POLÍTICAS COMPLIANCE

POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

CS Energy	CS Energy	CS Energy

1. INTRODUCCIÓN

En CS Energy, entendemos que el desarrollo de nuestras actividades implica un alto grado de responsabilidad en cuanto al cumplimiento normativo, la ética y la integridad empresarial. Como empresa líder en el mercado, reconocemos que nuestra interacción con los diversos actores requiere un actuar transparente y alineado con los valores y principios fundamentales que rigen nuestra organización, y que nos han permitido construir la reputación que tiene hoy nuestra empresa.

Reconocemos que la información es uno de nuestros activos más valiosos, cuya adecuada protección resulta esencial para la continuidad operativa, la sostenibilidad del negocio y el resguardo de nuestra reputación. Dada la naturaleza de nuestras operaciones, estamos expuestos a riesgos relevantes relacionados con la fuga, pérdida o manipulación indebida de información confidencial, tanto propia como de nuestros clientes y socios comerciales.

Por ello, asumimos el compromiso de garantizar la confidencialidad, integridad y disponibilidad de la información que gestionamos, mediante un enfoque sistemático de seguridad basado en estándares internacionales y mejores prácticas.

2. OBJETIVOS

Esta política establece las directrices para implementar un sistema efectivo de seguridad de la información, con los siguientes propósitos:

- **Proteger** la información estratégica de CS Energy y de nuestros clientes contra el acceso, uso, divulgación o destrucción no autorizados.
- **Asegurar** la integridad y disponibilidad de los sistemas clave para la operación.
- **Establecer** responsabilidades claras para la gestión de la seguridad de la información.
- **Prevenir** la comisión de delitos informáticos.

3. ALCANCE

Esta política es de cumplimiento obligatorio para todos los directores, gerentes, colaboradores, y se extiende a terceros que manejen información de CS Energy, como contratistas y proveedores de servicios. Cubre la información en cualquier formato, digital o físico, y en cualquier etapa de su ciclo de vida.

4. DEFINICIONES

4.1. Activos de información: Cualquier información que tiene valor para la empresa y/o para sus proveedores y clientes, independiente del soporte en el que se encuentre, así como todos los dispositivos, equipos, software, tecnología, redes, servicios, medios, procedimientos y otros bienes, tangibles o intangibles, que procesan, almacenan, mantienen, protegen o controlan el acceso a la información dentro la organización.

4.2. Confidencialidad: Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.

4.3. Integridad: Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de asegurar la exactitud y completitud de los activos de información.

4.4. Disponibilidad: Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.

4.5. Incidente de seguridad de la información: Evento, o serie de eventos, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.

Clasificación del acceso y uso de la información

4.6. Pública: Información disponible para cualquier persona y puede ser divulgada libremente.

4.7. Interna: Información disponible para todos los colaboradores y colaboradoras de CS Energy Sólo internos de la empresa pueden acceder y compartir esta información con terceros previa autorización de quien se encuentre facultado para hacerlo.

4.8. Confidencial: Información creada o procesada por la organización, ya sea interna, de proveedores o de clientes, a la cual tienen acceso sólo determinadas personas de la empresa. Se otorgará acceso a la información confidencial sólo a quienes sea necesario en virtud de las funciones de su cargo, y estén sujetos a obligaciones de confidencialidad debidamente estipuladas en contratos u otros reglamentos aplicables. Está prohibida la divulgación de esta información, salvo con autorización previa, expresa y escrita por quien tenga dicha potestad.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Principios rectores

Confidencialidad: La información será accesible únicamente para quienes estén autorizados, conforme a su perfil de acceso, evitando su divulgación, pérdida o exposición a terceros no autorizados.

Integridad: Los datos deben mantenerse precisos, completos y protegidos contra modificaciones no autorizadas.

Disponibilidad: La información estará disponible para su uso legítimo, minimizando interrupciones.
Cumplimiento normativo: Todas las actividades relacionadas con la gestión de la información cumplirán con las normativas aplicables y estándares internacionales.

Control de Acceso Todas las cuentas deberán ser desactivadas dentro de un plazo máximo de 72 horas cuando un colaborador cese funciones, para garantizar el cumplimiento de controles exigidos en materia de ciberseguridad en Chile.

- Sistemas críticos: El acceso a sistemas y software de gestión se basará en el principio de "mínimo privilegio", donde solo se dará acceso a lo estrictamente necesario para cada cargo. Las Gerencias deben revisar estos permisos con TI una vez al año.
- Gestión de la nube:
  - Se prohíbe el uso de cuentas personales de Drive o Gmail para almacenar o compartir información confidencial.
  - El Encargado de TI debe revisar los permisos de las carpetas compartidas de proyectos y subcontratistas para asegurar que los externos no tengan acceso a información interna de CS Energy.

Responsabilidad en el uso de tecnologías
El uso de la información y las tecnologías asociadas debe estar exclusivamente limitado a los servicios que ofrece CS Energy y contar con la autorización previa de los supervisores facultados. Las credenciales de acceso a sistemas, incluidas contraseñas y claves, son personales, intransferibles y de responsabilidad exclusiva de su titular. Solo los colaboradores autorizados pueden hacer uso de sus credenciales. Cualquier uso indebido será responsabilidad del infractor, quien deberá asumir las consecuencias ante la empresa y ante las autoridades regulatorias que correspondan.

Gestión responsable de credenciales y equipos Se deberán actualizar las contraseñas al menos cada 90 días para fortalecer la protección frente a delitos informáticos.

