Documento impreso – copia no controlada

★★★★★

POLITICA
SEGURIDAD DE LA INFORMACIÓN
INFORMACIÓN INTERNA

Versión de publicación:	4	**Entrada en vigencia:**	30/11/2023
Código:	POLI-00025	**Publicación:**	30/11/2023
Elaborado por:	Fernando Andrés Muñoz Araneda	**Vencimiento:**	29/11/2026
Cargo:	Jefe Seguridad de la Información		

Revisado por:	Gerardo Gabriel Yoppi Llombart	**Aprobado por:**	Francisco José Alliende Arriagada
Cargo:	Jefe Área Procesos y Certificaciones	**Cargo:**	Gerente General
		Aprobado por:	Sebastian Renato Saez Rees
		Cargo:	Gerente Legal

1. OBJETIVO

Establecer los lineamientos en torno a la seguridad de la información en el Grupo Saesa, con el objetivo de asegurar su adecuada integración a los procesos, estructura organizacional, gestión de riesgos y medidas de protección contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información de la Compañía.

2. ALCANCE Y APLICACIÓN

El alcance de esta política abarca desde el sistema de gestión, hasta los principios de seguridad de la información.
Esta política es de conocimiento y aplicación obligatoria para todos los trabajadores del Grupo Saesa y empresas contratistas.

3. DEFINICIONES

3.1 Activo de Información:

Conjunto de registros intangibles que se pueden encontrar en un medio físico y/o digital y que tiene un nivel de importancia para la Compañía.

Fuente: Área Seguridad de la Información

3.2 Amenaza:

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a las personas, a un sistema u organización, al medio ambiente o a la comunidad.

Fuente: Área Seguridad de la Información

3.3 Confidencialidad:

Necesidad de ocultar o mantener secreto sobre determinada información o recursos, con el objetivo de prevenir la divulgación no autorizada de la información.

Fuente: Área Seguridad de la Información

3.4 Disponibilidad:

Condición de la información donde ésta se mantiene accesible a elementos autorizados, con el objetivo de prevenir interrupciones no autorizadas sobre la información.

Fuente: Área Seguridad de la Información

3.5 Información:

Se entiende como información a toda forma proveniente de datos relacionados con los procesos del Grupo Saesa, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Fuente: Área Seguridad de la Información

3.6 Información confidencial:

Toda información o conocimiento, cualquiera sea su naturaleza, medio o forma, que la empresa considere privada o restringida, y que no sea de conocimiento común fuera del negocio, o que las leyes o un contrato exijan mantener en calidad de confidencial; y que en caso de divulgación pudiere ser de utilidad a los competidores o perjudicial para un negocio del Grupo Saesa, o que ésta tenga la intención que se desarrolle, pague por su desarrollo y/o sobre la cual tenga un derecho de exclusividad.

Fuente: Área Seguridad de la Información

3.7 Incidente de seguridad de la información:

Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad de la información.

Fuente: Área Seguridad de la Información

3.8 Integridad:

Condición de la información donde ésta se mantiene inalterada ante accidentes o intentos maliciosos, con el objetivo de prevenir modificaciones no autorizadas de la información.

Fuente: Área Seguridad de la Información

3.9 Riesgo:

Efecto de la incertidumbre sobre los objetivos. Los riesgos están insertos en los procesos de la compañía, estos no sólo generan incertidumbres negativas en sus efectos, sino también detectan oportunidades que pueden ser utilizadas en beneficio de la compañía.

Fuente: Área Seguridad de la Información

3.10 Seguridad de la información:

Es el nivel de confianza que la Compañía desea tener en base a su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger los activos de información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir con la misión y objetivos estratégicos de la Compañía.

Fuente: Área Seguridad de la Información

3.11 Gobierno de Datos:

Es el ejercicio de la autoridad y el control (planificación, el seguimiento y la aplicación) a través de la gestión de los activos de datos.

