ubikare

Política de seguridad

HOJA DE CONTROL

Documento	Política de seguridad
Referencia	

Versión	Fecha	Fichero	Política de seguridad.pdf		
2	18/11/2024	Descripción	Política de seguridad		
			Preparado	Revisado	Aprobado
		Nombre	Jaime Crovetto UBIKARE	Egoitz Arruti UBIKARE	Ángel Díez UBIKARE

CONTROL DE DOCUMENTACIÓN

Todas las modificaciones realizadas en posteriores revisiones deberán quedar registradas en la siguiente tabla:

Revisión	Fecha	Responsable	Cambios realizados
0	15/04/2023	Jaime Crovetto	Redacción inicial de la Política de seguridad
1	06/06/2024	Jaime Crovetto	Modificación del Comité de Seguridad
2	18/11/2024	Responsable Información	Adaptación para ISO 27001:2022

De esta manera se conocerá cual es la versión en vigor a la hora de distribuir copias controladas.

ubikare

CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 22 de noviembre de 2023 por la dirección de la organización.

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

2. INTRODUCCIÓN

Ubikare 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.

Consciente de ello, la alta dirección se ha comprometido a establecer un Sistema de Gestión de la Seguridad de la Información de acuerdo con los requisitos de la norma UNE-EN ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad.

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 con el artículo 7 del ENS.

La organización se compromete a la mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI). Esto implica la revisión periódica de los controles de seguridad, la identificación y mitigación de nuevas amenazas, y la adaptación a los cambios en el entorno tecnológico y regulatorio.

2.1. 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, están 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.

2.2. DETECCIÓN

Dado que los servicios se pueden 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 produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. 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).

2.4. 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.

4. MISIÓN, VISIÓN Y VALORES

Es importante definir la misión, visión y valores de la organización para comprender su alcance y objetivos y establecer una cultura de seguridad de la información.

Misión

Democratizar la salud y los cuidados a través de nuestro software de referencia en el sector sociosanitario, asegurando siempre el más alto nivel de calidad.

Visión

Convertirse en líder del mercado en la democratización del acceso a los servicios de atención domiciliaria. Este objetivo se logrará a través de nuestro experimentado equipo de gestión y a través del compromiso y dedicación de nuestros empleados.

Valores

En UBIKARE, nuestros valores son nuestra cultura y el éxito. Creemos en la responsabilidad social y nos esforzamos por promover la salud mientras liberamos recursos del sistema público. Nuestro equipo siente pasión por su trabajo y está comprometido a obtener la excelencia en todo lo que hace. Entendemos que la confianza es crucial en nuestra industria y la construimos a través de la empatía, el diálogo y la transparencia. A medida que continuamos creciendo, seguimos comprometidos en aportar conocimiento y trabajar para mejorar la calidad de vida de nuestros usuarios.

5. OBJETIVOS

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- ➔ Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- ➔ Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- ➔ Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- ➔ Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información

6. MARCO NORMATIVO

Son de aplicación las siguientes leyes:

- Ley 41/2002 de autonomía del paciente, que regula los derechos de los pacientes en relación a su historia clínica.
- Ley 14/1986 General de Sanidad, que regula los servicios sanitarios dentro del estado español.
- Reglamento europeo de protección de datos RGPD, para la libre circulación de los datos y la protección de la vida privada de las personas y de su información en las comunicaciones electrónicas.
- LPI (Ley de Propiedad Intelectual), que regula los derechos relativos a las creaciones de software.
- Leyes de Propiedad Industrial, que protegen marcas y nombres comerciales, patentes y modelos de utilidad.
- LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) que regula los aspectos jurídicos de las actividades económicas o lucrativas del comercio electrónico, la contratación en línea, la información y la publicidad y los servicios de intermediación.
- Real Decreto 1720/2007 - LOPD (Ley orgánica de protección de datos).
- Real decreto 3/2010 Esquema Nacional de Seguridad (Derogado)
- Real decreto 311/2022 Esquema Nacional de Seguridad
- Ley Orgánica 3/2018 - Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- REGLAMENTO (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Real Decreto Legislativo 2/2015, Estatuto de los trabajadores.
- Real Decreto Legislativo 2/2015, Estatuto de los trabajadores.
- Real Decreto Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Ley 31 /1995 de prevención de riesgos laborales
- ISO 27001/2022

