ESpanix

POLITICA DE SEGURIDAD

Control de Versiones

	Autor	Descripción	Fecha Entrega
1.0	Equipo consultor	Versión borrador	Marzo 2023
2.0	Equipo Técnico	Versión Final	Junio 2023

Responsabilidades

	Nombre	Compañía	Fecha
Realizado por:	Equipo Consultor	Proceso Social	Marzo 2023
Revisado por:	Equipo Técnico	Espanix	Junio 2023
Aprobado por:			

Documentos de referencia

Documento	Comentarios
EX_Política de Seguridad_v2	Versión Final
EX_Normativa de Seguridad_v2	Versión Final

Calificación del documento

Difusión		Seguridad	
IN1 Interna	**IN2**	**NL1: General**	**NL2**
IN2 Clientes		**NL2: Restringido**	
IN3 Exterior		**NL3: Confidencial**	

ESpanix

INDICE

INTRODUCCIÓN

Esta "Política de Seguridad de la Información" es efectiva desde su entrada en vigor el día 01 de Junio de 2023 por Espanix.

La Política es revisada por el responsable de Seguridad de la Información a intervalos planificados, sin exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, comunicándose de forma efectiva.

Los cambios sobre la Política de Seguridad de la Información serán aprobados por la Dirección de Espanix. Cualquier cambio sobre la misma deberá ser difundido para conocimiento de toda la Organización.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

ALCANCE

Sistemas de información que proporcionan apoyo interno a los servicios prestados por Espanix consistentes en la gestión de proyectos, servicios de auditoría y consultoría de procesos, sistemas y seguridad y servicios prestados en modo de asistencias técnicas realizadas sobre los propios sistemas del cliente.

Espanix, es una empresa privada que facilita a sus clientes una plataforma de interconexión de redes IP, para que puedan establecer acuerdos de peering.

Así mismo dispone un espacio telemático propio (Datacenter) en el que están situados los equipamientos de red tanto propios como de terceras partes (clientes).

MARCO NORMATIVO

Esta política se enmarca en la siguiente legislación:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ENS. Artículo 12. Organización e implantación del proceso de seguridad.
- 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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Guía de Seguridad de las TIC CCN-STIC 805 ENS. Política de seguridad de la información.
- Guía de Seguridad de las TIC CCN-STIC 801 ENS. Responsabilidades y funciones.

- El convenio colectivo aplicable, correspondiente a "Empresas de consultoría, y estudios de mercado y de la opinión pública".
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

MISIÓN

El propósito de esta Política de Seguridad de la Información es proteger la información de los servicios de Espanix.

La política de Seguridad, junto con la Normativa de Seguridad se realizará mediante una comunicación a todos los trabajadores, para que se efectúe el análisis, comprensión y lectura del documento.

Esta política aplica a Sistema de información propiedad de Espanix, para la adecuada prestación de los servicios de asistencia técnica, mediante la asignación de personal cualificado a organizaciones públicas, llevando a cabo su gestión y seguimiento en los ámbitos de:

- Asistencia técnica para el soporte a sistemas.
- Asistencia técnica para la atención y soporte a usuarios.
- Asimismo, realización de consultoría TIC y de seguridad, junto a auditorías técnicas y de cumplimiento, todo ello según las disposiciones del RD 311/2022, y la Declaración de Aplicabilidad vigente.

FUNCIONES DE SEGURIDAD

Espanix ha nombrado un comité de Seguridad con sus Funciones y Responsabilidades.

El establecimiento de este comité, así como la designación de los diferentes roles se hallan registrados en el Acta de Constitución del comité: EX_Acta Comité de Seguridad_v2 de fecha 01/06/2023 y en Acta de Nombramientos: EX_Acta Nombramientos ENS_v2

El Comité de Seguridad de la Información del ENS está formado por:

*Responsable de Seguridad

*Responsable de Dirección

Además, existen los roles:

*Responsable de la Información

*Responsable de Sistemas

*Responsable del Servicio

*Delegado de Protección de Datos

Se deben identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización. Se detallarán en la política de seguridad de la organización las atribuciones de cada responsable.

Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante. Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

Los diferentes roles junto con sus respectivas funciones y responsabilidades:

El **Responsable de la Información** tendrá como funciones:

- Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.
- Aunque la aprobación formal de los niveles corresponda al responsable de la Información, se puede recabar una propuesta al responsable de la Seguridad y conviene que se escuche la opinión del responsable del Sistema.
- Determinar los requisitos de la información tratada.
- Velar por la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad.
- Estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural

El **Responsable del servicio** tendrá las funciones:

- Determinar los requisitos de Seguridad de los servicios prestados en los Clientes.
- Revisar y aprobar los niveles de seguridad de los servicios.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios, se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los Clientes.
- Asumir la propiedad de los riesgos sobre los servicios.

El **Responsable de los sistemas** tendrá las funciones:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.

- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema y determinar las medidas de seguridad que deben aplicarse Elaborar y aprobar la documentación de seguridad del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al responsable de Seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

El **Responsable de seguridad** tendrá las funciones:

- Responsable de la Seguridad es la persona designada por la Dirección de la Organización.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Trabajar para conseguir una total seguridad de los datos de la empresa, así como la privacidad de estos.
- Supervisar, controlar y administrar el acceso a la información de la empresa, y de sus trabajadores.
- Elaborar un conjunto de medidas de respuesta ante incidentes de seguridad relacionados con la información, incluyendo la recuperación ante desastres.
- Garantizar el cumplimiento de la normativa relacionada con la seguridad de la información.
- En caso de servicios externalizados, la responsabilidad última la tiene siempre la Organización destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato) a la organización prestataria del servicio.
- 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.
- Garantizar el buen uso del equipamiento informático dentro de su ámbito de responsabilidad.
- Supervisar y coordinar al equipo encargado de llevar a cabo las medidas de respuesta en caso de brechas de seguridad.
- POC (Persona de contacto de seguridad de la información) Se responsabilizará de la seguridad con los Clientes, en los que presta servicio Espanix.
- Realizar operaciones de seguridad para luchar contra el fraude y el robo de información.
- Diseñar del Plan de formación, en el ámbito del ENS, para las personas de Espanix que prestan servicios en proyectos de AA.PP.

El **DPD** tendrá las funciones

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Además, el responsable del sistema puede *acordar* la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutado.

REPORTES

El administrador de seguridad reporta al responsable del Sistema o al responsable de la Seguridad, según sea su dependencia funcional:

- Incidentes relativos a la seguridad del sistema o acciones de configuración, actualización o corrección.
- El responsable del Sistema informa al responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- El responsable del Sistema informa al responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- El responsable del Sistema reporta al responsable de la Seguridad:
  - -actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema
  - -Resumen consolidado de los incidentes de seguridad.

ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART. 14)

Se realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos según lo previsto en el artículo 7 y 14 del BOE, 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.
- Cuando haya un incidente de seguridad relacionado con la normativa LOPDGDD
- Cuando haya una brecha de seguridad relacionada con la información tratada de un usuario según la normativa LOPDGDD.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios, o repercuta a dicha información tratada durante el servicio.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios de Espanix en los Clientes.

El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

GESTIÓN DE PERSONAL (ART. 15)

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en el documento Normativa de Seguridad que será aprobada por la dirección de Espanix.

Se difundirá a toda la Organización, siendo obligatorio su difusión para cada incorporación en Espanix.

PROFESIONALIDAD (ART. 16)

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Espanix determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

AUTORIZACIÓN Y CONTROL DE LOS ACCESOS (ART. 17)

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los privilegios de acceso de un recurso (persona) al sistema de información de Espanix, quedan restringidos por defecto al mínimo necesario para el desarrollo de sus funciones.

El sistema de información de Espanix se mantendrá siempre configurado, de tal manera que evite que un recurso (persona) pueda acceder accidentalmente a recursos con derechos distintos de los autorizados.

PROTECCIÓN DE LAS INSTALACIONES (ART. 18)

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD (ART. 19)

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004,

de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.

b) Otras certificaciones de seguridad adicionales que se requieran normativamente.

c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

d) Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

MÍNIMO PRIVILEGIO (ART. 20)

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA (ART. 21)

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO (ART. 22)

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS (ART. 23)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO (ART. 24)

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

INCIDENTES DE SEGURIDAD (ART. 25)

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

CONTINUIDAD DE LA ACTIVIDAD (ART. 26)

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

MEJORA CONTINUA DEL PROCESO DE SEGURIDAD (ART. 27)

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

APROBACIÓN DEL DOCUMENTO

Documento: Política de Seguridad

Estado: Aprobado

Firmado:

CG Nodo Neutro Espanix S.L.
Av. Comunidad de Madrid 37 Bis 1º F
28231 Las Rozas (Madrid)
C.I.F ESB87422937