Fuente: Área Seguridad de la Información

3.12 NERC CIP:

North American Electric Reliability Corporation - Critical Infraestructure Protection.

Fuente: Área Seguridad de la Información

4. DESARROLLO

4.1. Sistema de Gestión de Seguridad de la Información

La Gerencia General establece la política de seguridad de la información al alero del Sistema de Gestión de Seguridad de la Información (SGSI). Con ello, la alta dirección se compromete a dar cumplimiento a los requisitos aplicables al SGSI que se relacionen a la seguridad de la información y a la mejora continua del mismo sistema de gestión, a fin de mantener un nivel de seguridad cada vez más robusto y acorde a las necesidades de la Compañía.

4.2. Del Gobierno de Seguridad de la Información

Para el Grupo SAESA, el Gobierno de Seguridad de la Información, en adelante GSI, es fundamental a la hora de proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad. Es por ello, que el Grupo SAESA, adopta como marco referencial para su GSI, los principios y directrices basados en el modelo de las “Tres Líneas de defensa” definidas por el Instituto de Auditores Internos, (IIA). Fijando de esta manera un marco de trabajo que asegure la concordancia con los objetivos estratégicos de la organización, definiendo claramente las responsabilidades, controles y las medidas necesarias en cada una de las líneas, con la finalidad de proteger la información de la organización contra amenazas internas y externas; velando, además, por el cumplimiento del marco normativo y regulatorio aplicable en materia de seguridad de la información.

4.3 Del Gobierno de Datos

La gestión de información en el Grupo Saesa se conforma a partir de un conjunto de áreas de conocimiento que buscan maximizar el valor de ésta, encargándose de su gestión, calidad, almacenamiento y respaldo, transformación, uso y resguardo. Como parte de ese conjunto, la seguridad de la información asume la responsabilidad de resguardar la integridad, confidencialidad, disponibilidad y el cumplimiento de acuerdos contractuales derivados de los datos dentro de la Compañía a través de procesos de autenticación, autorización, acceso y auditoría de los activos de información. De manera coordinada, esta área en conjunto con otras, constituyen el Gobierno de Datos, el cual entrega la visión estratégica de cada parte de este conjunto de disciplinas.

4.4 Del estándar de Ciber Seguridad NERC CIP.

El Grupo SAESA, en lo relativo a su rol dentro del Sistema Eléctrico Nacional, manifiesta su adhesión a la Política Nacional de Ciberseguridad, y al cumplimiento del estándar NERC CIP para la protección de su infraestructura crítica.

4.5. Objetivos de Seguridad de la Información

Los objetivos de seguridad de la información abarcan cuatro perspectivas de interés para el Grupo Saesa:

4.5.1. Operacional

Reducir el impacto en los procesos de la Compañía y en los mismos activos de información ante incidentes de seguridad de la información.

4.5.2. Legal / Regulatorio

Minimizar el impacto por incumplimiento a lo estipulado y dictaminado por la autoridad y/o regulador.

4.5.3. Reputacional

Evitar una percepción negativa por parte de los Clientes del Grupo Saesa.

4.5.4. Financiero

Reducir la provisión de capital por concepto de multas o pérdidas financieras asociadas a incidentes de seguridad de la información.

4.4. Principios de seguridad de la información

- El tratamiento sobre los activos de información por parte de Colaboradores del Grupo Saesa debe ser consecuente con la presente política, sus derivadas (ver anexo 8.1) y los mismos procedimientos, instructivos y manuales formalizados.
- Los activos de información deben ser protegidos adecuadamente, de acuerdo con su importancia a su organización, en relación con el compromiso con requisitos legales / regulatorios, su valor, criticidad y sensibilidad. Es por ello por lo que, la Gerencia General provee los recursos que permitan la implementación de controles de seguridad de la información acorde al nivel de riesgo existente.
- Los activos de información deben estar clasificados y etiquetados a través de un proceso formal y documentado (ver capítulo 5) que considera cuatro perspectivas: financiera, legal / regulatorio, operacional y reputacional. El resultado de la clasificación del activo de información puede ser:

