Esquema Nacional de Seguridad

Política de seguridad

22 feb 2023

VEXIZA

Vexiza, S.L.
Oficina I-10 | Centro de Empresas de Base Tecnológica (CEBT)
Calle Santos Ovejero 1, 24009, León

+34 987 08 07 08
info@vexiza.com | vexiza.com

Contenido

Contenido 1
Control de versiones 1
1. Aprobación y entrada en vigor 2
2. Introducción 3
2.1. Prevención 4
2.2. Detección 5
2.3. Respuesta 5
2.4. Recuperación 5
3. Alcance 6
4. Misión 6
5. Marco normativo 7
5.1. Requisitos legales aplicables 7
6. Organización de la seguridad 8
6.1. Comités: funciones y responsabilidades 8
6.2. Roles: funciones y responsabilidades 10
6.3. Procedimientos de designación 11
6.4. Difusión, actualización y revisión de la política de seguridad de la información 11
6.5. Datos de carácter personal 12
7. Gestión de riesgos 12
8. Desarrollo de la política de seguridad de la información 13
8.1. Obligaciones del personal 13
8.2. Terceras partes 13

Control de versiones

Versión	Motivo	Autor	Fecha
01.00	Primera versión del documento	Vexiza	22 feb 2023

Información legal

Cláusula de confidencialidad - Este documento y documentos anexos son propiedad de Vexiza, Sociedad Limitada. Éstos son confidenciales y dirigidos exclusivamente a los destinatarios de los mismos. Si por error ha recibido este documento y no es el destinatario, por favor, notifíquesele al remitente y no use, informe, distribuya, imprima, copie o difunda este documento por ningún medio. Su uso no autorizado está sujeto a responsabilidades legales.

VEXIZA, S.L. informa que los datos personales contenidos en este documento son tratados de acuerdo a las disposiciones del RGPD y la LOPDGDD. La finalidad de este tratamiento será la gestión de la actividad empresarial habitual a través de sistemas de comunicación con todos los interesados. VEXIZA, S.L. le informa que los datos han sido obtenidos por consentimiento del interesado, por derivación de una obligación contractual, por una cesión legítima o desde una fuente de acceso pública. Si desea ejercer cualquier derecho en materia de protección de datos frente a VEXIZA, S.L., puede hacerlo en la dirección de correo electrónico info@vexiza.com. Para más información consulte nuestra política de privacidad en nuestra web, o visite www.aepd.es.

Vexiza, Sociedad Limitada - NIF: B24683559 - Inscrita en el Registro Mercantil de León, Tomo 1298, Folio 32, Sección 8, Hoja LE 23663. Domicilio Social: Calle El Hayedo 6, 1B, 24007, León, España.

1. Aprobación y entrada en vigor

Texto aprobado el día 22 de febrero de 2023, por Alberto Cerrillo Cuenca.

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

2. Introducción

Esta política cumple con el Control 3.1 del Esquema Nacional de Seguridad habiendo sido establecida por el Comité de Seguridad de la Información e incluyendo todos los requisitos que la norma exige. Este documento sienta las bases para la gestión de la Seguridad de la Información de VEXIZA.

Su alcance comprende todos los centros de datos de VEXIZA.

VEXIZA 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 de la organización 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.

La presente política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II del RD 311.2022 y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de los riesgos
c) Gestión de personal
d) Profesionalidad
e) Autorización y control de los accesos
f) Protección de las instalaciones
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de la actividad y detección de código dañino
m) Incidentes de seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

Estos requisitos mínimos se exigen en proporción a los riesgos identificados en nuestro sistema, de conformidad con lo dispuesto en el artículo 28 del RD 311.2022.

Esta política se encuentra disponible como información documentada a todo el personal de VEXIZA.

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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la politica, 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 9 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.

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.

VEXIZA se compromete a prestar sus servicios de forma gestionada y cumpliendo con los requisitos establecidos en su Sistema Integrado de Gestión de modo que se garantice un servicio ininterrumpido conforme a los requisitos de disponibilidad, seguridad y calidad hacia los clientes.

3. Alcance

Esta politica se aplica a todos los sistemas TIC de VEXIZA y a todos los miembros de la organización, sin excepciones.

4. Misión

VEXIZA depende de los sistemas TIC para alcanzar sus objetivos de prestación de servicios de desarrollo de software y soluciones IT.