- Las credenciales de acceso (usuarios, contraseñas, claves, tokens, etc.) son estrictamente personales, intransferibles y deben ser protegidas con diligencia. Su uso indebido conlleva responsabilidades disciplinarias y legales para el infractor.
- El correo corporativo (@csenergy.cl) es una herramienta oficial de comunicación y debe utilizarse exclusivamente con fines laborales, garantizando la precisión de los contenidos y la correcta identificación de los destinatarios. Cualquier uso inapropiado será considerado una falta grave. Este correo electrónico representa a CS Energy frente a terceros y es propiedad de la empresa, por lo que su uso debe ser responsable y ético.
- Los notebooks y celulares de la empresa deben tener contraseña y no deben dejarse desatendidos en lugares públicos (ej. obras, vehículos).

Protección de información confidencial Queda estrictamente prohibido almacenar información confidencial en dispositivos personales, incluyendo celulares particulares, pendrives no corporativos o servicios de nube no autorizados.
Está prohibida la divulgación, réplica o uso no autorizado de información clasificada como confidencial, reservada o secreta, salvo autorización expresa, documentada y conforme a los protocolos internos. Esta restricción aplica también a conversaciones informales o canales no autorizados.
Los documentos físicos confidenciales (planos, ofertas, entre otros) no deben dejarse a la vista en escritorios o impresoras. Deben ser guardados bajo llave o destruidos (triturados) si ya no se necesitan.

Control de acceso físico

Toda persona autorizada a ingresar a instalaciones o sistemas de CS Energy deberá registrar su acceso y respetar las áreas restringidas. El incumplimiento de estas directrices puede afectar la integridad de nuestras operaciones y comprometer la seguridad de nuestros clientes y aliados.

Gestión de Incidentes de Seguridad Todo incidente deberá ser registrado en el Registro de Incidentes dentro de un máximo de 24 horas desde su detección, asegurando trazabilidad y permitiendo la activación oportuna de medidas de mitigación.
Los incidentes de seguridad de la información en CS Energy deben ser reportados y gestionados conforme a las siguientes reglas:

a) Todo colaborador/a tiene la obligación de reportar inmediatamente al Compliance Officer cualquier sospecha o incidente relacionado con la seguridad de la información, independientemente de si

fue causado por ellos o no. Para esto, deberán utilizar los medios de comunicación definidos por la empresa, como el correo electrónico institucional del Compliance Officer.
Además de los incidentes ocurridos dentro de CS Energy, se debe estar atento a aquellos que puedan afectar a proveedores o a cualquier otro tercero que mantenga relaciones comerciales o de colaboración con la empresa.

b) El Compliance Officer, o la persona designada por él, será responsable de gestionar los incidentes reportados. Esto incluye evaluar la gravedad del incidente para determinar las acciones correctivas necesarias. Según la severidad del caso, se activarán los mecanismos de respuesta correspondientes, y se realizará un seguimiento detallado para asegurar que las medidas implementadas hayan sido efectivas y que el riesgo haya sido mitigado. Este proceso busca garantizar la protección continua de los activos de información de CS Energy y de los terceros vinculados, fortaleciendo la confianza e integridad en las operaciones de la empresa.

c) El Compliance Officer será además responsable de dejar un registro detallado de todos los incidentes de seguridad sobre los que se tenga conocimiento, a fin de documentar de manera sistemática todos los eventos que comprometan la seguridad de la información y los activos de la organización. Esto permite un análisis adecuado, facilita la implementación de acciones correctivas y contribuye a la mejora continua de los controles de seguridad. El Registro de Incidentes de Seguridad se encuentra en el Anexo Nº1 de esta Política.

Se llevará a cabo un seguimiento detallado para asegurar la efectividad de las medidas implementadas y mitigar los riesgos asociados. Este proceso busca mantener la protección continua de los activos de información de CS Energy y de sus socios estratégicos, fortaleciendo la integridad y confianza en las operaciones de la empresa.

6. MONITOREO Y ACTUALIZACIÓN

Esta Política deberá ser revisada por el Compliance Officer una vez al año o cuando sea necesario producto de cambios normativos, en las prácticas de la empresa o en caso de incidentes relacionados a este tema. En esta revisión se determinará si es necesario o no actualizar la Política.

7. CONTROL DE CAMBIOS

N° Versión	Fecha entrada en vigencia	Modificación
000	15.01.2026	Versión inicial

8. ANEXOS

8.1. Registro de incidentes de seguridad

ANEXO 1

REGISTRO DE INCIDENTES DE SEGURIDAD

Nº DE INCIDENTE	FECHA Y HORA DETECCIÓN	REPORTADO POR	ÁREA AFECTADA	DESCRIPCIÓN INCIDENTE	IMPACTO	CLASIFICACIÓN	ACCIONES INMEDIATAS	RESPONSABLE	ESTADO

Instrucciones:

1. Asignar un número de incidente único para facilitar el rastreo.
2. Documentar la fecha y hora en que se detectó el incidente.
3. Identificar a la persona o equipo que reportó el incidente.
4. Especificar el área o sistema afectado.
5. Describir de manera clara y concisa el incidente.
6. Evaluar el impacto inicial (bajo, medio, alto).
7. Clasificar el incidente (acceso no autorizado, malware, fuga de información, etc.).
8. Registrar las acciones inmediatas tomadas para mitigar el impacto.
9. Asignar un responsable para el seguimiento del incidente.
10. Actualizar el estado del incidente (abierto, en investigación, cerrado).