CLASIFICACIÓN (*)	CRITERIO
Información "Pública"	Información de libre conocimiento y/o modificación.
Información "Interna"	Información de conocimiento y/o modificación para solo personal del Grupo Saesa o contratistas con cláusulas de no divulgación pactada en contrato.
Información "Condicionada"	Información de conocimiento y/o modificación condicionada a la autorización de quien aplique.
Información "Restringida"	Información de conocimiento y/o modificación limitada a una doble autorización.

- El Grupo Saesa debe proveer los mecanismos para que la información pueda ser de acceso de los trabajadores y utilizada por éstos cuando en relación con sus funciones así lo requieran. Sin embargo, se reserva el derecho de revocar a los trabajadores, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten.
- Los activos de información deben pertenecer a un dueño que para efectos de esta política se denomina "Propietario de la Información". También existen roles asociados a la custodia de la información, responsables de proveer almacenamiento y protección a la información que custodian; dicho rol puede ser asumido por el mismo Propietario de la Información, como también por la Gerencia de Tecnologías de la Información (información de las tecnologías informáticas), Área SCADA y Área Desarrollo Operacional (información de las tecnologías operacionales) y el Área Administración de infraestructura (Bodega documental).
- Tanto la información proveniente desde una fuente de información externa como interna que se encuentra custodiada por el Grupo Saesa, es susceptible a los controles de seguridad de la información documentados de acuerdo con el nivel de clasificación.
- El Grupo Saesa se reserva el derecho de auditar en todo momento y sin previo aviso el cumplimiento de las políticas, procedimientos, instructivos, manuales y planes vigentes y que dicen relación con la seguridad de la información de la Compañía.
- La Gerencia General procura que los Colaboradores reciban el entrenamiento suficiente en materia de seguridad de la información, consistente con sus necesidades y su rol dentro del Grupo Saesa. Además, la Gerencia General realiza revisión de esta política una vez al año, con el objetivo de asegurarse la pertinencia de este documento bajo el contexto actual y al objetivo de la organización.
- El Grupo Saesa define roles y responsabilidades para los Colaboradores del Grupo Saesa, de acuerdo con las necesidades de la Compañía, la estructura organizacional y las funciones de cada cargo (ver capítulo 5). Además, existe una segregación de funciones que busca reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de información.
- Los Colaboradores del Grupo Saesa deben utilizar la información y los activos asociados a este de acuerdo con el propósito de su labor en la Compañía aplicando criterios de buen uso en su utilización. También debe considerar las obligaciones emanadas de las demás políticas de seguridad

de la información, tales como de control de acceso, respaldos, transferencia de información, ente otros (ver capítulo 5).

- Con el objetivo de una correcta integración de la política en la cultura organizacional, el Grupo Saesa gestiona un plan formal de concientización y capacitación en cuanto a seguridad de la información se refiera que también incluye la difusión de la presente política.

5. DOCUMENTOS RELACIONADOS

Documentos Internos

Tipo de documento:	Manual
Nombre del documento:	Sistema de gestión de seguridad de la información del Grupo Saesa
Código:	MANU-00033

Tipo de documento:	Politica
Nombre del documento:	Control y acceso lógico TO
Código:	POLI-00044

Tipo de documento:	Politica
Nombre del documento:	Control de acceso lógico al SMMC
Código:	POLI-00010

Tipo de documento:	Politica
Nombre del documento:	Control de acceso lógico TI
Código:	POLI-00045

Tipo de documento:	Politica
Nombre del documento:	Seguridad de la información para las relaciones con el proveedor
Código:	POLI-00019

Tipo de documento:	Politica
Nombre del documento:	Desarrollo seguro
Código:	POLI-00043

Tipo de documento:	Politica
Nombre del documento:	Gestión de vulnerabilidades técnicas
Código:	POLI-00039

Tipo de documento:	Politica
Nombre del documento:	Respaldo de información
Código:	POLI-00027

Tipo de documento:	Politica
Nombre del documento:	Emplazamiento y protección de equipos
Código:	POLI-00041

Tipo de documento:	Procedimiento
Nombre del documento:	Administrar inventario de activos de información
Código:	PROC-01176

Documentos externos

No existen documentos externos relacionados.

