# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

CYBERXIA SECURITY, S.L.

Versión pública

Fecha de aprobación: 11/11/2025

02-PLT-01 · Versión 1.0

# 1 Finalidad y compromiso

Cyberxia Security, S.L. establece esta Política de Seguridad de la Información y Protección de Datos Personales para orientar la protección de la información y de los sistemas que sustentan sus servicios. Su finalidad es preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como proteger los datos personales tratados por la organización.

La seguridad se integra en la actividad de la organización y en la prestación de sus servicios. CYBERXIA promueve una gestión basada en los riesgos, la profesionalidad de las personas y la mejora continua, con medidas proporcionales a la información y a los servicios que deben protegerse.

## 2 Alcance

La política se aplica a la información y a los sistemas que soportan la actividad de CYBERXIA, al personal que los utiliza o administra y a las terceras partes en los términos que correspondan a su relación con la organización. Comprende las siguientes líneas de servicio:

- Seguridad ofensiva o Red Team: auditorías de seguridad, análisis de malware, análisis forense y vigilancia digital.
- Consultoría normativa: análisis de riesgos, formación y concienciación, protección de datos, cumplimiento normativo y servicios de delegado de protección de datos.
- Seguridad defensiva o Blue Team: respuesta a incidentes, seguridad gestionada y servicios de seguridad defensiva.

## 3 Objetivos y marco de referencia

CYBERXIA orienta su actividad a reducir la exposición a riesgos, prevenir y gestionar incidentes, proteger la información propia y de sus clientes y fomentar una cultura de seguridad. La confianza, la innovación, la calidad profesional, la transparencia y la colaboración guían este compromiso.

La política se desarrolla de acuerdo con los principios y requisitos de seguridad aplicables del Esquema Nacional de Seguridad, la normativa vigente de protección de datos personales y las obligaciones legales, regulatorias y contractuales que correspondan a la actividad de la organización. Su desarrollo operativo se concreta en la normativa y los procedimientos internos de seguridad.

# 4 Principios de seguridad de la información

## 4.1 Seguridad integral y mínimo privilegio

La seguridad se entiende como un proceso integral que comprende los elementos técnicos, humanos, materiales y organizativos relacionados con la información. Debe estar presente durante todo el ciclo de vida de los sistemas y de los servicios.

Los sistemas deben proporcionar la funcionalidad necesaria para la actividad de la organización y limitar el acceso a las personas y funciones autorizadas. Las funciones innecesarias se eliminarán o desactivarán y el uso ordinario de los sistemas deberá facilitar una operación segura.

## 4.2 Gestión basada en los riesgos

Los sistemas incluidos en el alcance de la política deberán contar con un análisis de riesgos que identifique y valore las amenazas relevantes. Sus resultados servirán para seleccionar y justificar medidas proporcionadas al nivel de riesgo, utilizando metodologías de referencia reconocidas.

El análisis se revisará, al menos, anualmente y cuando se produzcan cambios relevantes en la información, los servicios, los sistemas o los procesos, así como ante incidentes graves o vulnerabilidades críticas. La gestión de riesgos comprende tanto el análisis como el tratamiento y el seguimiento de los riesgos identificados.

## 4.3 Control de acceso y responsabilidades de uso

El acceso a la información y a los sistemas se limitará a lo estrictamente necesario y deberá estar debidamente autorizado. La identificación de las personas usuarias y la asignación de permisos deben permitir la trazabilidad y la atribución de responsabilidades, de acuerdo con las necesidades de cada función.

El personal debe conocer las normas de uso seguro y actuar conforme a ellas. La seguridad de los sistemas será responsabilidad de personas con la cualificación adecuada para las funciones que desempeñen.

## 4.4 Protección de la información

La información deberá protegerse tanto cuando se almacena como durante su transmisión, atendiendo a su naturaleza y a los riesgos asociados. La protección se extiende a la información electrónica y a la conservada en soportes físicos, así como a los dispositivos utilizados para acceder a ella.

Las medidas de protección deben contemplar la seguridad de las comunicaciones, la prevención del código dañino y la conservación y recuperación de la información. El tratamiento de la información y su acceso deben ajustarse a los requisitos de seguridad definidos por la organización.

# 5 Prevención y respuesta

## 5.1 Vigilancia y revisión de la seguridad

CYBERXIA establece controles y evaluaciones de seguridad para conocer el estado de los sistemas, identificar desviaciones y gestionar las vulnerabilidades que puedan afectarles. La incorporación de nuevos elementos y los cambios relevantes deberán ser autorizados y compatibles con los requisitos de seguridad de la organización.

Las revisiones periódicas y las evaluaciones independientes contribuyen a comprobar la eficacia de las medidas. Los resultados e indicadores se utilizarán para detectar oportunidades de mejora y adaptar la protección a la evolución de los riesgos y las amenazas.

## 5.2 Gestión de incidentes

La organización dispone de procedimientos para detectar, clasificar, analizar y gestionar los incidentes de seguridad y las vulnerabilidades. La respuesta deberá ser coordinada y proporcionada a la situación, con registro de las actuaciones y comunicación a las partes que corresponda.

La gestión de incidentes se alinea con las recomendaciones de los organismos de referencia y con las obligaciones aplicables. El análisis de los incidentes y de sus causas permitirá incorporar mejoras y reducir la posibilidad de repetición.

## 5.3 Recuperación de los servicios y de la información

La gestión de la seguridad incorpora medidas orientadas a restablecer los servicios afectados por un incidente y a proteger la información comprometida. Las copias de seguridad y los procedimientos de recuperación deben contribuir a preservar la disponibilidad y la conservación de la información necesaria para la actividad.

