POLÍTICA DE SEGURIDAD PLUXEE ESPAÑA S.A.U

[IST.31.POL.001]

IST – Seguridad en los Sistemas

CONFIDENTIAL © Pluxee 2024 – All rights reserved

Contenido

Compromiso institucional 2
Comité de Seguridad de la Información 2
Alcance y aplicación 3
Principios de seguridad 3
1. Prevención, detección y vigilancia continua 3
2. Gestión del riesgo y mejora continua (PDCA) 3
3. Protección de los datos personales y cumplimiento normativo 3
4. Continuidad del negocio y resiliencia operativa 4
5. Formación y concienciación en seguridad 4
6. Control y supervisión de terceros y proveedores 4
7. Seguridad desde el diseño y por defecto (Security by Design & Default) 4
8. Responsabilidad y trazabilidad 4
9. Coordinación, cooperación y cumplimiento legal 4
10. Compromiso de la Dirección 4
Comunicación y difusión 5
Aprobación 5

Compromiso institucional

La **Dirección de Pluxee España S.A.U**, consciente de la importancia de garantizar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información y los servicios que gestiona, establece la presente **Política de Seguridad de la Información** en cumplimiento del **Esquema Nacional de Seguridad (ENS, Real Decreto 311/2022),** de la norma **ISO/IEC 27001:2022**, de los requisitos del estándar **PCI DSS** y las políticas corporativas del **Grupo Pluxee**.

El objetivo de esta política es **proteger la información y los servicios** frente a riesgos o incidentes que puedan afectar a la organización, sus clientes, usuarios, empleados y proveedores, garantizando la **confianza, continuidad y resiliencia** en todas sus operaciones.

Comité de Seguridad de la Información

Pluxee España cuenta con un **Comité de Seguridad de la Información**, órgano colegiado responsable de coordinar, supervisar y garantizar la correcta aplicación de las políticas, normas y medidas de seguridad dentro de la organización.
Entre sus funciones destacan:

- Aprobar y revisar anualmente la **Política de Seguridad de la Información** y su documentación asociada.
- Analizar los riesgos, incidentes e informes de auditoría en materia de seguridad y proponer medidas correctoras.
- Supervisar la eficacia de las medidas de seguridad y promover la mejora continua del sistema.
- Garantizar la **difusión interna** de las políticas, procedimientos y buenas prácticas de seguridad.
- Coordinar la **formación y concienciación en ciberseguridad** de todo el personal.
- Verificar la adecuada integración de los controles de seguridad en los contratos con proveedores TIC.

El Comité está integrado, al menos, por el **CEO**, el **Responsable de Seguridad**, el **Responsable de Sistemas**, el **Responsable de Información y Servicios**, y otras figuras de apoyo técnico o jurídico según la materia tratada.

Se reúne con carácter ordinario al menos una vez al año y de manera extraordinaria cuando la situación lo requiera. De cada reunión se levanta acta formal de los acuerdos y acciones.

Responsables de Seguridad

Conforme al artículo 10 del ENS, Pluxee España S.A.U. designa las siguientes figuras:

- **Responsable de la Información:** define los requisitos de seguridad de la información gestionada y vela por su protección.
- **Responsable del Servicio:** determina los requisitos de seguridad aplicables a los servicios ofrecidos a clientes y usuarios.
- **Responsable del Sistema:** implementa las medidas técnicas necesarias para garantizar la protección de los sistemas TIC.

- **Responsable de Seguridad:** coordina la aplicación del ENS, asesora a la Dirección y lidera el Comité de Seguridad.

Estas figuras actúan de forma coordinada, bajo el principio de separación de funciones y responsabilidad no delegable, con el apoyo del Comité de Seguridad de la Información.

Alcance y aplicación

Esta política aplica a:

- **Todos los sistemas de información, procesos, personas y proveedores de Pluxee España S.A.U.**
- **Los servicios tecnológicos internos y externalizados, incluidos aquellos sujetos a certificaciones ISO/IEC 27001, PCI DSS y ENS nivel medio.**
- **Todos los empleados, contratistas y terceros que accedan o procesen información de la organización.**

Principios de seguridad

Pluxee España orienta su Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los principios establecidos en el Esquema Nacional de Seguridad (ENS), en la ISO/IEC 27001:2022, y en la legislación vigente sobre protección de datos.
Estos principios inspiran todas las decisiones, políticas y actuaciones relacionadas con la protección de los activos de información, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas y servicios de la organización.

