1. Alcance

Esta política establece las directrices para la seguridad de la información en todo Sencinet.

Protegemos la confidencialidad, integridad y disponibilidad de nuestra información y activos.

Los protegemos de ataques maliciosos, fugas deliberadas, pérdida accidental y cualquier otra cosa en el medio. Las amenazas son reales y pueden venir tanto del interior como fuera de la organización, así que todos tenemos que ser conscientes del papel que desempeñamos en la protección de nuestro negocio.

La presente política se publica y se comunica a todos. Es propiedad del foro de seguridad y se revisa al menos cada año para asegurarse de que sigue cumpliendo con los requisitos, así como con nuestros objetivos de negocio como se describe en el Sistema de Gestión de Seguridad de la Información (ISMS).

Se aplica a todos los que trabajan para Sencinet.

2. Declaración del CISO

Lo Que Creemoss

Tratamos con una gran cantidad de información sobre nuestros clientes, nuestros empleados y nuestra empresa todos los días. Somos responsables de mantenerla segura, porque además de la regulación, la legislación, somos una empresa de servicios de ciberseguridad y debemos cuidar los pilares de integridad, confidencialidad y disponibilidad.

Por Qué esto es Importante

La seguridad de la información debe permear todas las áreas de la empresa, las acciones que realizamos en nuestro día a día corporativo deben estar alineadas con las políticas y procesos definidos. Estar atentos a las señales y posibles amenazas es responsabilidad de todos.

Nuestro Enfoque Es Simple

La política de seguridad de la información debe ser entendida, aceptada y aplicada por todos.

El área de Gobernanza establece deberes y responsabilidades en materia de seguridad de la información.

La seguridad de los datos también es un requisito legal y existen severas sanciones para las personas y empresas que violen estos requisitos.

Gustavo Duani – CISO Sencinet

3. Quién es el responsable

La presente política se aplica a cualquier persona que trabaje para, o, en nombre de Sencinet, que maneje información de Sencinet.

Debe leer y comprender los requisitos de la presente política, incluidas las otras políticas y normas asociadas, y adherirse a la mismas y al Código de Ética y Conducta de Sencinet. El incumplimiento de la presente política puede dar lugar a medidas disciplinarias y, en casos graves, al despido. También podría traer problemas con la ley. Hay sanciones graves para cualquier persona, o cualquier empresa, que viole la ley, incluyendo multas ilimitadas y encarcelamiento.

Los gerentes son responsables de asegurarse de que su gente esté familiarizada y cumpla con los requisitos de la presente política y las otras políticas y normas asociadas.

Podemos cambiar la presente política, cuando sea requerido, sujeto a procesos de consulta acordados.

Protegemos la información y mantenemos seguros los activos de la Compañía.

Valoramos la confidencialidad de toda la información en poder de la Compañía, ya sea de clientes, proveedores, socios comerciales o propios.

Prohibimos el uso de información privilegiada obtenida en servicio para la empresa, para obtener ganancias personales indebidas.

La información confidencial no debe divulgarse ni discutirse deliberadamente. Debe reservarse para casos de requisitos comerciales y/o legales.

4. Nuestros principios

La estrategia general de gestión de Sencinet con respecto al programa de seguridad de la información se detalla en el Manual del Sistema de Gestión de Seguridad de la Información (ISMS), incluyendo funciones y responsabilidades.

El Manual ISMS y todo el marco de referencia, se revisará periódicamente con el objetivo de mejorar continuamente.

5. Directrices de la política

5.1. Todas las políticas de seguridad, estándares, programas, procesos y directrices se documentarán, mantendrán, publicarán y deberán:

a. Abordar todos los requisitos legales, reglamentarios, comerciales y contractuales aplicables.

b. Para las Políticas de Seguridad que se derivan de la presente política (ver sección 6) se deben realizar como mínimo, revisiones y actualizaciones cada 2 (dos) años o cuando el entorno cambie. Para la presente Política de Seguridad que incluye un compromiso con el cumplimiento de requisitos asociados a PCI-DSS, esta revisión deberá realizarse como mínimo una vez al año.

c. Definir claramente las responsabilidades de seguridad de la información para todos los que trabajan para Sencinet.

5.2. Asegurar la confidencialidad de la información.

5.3. Mantener la integridad de la información.

5.4. Mantener la disponibilidad de información para los procesos del negocio.

5.5. Mantener todos los controles apropiados para asegurar nuestras instalaciones de procesamiento de información.

5.6. Designar a todos los activos informativos en poder de Sencinet, un propietario en nombre de la empresa.

5.7. Definir una política relativa al uso aceptable de los sistemas de información y la información misma.

5.8. Proteger la información contra el acceso o uso no autorizados.

5.9. Clasificar la información de acuerdo con su valor y sensibilidad relativa al negocio y la pérdida o exposición potencial.

5.10. Manejar toda la información en función de su clasificación durante su ciclo de vida (tal como creación, almacenamiento, acceso, procesamiento, distribución, transmisión y eliminación).

5.11. Mantener capacitación en concienciación sobre la seguridad de la información de manera obligatoria para todos los empleados.

5.12. Distribuir la información a los empleados, contratistas y terceros sobre una base de "necesidad comercial".

5.13. Aplicar todos los controles apropiados al procesar información con terceros.

5.14. Desarrollar procedimientos operativos de seguridad para controlar la aplicación de nuestras políticas de seguridad de la información, estándares, obligaciones legales y regulatorias.