6. CONTROL DE REGISTROS

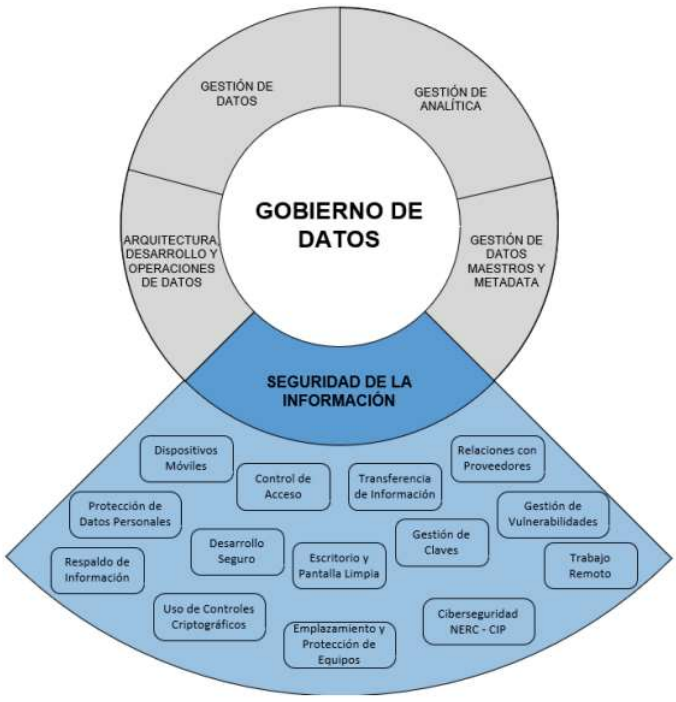
En este documento no se visualizan registros.

7. CONTROL DE MODIFICACIONES

Versión	Publicación	Entrada en vigencia	Vencimiento	Deroga a	Modificación
1	10/01/2014	16/01/2014	*Sin Datos*	*N/A*	Versión inicial.
1	02/10/2015	02/10/2015	*Sin Datos*	*N/A*	Esta versión corresponde a 1.1. Se complementa el capítulo de clasificación de la información. Se agrega el capítulo sobre la entrega de recursos en desuso. Se elimina el capítulo de documentos relacionados.
2	08/11/2019	08/11/2019	*Sin Datos*	*N/A*	Ser realizan cambios mayores en el documento modificando la estructura del documento o incorporando los siguientes capítulos: - Del Gobierno de datos - De la información Interna - De la información de los Usuarios externos - Difusión de la política - Segregación de funciones y - Esquema de Política Seguridad de la Información y sus Políticas Relacionadas
3	05/11/2021	05/11/2021	01/12/2024	*N/A*	Actualizar versión 2.0 Se modifica esquema de clasificación de información y se quitan roles y responsabilidades que quedan en el anexo correspondiente. También se agregan al esquema de políticas la relacionada al Estándar de Ciberseguridad para el Sector Eléctrico.
4	30/11/2023	30/11/2023	29/11/2026	*N/A*	Se agrega capítulo de Gobierno de Seguridad de la Información basado en el modelo de las “Tres Líneas”, (IIA), Instituto Internacional de Auditores.

