dirección de Administración del Talento Humano debe apoyar en la identificación de las personas involucradas y en la implementación de medidas correctivas, conforme al plan de seguimiento y control de las medidas de mejora y acciones correctivas elaborado por el OSI. Además de colaborar en la capacitación relacionada con la gestión de incidentes.

i) Monitoreo y Registro de Actividades Relacionadas con la Seguridad:

Mantener registros de todas las actividades de capacitación, sensibilización y evaluación en seguridad de la información, asegurando que toda la documentación esté actualizada y disponible para auditorías y revisiones.

2.4.6 Dirección de Tecnologías de la Información y Comunicación

La Dirección de Tecnologías de la Información y Comunicación, tiene las siguientes responsabilidades:

a) Implementación de la Infraestructura Tecnológica Segura:

Garantizar la implementación, mantenimiento y actualización de la infraestructura tecnológica de la ARCONEL, asegurando que todos los sistemas, redes y equipos informáticos sean seguros, estén protegidos contra vulnerabilidades y cumplan con los estándares establecidos en el EGSI.

b) Gestión de la Seguridad de los Sistemas y Redes:

Implementar y supervisar los controles de seguridad de los sistemas y redes de la ARCONEL, incluidos los sistemas de protección contra malware, firewall, detección de intrusiones y sistemas de respaldo, para salvaguardar la integridad y disponibilidad de los datos institucionales.

c) Desarrollo y Gestión de Controles de Acceso:

Definir y gestionar los controles de acceso a los sistemas y recursos informáticos, asegurando que solo el personal autorizado pueda acceder a la información sensible y que se mantenga un registro adecuado de los accesos.

d) Implementación de Políticas de Seguridad de la Información en TIC:

Asegurar que todas las políticas de seguridad de la información sean implementadas y cumplidas en los sistemas y servicios tecnológicos de la institución, en alineación con el EGSI y la Política de Seguridad de la Información de la ARCONEL.

e) Monitoreo y Auditoría de la Seguridad:

Realizar el monitoreo continuo de la infraestructura tecnológica para detectar posibles incidentes de seguridad o actividades sospechosas, y coordinar con el Oficial de Seguridad de la Información (OSI) para la respuesta ante incidentes.

f) Mantenimiento y Actualización de los Sistemas:

Asegurar que todos los sistemas de información y software utilizados en la ARCONEL sean actualizados regularmente, aplicando parches de seguridad y otras medidas necesarias para mitigar riesgos de ciberseguridad.

g) Gestión de los Incidentes de Seguridad:

Actuar como responsable de la gestión de incidentes de seguridad tecnológica, implementando medidas correctivas y realizando análisis post-incidente para prevenir futuros eventos.

h) Implementación de Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP):

Desarrollar, implementar y mantener un Plan de Continuidad de Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), asegurando que los sistemas de información de la ARCONEL puedan recuperarse rápidamente ante cualquier interrupción o desastre.

i) Colaboración en la Concienciación y Capacitación en Seguridad Tecnológica:

Trabajar de manera conjunta con la Dirección de Administración del Talento Humano y el Comité de Seguridad de la Información (CSI) en la creación y ejecución de programas de formación y sensibilización para el personal de la ARCONEL sobre buenas prácticas en seguridad informática.

j) Cumplimiento con la Normativa Legal y Regulatoria:

Asegurar que todos los sistemas y servicios tecnológicos de la ARCONEL cumplan con las leyes y normativas de seguridad de la información, incluidos los requisitos establecidos en la Ley Orgánica de Protección de Datos Personales y las directrices del MINTEL.

