TÍTULO: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Lista de distribución:	
Copia controlada número:	

Anexos		
Núm. Doc.	***Ed.***	***Título***

Histórico de cambios			
Edición	***Fecha***	***Cambio realizado***	***Motivo***
1	08/09/2022	Documento Inicial	
2	02/09/2024	Cambios de logo y fechas y Referencias	

COPIA CONTROLADA Nº:

INDICE

1. APROBACIÓN Y ENTRADA EN VIGOR 2

2. INTRODUCCIÓN 2

3. PREVENCIÓN 2

4. DETECCIÓN 2

5. RESPUESTA 3

6. RECUPERACIÓN 3

7. ALCANCE 3

8. MISIÓN 3

9. MARCO NORMATIVO 4

10. ORGANIZACIÓN DE LA SEGURIDAD 4

11. ROLES: FUNCIONES Y RESPONSABILIDADES 4

12. PROCEDIMIENTOS DE DESIGNACIÓN 5

13. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 5

14. DATOS DE CARÁCTER PERSONAL 5

15. GESTIÓN DE RIESGOS 6

16. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 6

17. OBLIGACIONES DEL PERSONAL 6

18. TERCERAS PARTES 7

19. DOCUMENTACIÓN RELACIONADA 7

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 09 de Septiembre de 2024 por Comité de Seguridad.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

Makenai depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

3. PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7. ALCANCE

Esta política se aplica a todos los sistemas TIC de MAKENAI SOLUTIONS, INNOVATION & CREATIVE IDEAS, S.L., en adelante Makenai y a todos los miembros de la organización, sin excepciones para:

Los sistemas de información que dan soporte a la ingeniería, implantación y soporte de equipos de telecomunicaciones y desarrollo de aplicaciones de acuerdo al documento de determinación de la categoría vigente.

ENS: The information systems that support the engineering, implementation and support of telecommunications equipment and application development according to the current category determination document.

8. MISIÓN

Contribuir al desarrollo de las compañías para las que trabajamos, nuestros clientes, a través de la creación de soluciones y servicios que generen valor para su negocio.

Nos adaptarnos a sus necesidades ofreciéndoles un amplio catálogo de productos y servicios de Telecomunicaciones siguiendo los criterios de máxima flexibilidad y precios óptimos y haciendo fácil lo difícil.

Gestionar el servicio que damos con la máxima calidad y eficiencia, asegurando la excelencia en el servicio para incrementar la productividad de nuestros clientes.

9. MARCO NORMATIVO

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (Esquema nacional de seguridad)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. (Esquema nacional de seguridad).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.

10. ORGANIZACIÓN DE LA SEGURIDAD

Makenai cuenta con un área de seguridad específica en su organigrama.

Se cuenta con un Comité de Seguridad compuesto por el responsable de seguridad, el director financiero, y Dirección General.

Se han establecido las siguientes figuras dependientes del Comité de Seguridad:

- Responsable de Seguridad.
- Responsable de la información: Comité de Seguridad.
- Responsable del servicio. Responsables de cada línea de negocio o servicio prestado.
- Responsables de cada sistema. Identificado en cada procedimiento de gestión de la configuración del sistema.

Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en el documento Perfil del puesto de trabajo.

11. ROLES: FUNCIONES Y RESPONSABILIDADES

Se han establecido las siguientes funciones y responsabilidades:

a) El responsable de la información determina los requisitos de la información tratada

b) El responsable del servicio determina los requisitos de los servicios prestados.

c) El responsable de la seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en el documento Perfil del puesto de trabajo.

12. PROCEDIMIENTOS DE DESIGNACIÓN Y RENOVACIÓN

El Responsable de Seguridad de la Información será nombrado por el D. General a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

13. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el D. General y difundida para que la conozcan todas las partes afectadas.

14. DATOS DE CARÁCTER PERSONAL

Makenai trata datos de carácter personal. El responsable de Protección de Datos cuenta con un registro de actividad en el que se describe el tratamiento realizado a los mismos.

Además, se analizan los riesgos derivados de su tratamiento y se establecen los controles necesarios para su protección y conservación.

15. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

16. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Makenai en diferentes materias:

■ Listar referencias a otras políticas en materia de seguridad.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad está disponible en la intranet de la organización a la que se accede mediante una carpeta compartida, y se compone de:

- Esta política de seguridad.
- Un Manual (Manual ENS y procedimientos operativos de seguridad).
- La categoriazación del sistema.
- Análisis de riesgos.
- Declaración de aplicabilidad (Controles ISO 27001 y ENS).
- Plan de continuidad de negocio.

Además de esta documentación, son de aplicación los documentos que figuran en el listado de documentación en vigor.

17. OBLIGACIONES DEL PERSONAL

Todos los miembros de Makenai tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Makenai atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Makenai, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

18. TERCERAS PARTES

Cuando Makenai preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Makenai utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

19. DOCUMENTACIÓN RELACIONADA

- Guía de seguridad CCN-STIC-805. Esquema nacional de seguridad. Política de seguridad de la información.
- CCN-STIC 402
- Apartado 5.2 de la norma UNE-EN ISO/IEC 27001:2017. Sistemas de gestión de seguridad de la información. Requisitos.

Firmado Comité de Seguridad

Diego Barón	Julián Ortiz	Ángel Violero
Dir. General.	Dir. Financiero	Resp. Seguridad