7. ORGANIZACIÓN DE LA SEGURIDAD

La implantación de la Política de Seguridad en Ubikare requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

7.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El comité de seguridad estará formado por:

- Responsable de Seguridad
- Responsable del Servicio
- Responsable de la Información
- Responsable de Sistema
- Responsable del SGSI
- Delegado de Protección de datos

El Comité de Seguridad TIC estará presidido el CEO, y actuará como secretario el CTO, teniendo como funciones:

- Convocar por orden del Presidente las reuniones del Comité de Seguridad de la Información.

- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.

La Comisión se reunirá en sesión ordinaria al menos una vez al año para la revisión de los indicadores. Podrá reunirse, igualmente, en sesión extraordinaria en cada ocasión en que los asuntos relacionados con sus competencias lo requieran. Las reuniones serán convocadas por la presidencia de la Comisión, ya sea por propia iniciativa, y a petición de cualquiera de sus componentes, con una antelación mínima de 5 días hábiles en el caso de tratarse de una sesión ordinaria y de 48 horas cuando se trate de una sesión extraordinaria.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Divulgación de la política y normativa de seguridad.
- Aprobación de la normativa de seguridad.
- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Promoción, supervisión y aprobación de las tareas de seguimiento del ENS:
    - Tareas de adecuación
    - Análisis de Riesgos
    - Planes de mejora de seguridad de la información
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Monitorizar los principales riesgos residuales asumidos por Ubikare y recomendar posibles actuaciones respecto de ellos.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

7.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los roles y responsabilidades se encuentran descritos en el apartado Roles y responsabilidades del Documento de Seguridad, el cual está disponible en drive corporativo de Ubikare.

7.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por el/la Director/a 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.

7.4. 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/la Director/a y difundida para que la conozcan todas las partes afectadas.

7.5. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN

Directrices de estructuración de la documentación

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles de manera que cada documento de un nivel se fundamenta en los de nivel superior:

a) Primer nivel: Política de Seguridad de la Información. Documento de obligado cumplimiento por todo el personal, interno y externo, recogido en el presente documento y aprobado por la Dirección.

b) Segundo nivel: Normativa de uso de medios y códigos de conducta en relación a la Tecnología de la Información. De obligado cumplimiento de acuerdo al ámbito organizativo,

técnico o legal correspondiente. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia de la Dirección.

c) Tercer nivel: Procedimientos Técnicos de Seguridad. Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. La responsabilidad de aprobación de estos procedimientos técnicos es del Director de Seguridad.

d) Cuarto nivel: Informes, registros y evidencias electrónicas. Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida de los sistemas de la información. La responsabilidad de que existan este tipo de documentos es de cada uno de los responsables de los Sistemas de Información en su ámbito de actuación.

8. DATOS DE CARÁCTER PERSONAL

Ubikare trata datos de carácter personal. Todos los sistemas de información de Ubikare se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos.

Ubikare cuenta con delegado de protección de datos debidamente nombrado comunicado a la Agencia Española de Protección de Datos.

9. 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.

El responsable de seguridad será el responsable de la custodia y divulgación de la versión aprobada de la documentación generada. La documentación se encuentra dentro del sistema de gestión documental de google drive corporativo de Ubikare.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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

- Uso aceptable.
- Seguridad de la gestión de recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.

Estas Políticas se desarrollarán por medio de una normativa de seguridad que afronte aspectos específicos.

Estas políticas estarán a disposición de todos los miembros de la organización que necesiten conocerlas, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de Ubikare 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 Ubikare 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 Ubikare, 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.

12. TERCERAS PARTES

Cuando Ubikare 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 Ubikare 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 atañe 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 esté 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.

16067492Z ANGEL DIEZ (R: B95843413)

Firmado digitalmente por 16067492Z ANGEL DIEZ (R: B95843413)
Fecha: 2025.11.28 10:57:01 +01'00'