2.4.7 Coordinadores y Directores de las gestiones internas de la Agencia

Los Coordinadores y Directores de las gestiones internas de la Agencia, tienen las siguientes responsabilidades:

a) Cumplir con la Política de Seguridad de la Información:

Asegurar que todas las actividades y procesos dentro de sus respectivas áreas sean ejecutados de acuerdo con las directrices establecidas en la Política de Seguridad de la Información de la ARCONEL y el EGSI, promoviendo su cumplimiento entre los miembros de su equipo.

b) Identificación y Gestión de Riesgos Relacionados con la Información:

Colaborar con el Comité de Seguridad de la Información (CSI) y el Oficial de Seguridad de la Información (OSI) para identificar y gestionar los riesgos asociados con la información y los recursos tecnológicos dentro de su área de responsabilidad.

c) Implementación de Controles de Seguridad en sus Áreas:

Implementar controles de seguridad específicos dentro de sus áreas de gestión para proteger los datos e información que manejan, garantizando que se cumplan las medidas de protección de la confidencialidad, integridad y disponibilidad de la información.

d) Supervisión y Evaluación de la Seguridad de la Información en sus Áreas:

Supervisar el cumplimiento de los procedimientos de seguridad en sus respectivas áreas, asegurando que el personal esté debidamente capacitado y sensibilizado sobre la seguridad de la información. Realizar auditorías internas periódicas para verificar la efectividad de las medidas de seguridad implementadas.

e) Colaboración en la Gestión de Incidentes de Seguridad:

Colaborar activamente con la Dirección de Tecnologías de la Información y Comunicación (TIC) y el OSI en la gestión de incidentes de seguridad de la información, asegurando una respuesta rápida y efectiva en caso de que se presenten vulnerabilidades o brechas de seguridad.

f) Garantizar la Confidencialidad de la Información en sus Áreas:

Asegurar que toda la información que maneja su área, especialmente la información confidencial o sensible, sea tratada de acuerdo con las políticas de seguridad de la ARCONEL y las normativas vigentes de protección de datos.

g) Colaboración en el Cumplimiento de Normativas Legales y Regulatorias:

Asegurar que sus equipos cumplan con todas las normativas y leyes relacionadas con la seguridad de la información, incluyendo la Ley Orgánica de Protección de Datos Personales y las normativas establecidas por el MINTEL.

h) Revisión y Actualización de Procedimientos Internos de Seguridad:

Participar en la revisión y actualización de los procedimientos internos relacionados con la seguridad de la información, asegurando que se adapten a los cambios tecnológicos, operativos y normativos.

i) Responsabilidad sobre el Uso Correcto de los Recursos Tecnológicos:

Garantizar que los recursos tecnológicos, incluyendo sistemas informáticos, bases de datos y plataformas, sean utilizados correctamente y de manera segura, previniendo su uso indebido o para fines no autorizados.

2.5. Alcance y usuarios

La Política de Seguridad de la Información de la ARCONEL se aplica a toda la información, ya sea física o digital, que sea recibida, generada o gestionada por los procesos operativos, sustantivos y administrativos de la Agencia. Esto incluye, pero no se limita a, la información que se encuentra bajo la custodia de los servidores de la ARCONEL durante la atención de trámites, en archivos físicos o electrónicos, bases de datos, y recursos tecnológicos utilizados para su almacenamiento. Asimismo, abarca la información que se encuentre en etapa de gestión dentro de los procesos internos de la ARCONEL, así como la custodia y el uso de los activos informáticos relacionados con los sistemas de información.

El alcance de esta política incluye todas las plataformas, aplicaciones y herramientas tecnológicas utilizadas por la ARCONEL, así como la información asociada que pueda encontrarse en servidores, dispositivos de almacenamiento, y comunicaciones electrónicas, ya sea que estén ubicadas dentro de las instalaciones de la Agencia o en servicios externos o en la nube.

Los usuarios de esta política son todos los servidores, funcionarios y empleados de la ARCONEL, así como contratistas, proveedores y terceros que mantengan una relación contractual o de colaboración con la Agencia. Todos estos usuarios deberán cumplir con las normativas y procedimientos de seguridad establecidos en esta política para garantizar la protección adecuada de la información y los activos informáticos de la ARCONEL.