## 5.4 Infraestructuras e interconexiones

La seguridad debe contemplar la protección de las infraestructuras y de los equipos, la prevención de accesos no autorizados y las condiciones de conexión con otros sistemas. Antes de establecer interconexiones con clientes, proveedores u otras organizaciones, deberán analizarse sus riesgos y definirse las condiciones de seguridad correspondientes.

Las medidas de protección se determinarán en función de las necesidades del servicio y de la información tratada. La adquisición de productos y servicios tendrá en cuenta los requisitos de seguridad y las garantías que resulten aplicables.

# 6 Organización de la seguridad

CYBERXIA organiza la seguridad mediante funciones diferenciadas y responsabilidades definidas. Esta distribución facilita la coordinación, la supervisión y la atribución de responsabilidades dentro de la organización.

## 6.1 Comité de Seguridad de la Información

El Comité está integrado por la Presidencia, ejercida por el Responsable de Seguridad; el Responsable de Sistema; la Secretaría, ejercida por personal delegado de CYBERXIA, y las vocalías, desempeñadas por personal de la organización.

Asume las funciones de responsabilidad sobre la información y los servicios: determina sus requisitos de seguridad y aprueba su valoración y modificación. Define la estrategia y los planes de seguridad y realiza el seguimiento de su ejecución.

Coordina las funciones de seguridad y las propuestas de adquisición y desarrollo; verifica y aprueba los procedimientos y la documentación; mantiene actualizado el marco normativo de seguridad e identifica las guías de referencia aplicables. También impulsa la formación, las auditorías y la mejora continua y resuelve los conflictos de responsabilidad.

## 6.2 Responsable de Seguridad del ENS

Es responsable de coordinar la implantación de las medidas de seguridad y verificar su cumplimiento, su idoneidad y su alineación con los objetivos de la organización. Preside el Comité de Seguridad de la Información e informa sobre el rendimiento de las medidas, proponiendo y coordinando mejoras.

Supervisa la gestión de los incidentes y la obtención de indicadores; difunde la política, la normativa y los programas de formación; asesora a las áreas de la organización y colabora en las auditorías internas y externas. Coordina la implantación y supervisión de la normativa de seguridad.

## 6.3 Responsable de Sistema

Es responsable de ejecutar las medidas de protección de los activos y servicios de los sistemas de información. Define las funciones y obligaciones del personal técnico y sus actuaciones en los distintos entornos, y mantiene los procedimientos técnicos alineados con las medidas aprobadas.

Vela por la actualización del inventario y por la adecuación del nivel de protección de los activos. Comprueba que los nuevos sistemas y los cambios cumplen los requisitos establecidos; establece controles de monitorización, coordina la investigación y resolución de las incidencias y comunica sus resultados al Responsable de Seguridad.

# 7 Personal y protección de datos

## 7.1 Formación y concienciación

Todo el personal debe conocer esta política, la normativa de seguridad que le resulte aplicable y las obligaciones de su puesto. CYBERXIA promueve su difusión y dispone de un programa de formación y concienciación, con especial atención a las nuevas incorporaciones.

Las personas con responsabilidades de uso, operación o administración de sistemas recibirán la formación específica necesaria antes de asumir sus funciones o cuando cambien sus responsabilidades. El personal externo deberá conocer y cumplir las obligaciones de seguridad que le correspondan.

## 7.2 Protección de datos personales

Los sistemas y tratamientos de CYBERXIA deberán ajustarse a la normativa vigente de protección de datos personales y a los niveles de seguridad que esta requiera. La organización adaptará sus medidas a los cambios legales o regulatorios que resulten aplicables.

La protección de los datos personales forma parte de la gestión de la seguridad de la información y deberá tenerse en cuenta en la prestación de servicios, en las relaciones con terceros y en la gestión de incidentes que puedan afectar a dichos datos.

# 8 Relaciones con terceros y revisión

## 8.1 Clientes y proveedores

Cuando CYBERXIA preste servicios a otras organizaciones o gestione información de terceros, las partes deberán conocer las obligaciones de seguridad que correspondan a su relación. Se establecerán los mecanismos de comunicación y coordinación necesarios para la protección de la información y la gestión de incidentes.

Cuando la organización recurra a servicios externos o comparta información con terceros, les trasladará esta política y los requisitos de seguridad aplicables. La relación deberá contemplar las responsabilidades de cada parte y las condiciones necesarias para preservar la seguridad de los servicios y de la información.

Las situaciones en las que una tercera parte no pueda cumplir íntegramente un requisito deberán analizarse y someterse a la aprobación que corresponda, valorando los riesgos y las medidas alternativas de protección.

## 8.2 Cumplimiento

La política y la normativa de seguridad de la información son de cumplimiento obligatorio en el ámbito que les corresponda. Su incumplimiento podrá dar lugar a las responsabilidades y medidas previstas en la legislación, en la normativa laboral aplicable o en los compromisos contractuales establecidos.

## 8.3 Revisión y mejora continua

El Responsable de Seguridad propondrá la revisión de la política y las modificaciones necesarias para mantenerla adecuada a la actividad y a los requisitos aplicables. Las modificaciones y actualizaciones deberán ser aprobadas por el Comité de Seguridad de la Información.

La mejora continua se apoya en la revisión de los riesgos, los resultados de los controles y de las auditorías, los incidentes y los cambios en el contexto de la organización. La política se difundirá para que las personas y entidades afectadas conozcan sus compromisos y obligaciones.

Aprobación de la política: 11/11/2025. Órgano de aprobación: Comité de Seguridad de la Información.