5.15. Reportar, investigar y remediar todas las infracciones de seguridad de la información reales o sospechosas.

5.16. Evaluar y dirigir la seguridad de nuestro negocio, incluidos todos nuestros servicios y procesos, para garantizar que se identifiquen los riesgos, y se documenten, implementen y supervisen los controles adecuados para obtener eficacia en las tres Líneas de Defensa (3LoD).

5.17. Desarrollar, mantener y probar los planes de continuidad del negocio.

5.18. Revisar y mejorar continuamente nuestro ISMS y nuestro marco de referencia.

5.19. Cumplir con la regulación y las normas externas, siempre y cuando no comprometan nuestras políticas y controles de seguridad. Nota: Si existe el riesgo de que esto suceda, póngase en contacto con askcompliace@sencinet.com.

5.20. Abordar la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto.

5.21. Cuando abordar la seguridad de la información bajo el estándar PCI-DSS, sea un requisito contractual establecido por alguno de nuestros clientes, se deberán delimitar claramente y en consenso con el cliente, cuáles son los requisitos aplicables a cada una de las partes, dependiendo del alcance y objeto del contrato. Siempre que se tenga un tipo de solicitud PCI-DSS de parte de algún cliente póngase en contacto con askcompliace@sencinet.com.

6. Políticas Complementares

Esta política de Seguridad de la Información es una consolidación de las políticas de seguridad que se indican a continuación, donde encontrará detalles y especificidades de cada área de seguridad de la información. Deben consultarse y aplicarse conjuntamente siempre que sea necesario.

- **3rd Party Security Responsibilities Policy:** Contiene controles y medidas de seguridad que deben implementarse, como la gestión, el seguimiento y la mitigación de riesgos en relación con nuestra cadena de suministro.
- **Acceptable Use Policy:** Contiene controles y medidas de seguridad que deben implementarse para proteger los sistemas y activos que utilizamos en el trabajo.
- **Access Control Standard:** Contiene los principios clave para garantizar el control de acceso a las aplicaciones, sistemas, redes y dispositivos de Sencinet.
- **Cryptographic Control Standard:** Define cómo se deben implementar y configurar los controles criptográficos para cumplir con los requisitos de la legislación y las directrices internacionales.
- **Data Sanitization and Disposal Policy:** Contiene información sobre cómo gestionar la eliminación segura de datos y activos.
- **Information Classification Data Handling Standard:** Contiene información sobre la clasificación de la información, el etiquetado, la manipulación/transformación, la conservación y la eliminación.
- **Information Retention Policy:** Contiene directrices para estipular los períodos de retención de información para diversas categorías y ubicaciones.
- **People Manager Security Requirements:** Contiene requisitos específicos para que los gerentes se aseguren de que su equipo cumpla con las expectativas y necesidades de la empresa.
- **Physical Security Policy:** Contiene directrices sobre cómo mantener nuestra infraestructura segura.
- **Technical Security Policy:** Contiene un resumen de alto nivel de los controles técnicos de seguridad que deben implementarse para proteger nuestros sistemas y la información que manejan o almacenan.
- **Data Privacy and Protection:** Contiene directrices para la protección de los datos personales y la salvaguarda de la privacidad de las personas, asegurando que los datos personales en posesión de Sencinet se manejen de manera responsable, ética y de acuerdo con los principios, políticas y legislación aplicables.

7. Enlaces e información útiles

Enlace Intranet para Políticas Complementares de Seguridad de la Información: Complementary Security Policies

Para informar de un "incidente de seguridad de la información", envíe un correo electrónico: security.incidents@sencinet.com

Si necesita más información u orientación sobre esta política o cualquier otra política o estándar de seguridad, póngase en contacto con: askcompliance@sencinet.com.

8. Glosario

término	explicación
ISMS	Sistema de Gestión de la Seguridad de la Información
3LoD	Tres líneas de defensa Ejemplo seguridad física Datacenter: Primera Línea de Defensa: Controles de acceso físico y lógico, Mantenimiento infraestructura, Gestión activos. Segunda Línea de Defensa: Gestión de Riesgos, Seguimiento de la Oficina de Compliance. Tercera Línea de Defensa: Realización de Auditorías Internas

9. Historial de revisiones

Versión	Fecha	Autor(es)	Contenido Revisado
1	18/02/2021	Silvio Freitas	Creación del Documento
2	14/04/2021	Silvio Freitas	Se cambia correo de reporte de incidentes de Seguridad, se ajusta ejemplo de 3LoD
3	05/05/2021	Silvio Freitas	Se ajusta la periodicidad de revisión de la presente política a 1 año y de cualquier política que incluya compromisos PCI-DSS. Se incluye numeral 5.21 sobre delimitación de los requisitos PCI-DSS cuando sean un requerimiento contractual de cliente
4	09/05/2022	Silvio Freitas	Se revisa vigencia de la política
5	13/09/2022	Julia Limas Rolim	Cambio de la declaración del CEO para el CISO y cambio de aprobador
6	06/11/2023	Silvio Freitas	Informaciones sobre Políticas complementares añadidas y validad de las políticas explicadas (5.1)