2.6. Comunicación de la Política

La Política de Seguridad de la Información de la ARCONEL será comunicada a todos los servidores y colaboradores de la Agencia mediante los siguientes canales y herramientas de comunicación:

a) Correo Electrónico Institucional: La política será enviada a través del correo electrónico institucional de cada servidor de la ARCONEL, asegurando que todos los empleados reciban la información de manera directa.

b) Página Web Institucional: La Política de Seguridad de la Información estará disponible para su consulta en la página web institucional de la ARCONEL, permitiendo el acceso a cualquier empleado o tercero interesado.

c) Agrupación Virtual de WhatsApp: Se utilizará la agrupación virtual de WhatsApp del personal de la Agencia para enviar recordatorios, resúmenes clave de la política, y mantener una comunicación fluida sobre cualquier actualización o cambio relacionado con la seguridad de la información.

d) Protectores y Fondos de Pantalla: Se implementarán protectores y fondos de pantalla en los equipos informáticos institucionales con mensajes clave de la política, con el fin de reforzar la importancia de la seguridad de la información y mantener la concienciación constante entre los servidores de la ARCONEL.

e) Plataformas de Comunicación Virtual: Se utilizarán otras plataformas virtuales de comunicación interna, como intranet y foros corporativos, para la difusión de la política, así como para la realización de sesiones de capacitación y sensibilización periódicas.

Además, se organizarán sesiones de capacitación y talleres en línea y presenciales para asegurar que todos los servidores comprendan los lineamientos y las responsabilidades derivadas de la política de seguridad.

3. Documentos de referencia

Para la elaboración de la Política de Seguridad de la Información de la ARCONEL, se tomaron como referencia los siguientes documentos y normativas clave:

- Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003: Establece el Esquema Gubernamental de Seguridad de la Información (EGSI), que es el marco normativo obligatorio para todas las entidades del sector público, incluyendo a la ARCONEL.
- Esquema Gubernamental de Seguridad de la Información – EGSI versión 3.0: Documento que

detalla las directrices, requisitos y procedimientos para implementar un sistema de gestión de seguridad de la información en las instituciones gubernamentales, promoviendo la protección de los activos de información.

- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001: Estándar internacional que proporciona los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier organización, siendo un referente esencial para las políticas de seguridad en la ARCONEL.
- Ley Orgánica de Protección de Datos Personales: Establece las normativas legales para la protección de datos personales en Ecuador, y su cumplimiento es fundamental para garantizar la privacidad y seguridad de la información gestionada por la ARCONEL.
- Ley Orgánica de Telecomunicaciones: Regula la seguridad de la información y las comunicaciones en el país, alineando las políticas de la ARCONEL con los estándares legales relacionados con la infraestructura tecnológica y la ciberseguridad.
- Directrices del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL): Establecen las directrices para la gestión de la seguridad de la información en el sector público, proporcionadas por el MINTEL, con el fin de garantizar el cumplimiento de los estándares nacionales en esta materia.

4. Terminología

Para una mejor comprensión de la Política de Seguridad de la Información de la ARCONEL, a continuación se detallan los términos comúnmente utilizados y su respectivo significado:

Activo: Cualquier recurso o elemento que tiene valor para la ARCONEL, incluyendo tanto recursos físicos como digitales, utilizados para el cumplimiento de sus funciones.

Activo de Información: Información, ya sea física o electrónica, que tiene valor para la institución y es necesaria para la toma de decisiones, la ejecución de funciones o la prestación de servicios.

Áreas de Procesamiento de Información: Espacios donde se ubican equipos utilizados para procesar información, como estaciones de trabajo, servidores o dispositivos que permiten gestionar datos de manera operativa.

Áreas Seguras: Espacios que cuentan con una infraestructura tecnológica centralizada, como el Centro de Datos, donde se almacenan y procesan datos sensibles y de alto valor para la ARCONEL, con medidas adicionales de seguridad.

Autenticación: El proceso de verificar la identidad de un usuario o sistema para garantizar que las solicitudes de acceso sean legítimas.

Autenticidad: Garantizar que la información proviene de una fuente validada y fiable, asegurando que los datos no han sido alterados y que el origen de la información es correcto.

Confianza: La capacidad de confiar en que la información y los sistemas operativos son adecuados para sustentar la toma de decisiones y las funciones institucionales, de acuerdo con los estándares establecidos.