---

1. Prevención, detección y vigilancia continua
Pluxee España adoptará una postura proactiva ante las amenazas a la seguridad, estableciendo medidas de prevención, detección temprana y respuesta eficaz frente a vulnerabilidades o incidentes.
Se mantendrá un modelo de vigilancia continua, apoyado en herramientas de monitorización y alerta, que permita identificar comportamientos anómalos y anticipar riesgos antes de que se materialicen.

---

2. Gestión del riesgo y mejora continua (PDCA)
Toda decisión en materia de seguridad se basará en una evaluación sistemática de riesgos, conforme a la metodología definida en el ENS y alineada con la norma ISO/IEC 27005.
Los controles se establecerán bajo el principio de proporcionalidad, garantizando una relación equilibrada entre coste, impacto y beneficio.
El sistema se mantendrá en un ciclo de mejora continua (Plan-Do-Check-Act), integrando auditorías, revisiones y acciones correctivas que refuercen la resiliencia de la organización.

---

3. Protección de los datos personales y cumplimiento normativo
Pluxee España garantiza el pleno cumplimiento del Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y el Esquema Nacional de Seguridad (ENS), asegurando la protección de los datos personales y la privacidad de los interesados.
Las medidas técnicas y organizativas se adoptarán conforme a los principios de minimización, limitación de la finalidad, licitud y responsabilidad proactiva.

---

4. Continuidad del negocio y resiliencia operativa
La organización asegurará la disponibilidad de los servicios esenciales mediante la implantación y prueba periódica de Planes de Continuidad de Negocio (BCP) y Planes de Contingencia (DRP), de acuerdo con los requisitos del ENS.
Estos planes definirán los objetivos de recuperación (RTO, RPO) y garantizarán la capacidad de respuesta y recuperación ante desastres o incidentes críticos.

---

5. Formación y concienciación en seguridad
La seguridad de la información es responsabilidad de todo el personal de Pluxee España.
La organización desarrollará programas de formación y concienciación en ciberseguridad de carácter anual, adaptados a los distintos perfiles y funciones, promoviendo una cultura de seguridad transversal y sostenible en el tiempo.

---

6. Control y supervisión de terceros y proveedores
Todo tercero o proveedor con acceso a información o sistemas de Pluxee España deberá cumplir con los requisitos de seguridad del ENS y las cláusulas contractuales específicas en materia de confidencialidad y ciberseguridad.
La organización establecerá mecanismos de evaluación y supervisión continua de proveedores, verificando su conformidad y nivel de madurez en seguridad antes, durante y después de la prestación del servicio.

---

7. Seguridad desde el diseño y por defecto (Security by Design & Default)
Todos los proyectos, servicios y desarrollos tecnológicos incorporarán la seguridad desde las fases iniciales de diseño, garantizando la confidencialidad, integridad y disponibilidad de los datos desde su origen.
Se aplicará el principio de seguridad por defecto, asegurando que las configuraciones iniciales minimicen los riesgos y restrinjan los accesos innecesarios.

---

8. Responsabilidad y trazabilidad
Cada acción sobre los sistemas de información deberá ser rastreable y atribuible a un responsable identificado.
Se mantendrán roles definidos (Responsable de la Información, del Servicio, del Sistema y de Seguridad), conforme al ENS, asegurando la separación de funciones y la rendición de cuentas en todo el ciclo de vida de la información.

---

9. Coordinación, cooperación y cumplimiento legal
Pluxee España colaborará activamente con las autoridades competentes, organismos de ciberseguridad y el CCN-CERT cuando proceda, garantizando una comunicación ágil ante incidentes de seguridad.
Toda actuación se ajustará a la legislación vigente y a las políticas internas de cumplimiento normativo y ética corporativa.

---

10. Compromiso de la Dirección
La Alta Dirección de Pluxee España asume el compromiso de dotar los recursos humanos, técnicos y financieros necesarios para garantizar la seguridad de la información y mantener el cumplimiento del ENS.
El Comité de Seguridad de la Información supervisará de forma continua la eficacia del sistema y la correcta aplicación de estos principios.

Comunicación y difusión

La versión vigente de la Política de Seguridad se encuentra disponible en la **intranet corporativa** y en los canales públicos de Pluxee España S.A.U.

Todo el personal y los proveedores con acceso a los sistemas o datos de la organización deberán:

- Conocer y aceptar el contenido de esta Política.
- Cumplir las normas, procedimientos y estándares técnicos que la desarrollan.
- Participar en las acciones de formación y concienciación establecidas.

Aprobación

La presente **Política de Seguridad de la Información** ha sido aprobada por la **Dirección Ejecutiva** y el **Comité de Seguridad de la Información** de Pluxee España S.A.U.

Su revisión se efectuará **al menos una vez al año**, o cuando se produzcan cambios significativos en los sistemas, la estructura organizativa o la normativa aplicable.