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, confidencialidad o trazabilidad 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 servicios prestados consiguen obtener una mejora en el rendimiento de la infraestructura, mejorar la productividad del personal técnico y reducir significativamente el coste de las inversiones. Es decir, se busca maximizar el tiempo útil y la seguridad de los sistemas de información, sin tener que realizar inversiones en equipamiento, software o formación de recursos humanos.

Debido a nuestra actividad, en VEXIZA sabemos que la información es un activo con un elevado valor para nuestra organización y sobre todo la de nuestros clientes y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad a nuestra línea de negocio y minimizar los posibles daños ocasionados por fallos en la Seguridad de la Información.

Para ello, la organización:

- Protegerá adecuadamente la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de sus activos de información mediante la

introducción de una serie de controles para gestionar los riesgos de seguridad relevantes.

- Priorizará la protección y salvaguarda de sus clientes y los datos de los clientes como una prioridad de negocio.
- Establecerá, implementará, monitoreará, mantendrá y mejorará continuamente su gestión de seguridad de la información como parte de su enfoque más amplio de gestión empresarial, y mantendrá la Certificación Acreditada a los estándares adecuados.
- Gestionará cualquier violación de la seguridad de la información de manera oportuna y responsable, e invertirá en estrategias adecuadas de detección, respuesta y remediación.
- A intervalos planificados, probará sus controles de seguridad de la información y sus respuestas a escenarios que puedan causar una amenaza a sus operaciones.
- Proporcionará los recursos adecuados a la organización para establecer, mantener y mejorar el entorno de seguridad según sea apropiado para el cambiante panorama de riesgos.
- Invertirá en las competencias del personal para llevar a cabo sus tareas y proporcionará al personal la capacitación y la conciencia adecuadas relevantes para su función y la información a la que tienen acceso.
- Garantizará que nuestros proveedores y organizaciones asociadas hagan lo mismo, y que establezcan y hagan cumplir los estándares de seguridad a aquellos a quienes transmitimos cualquier información.

5. Marco normativo

Esta Política de Seguridad complementa las políticas de seguridad de VEXIZA en diferentes materias. La documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de seguridad.
- Segundo nivel: Normativas y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas

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.

5.1. Requisitos legales aplicables

En el ámbito de los datos de carácter personal, aplica:

- 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.

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

6. Organización de la seguridad

6.1. Comités: funciones y responsabilidades

El Comité de Seguridad de la Información estará formado por:

- Responsable de Seguridad: Álvaro Calero
- Responsable del Sistema: Javier Oliver
- Responsable de la Información: Alberto Cerrillo
- Responsable del Servicio de Desarrollo de Producto: Guillermo Marqués

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización.

6.2. Roles: funciones y responsabilidades

Se detallarán a continuación las funciones de los responsables de la organización:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.

Responsable de la Seguridad

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El responsable de la Seguridad será el secretario (o presidente) del Comité de Seguridad de la Información con las funciones indicadas en este documento.

Responsable del Sistema

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Responsable de Privacidad

Sus funciones serán las siguientes:

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de VEXIZA en materia de protección de datos de carácter personal.
- Coordinar, junto con el responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

6.3. Procedimientos de designación

El responsable de Seguridad de la Información es nombrado por el Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad de la Información mediante acta de reunión.

6.4. Difusión, actualización y revisión de la política de seguridad de la información

Será misión del Comité de Seguridad de la Información 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 Órgano de Gobierno y difundida para que la conozcan todas las partes afectadas.

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.

6.5. Datos de carácter personal

El Documento de Seguridad al que tendrán acceso sólo las personas autorizadas, recoge los registros de actividad de tratamiento de datos afectados y los responsables correspondientes. Todos los sistemas de información de VEXIZA se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

7. 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 de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. Desarrollo de la política de seguridad de la información

8.1. Obligaciones del personal

Todos los miembros de VEXIZA 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de VEXIZA atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de VEXIZA 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.

8.2. Terceras partes

Cuando VEXIZA preste servicios a otras organizaciones públicas o privadas o maneje información de otras organizaciones públicas o privadas, 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 de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinares que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Cuando VEXIZA 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 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.

Aprobación de la Política de Seguridad:

Fdo, Responsable de Seguridad: Álvaro Calero

Responsable del Sistema: Javier Oliver

Responsable del Servicio de Desarrollo de Producto: Guillermo Marqués

Responsable de la Información: Alberto Cerrillo