Equipos de Procesamiento: Todos los dispositivos informáticos que permiten el procesamiento de

datos, como computadoras de escritorio, laptops, servidores y otros equipos utilizados en las operaciones de la ARCONEL.

Hardware: La parte física de los dispositivos tecnológicos, incluidos los componentes electrónicos, computadoras y equipos de telecomunicaciones.

Información: Conjunto de datos organizados y procesados que tienen valor para la toma de decisiones, que puede ser en forma de texto, imágenes, audios, videos, bases de datos u otros formatos, almacenados en cualquier medio.

Internet: Red global de computadoras que permite el acceso a información y servicios en línea, como correo electrónico, sitios web, almacenamiento de datos en la nube, y otros servicios asociados.

No Repudio: Mecanismo para asegurar que ninguna de las partes involucradas en una transacción de información pueda negar haber realizado dicha acción, garantizando la integridad del proceso.

Legalidad: Cumplimiento de todas las leyes, normativas y disposiciones legales aplicables a la ARCONEL, especialmente aquellas relacionadas con la protección de la información y la privacidad de los datos.

Protección contra Duplicación: Mecanismo para evitar que una transacción o solicitud se realice más de una vez, asegurando la exactitud y validez de los datos procesados.

Redes: Infraestructura de comunicaciones que permite la interconexión de sistemas y equipos, incluyendo tanto la parte física (cableado, enrutadores, switches) como los sistemas lógicos (redes de datos, voz, video y dispositivos de almacenamiento).

Responsable de los Activos de Información: Persona designada dentro de cada área para ser el custodio de los activos de información, tanto en formato físico como digital, y encargada de mantener actualizado el inventario de la información de su área.

Seguridad de la Información: Conjunto de prácticas, políticas y medidas de protección que se implementan para garantizar las siguientes características de la información de la ARCONEL:

Confidencialidad: Garantizar que la información esté accesible solo a las personas autorizadas para su uso.

Integridad: Asegurar que la información no sea alterada o modificada sin autorización, manteniendo su exactitud y completitud.

Disponibilidad: Garantizar que la información esté disponible y accesible para los usuarios autorizados siempre que lo necesiten.

Sistemas de Información: Conjunto de recursos organizados que incluyen tecnologías, procesos y personas, destinados a la recopilación, procesamiento, almacenamiento y difusión de información relevante para la ARCONEL.

Software: Conjunto de programas y aplicaciones utilizadas para realizar tareas específicas dentro de la ARCONEL, tales como la gestión de datos, procesamiento de información, administración de recursos y otros.

Tecnología de la Información (TI): Conjunto de tecnologías, sistemas y herramientas que procesan y gestionan información, incluyendo tanto hardware como software, utilizados por la ARCONEL para realizar sus funciones y servicios institucionales.

Usuario(s): Cualquier persona, interna o externa, que tenga acceso autorizado a los sistemas de información de la ARCONEL, y que esté sujeta a las políticas y controles establecidos para garantizar la seguridad de la información.

Versión	Fecha	Detalle de la modificación
1.0	30/09/2025	Documento inicial.

5. Firmas de responsabilidad

	Responsable	Fecha	Firma
Elaborado por:	Mgs. Hector William López Torres **Oficial de Seguridad de la Información OSI – ARCONEL**	02 /10/2025	Firmado electrónicamente por: HECTOR WILLIAM LOPEZ TORRES Validar únicamente con FirmaEC
Revisado por:	Ing. Gabriela Patricia Moreno Villacís **Director de Planificación, Inversión, Seguimiento y Evaluación**	02/10/2025	Firmado electrónicamente por: GABRIELA PATRICIA MORENO VILLACIS Validar únicamente con FirmaEC
Aprobado por:	Dr. Augusto Fabricio Porras Ortiz **Director Ejecutivo Encargado**	03/10/2025	Firmado electrónicamente por: AUGUSTO FABRICIO PORRAS ORTIZ Validar únicamente con FirmaEC