8. ANEXOS

8.1 ESQUEMA “POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN Y RELACIONADAS”



8.2 MODELO DE LAS TRES LÍNEAS DE DEFENSA DEL IIA 2020

Primera línea de defensa

En el ámbito de la seguridad de la información, la primera línea de defensa está representada por los dueños o responsables de los activos de información en las distintas áreas de negocio. Estos responsables incluyen a los gerentes y colaboradores que operan en las diferentes áreas de la organización, siendo su principal responsabilidad, asegurar que los activos de información estén protegidos adecuadamente y que se implementen los controles de seguridad necesarios para mitigar posibles amenazas de riesgo.

Los responsables de la primera línea de defensa deben:

- Identificar y gestionar los riesgos de seguridad de la información en sus áreas de responsabilidad.
- Implementar controles de seguridad apropiados y asegurarse de que se sigan los estándares y procedimientos establecidos.
- Promover la conciencia y la capacitación en seguridad de la información entre su equipo y garantizar el cumplimiento de las políticas y controles establecidos.
- Informar cualquier incidente de seguridad de la información detectado y colaborar en su resolución.

Segunda línea de defensa

La segunda línea de defensa está representada por las funciones del Jefe de Seguridad de la información y del Comité de Seguridad de la Información, (CSI). Estas funciones tienen la responsabilidad de brindar supervisión, orientación y apoyo a la primera línea de defensa, asegurando que se implementen controles de seguridad de manera efectiva y se cumplan los requisitos normativos y legales.

Estas funciones implican:

- Establecer políticas, estándares y procedimientos de seguridad de la información que sean aplicables a toda la organización.
- Proporcionar asesoramiento y apoyo en la implementación de controles de seguridad de la información en las diferentes áreas de negocio.
- Realizar evaluaciones periódicas de riesgos y controles para monitorear el cumplimiento de las políticas y estándares establecidos.
- Mantener actualizada sobre las mejores prácticas y las nuevas amenazas y vulnerabilidades en el campo de la seguridad de la información, y ajustar las políticas y controles en consecuencia.

Tercera línea de defensa

La tercera línea de defensa en el contexto de la seguridad de la información está representada por la función de auditoría interna. Tiene la responsabilidad de proporcionar una evaluación objetiva e independiente de los sistemas de gestión de seguridad de la información y los controles implementados.

La función de auditoría interna o auditoría de seguridad debe:

- Realizar auditorías internas periódicas para evaluar la conformidad con las políticas y controles establecidos.
- Evaluar la efectividad de los controles de seguridad de la información implementados en toda la organización.
- Emitir informes de auditoría con recomendaciones para mejorar los procesos y prácticas de gestión de riesgos y seguridad de la información.
- Monitorear la implementación de las recomendaciones de auditoría y realizar un seguimiento para verificar su efectividad.

La primera línea comprende a los responsables de los activos de información en diversas áreas de la organización, quienes tienen la responsabilidad principal de proteger adecuadamente los activos y mitigar riesgos. Esto implica identificar y gestionar riesgos, implementar controles de seguridad, promover conciencia y capacitación, así como informar y colaborar en la resolución de incidentes.

La segunda línea está representada por el Oficial de Seguridad de la Información y el Comité de Seguridad de la Información. Estas funciones supervisan, orientan y respaldan a la primera línea, asegurando la efectiva implementación de controles de seguridad, el cumplimiento normativo y legal, y estableciendo políticas, estándares y procedimientos aplicables a toda la organización. Además, realizan evaluaciones periódicas de riesgos y controles, manteniéndose actualizados sobre las mejores prácticas y amenazas emergentes.

La tercera línea, la auditoría interna, proporciona una evaluación objetiva e independiente de los sistemas de gestión de seguridad de la información y los controles implementados. Realiza auditorías periódicas para evaluar la conformidad con políticas y controles, evalúa la efectividad de los controles en toda la organización, emite informes con recomendaciones para mejorar prácticas de gestión de riesgos y seguridad de la información, y realiza un seguimiento para verificar la implementación efectiva de dichas recomendaciones.