Política de Seguridad

Esquema Nacional de Seguridad [RD 311/2022]

ISO 27001:2022-SGSI-Seguridad de la Información

Departamento IT & PMO

Control de Versiones

Versión	Responsable	Fecha	Cambio
1.0	Dirección	16/12/2019	Versión inicial de la política
2 0	Responsable de calidad	30/10/2020	Revisión anual y actualización de responsabilidades
3.0	Responsable de calidad	01/04/2025	Revisión por la Dirección. Actualización a contexto tecnológico actual
4.0	Responsable SGI	20/04/2026	Unificación ENS (RD 311/2022) + ISO/IEC 27001:2022.

Revisado	Aprobado
Responsable de Seguridad	Dirección General

ÍNDICE

1. Introducción y contexto de la organización

EXCELTIC, S.L. es una empresa de servicios tecnológicos cuya actividad depende en gran medida de los sistemas de información y de la prestación de servicios gestionados a terceros. En este contexto, la seguridad de la información se considera un elemento estratégico esencial para garantizar tanto la continuidad del negocio como el cumplimiento de obligaciones legales y contractuales con clientes

EXCELTIC, S.L. asume su compromiso con la seguridad de la información y se compromete a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la información utilizada y a los servicios prestados. La protección de los activos de información propios y de los clientes es una prioridad clave.

La organización adopta un enfoque preventivo, orientado a minimizar la probabilidad de incidentes de seguridad y a reducir su impacto cuando sean inevitables, ya sean por causas accidentales o deliberadas

Partes interesadas (ISO 27001:2022 cláusulas 4.1 y 4.2): se identifican como partes interesadas relevantes para el SGSI los clientes, los empleados, los proveedores y las autoridades regulatorias. Sus requisitos, expectativas y obligaciones legales aplicables son considerados en la planificación y operación del SGSI.

2. Objetivo

El objetivo principal de esta Política es garantizar la protección de la información en cualquier formato o medio, asegurando los siguientes pilares fundamentales:

- **Confidencialidad:** acceso restringido únicamente a personas autorizadas, evitando usos indebidos o divulgación no autorizada, especialmente en datos personales.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus procesos asociados
- **Disponibilidad:** acceso garantizado a la información cuando sea necesario para el desarrollo de las actividades y servicios.
- **Autenticidad y trazabilidad:** garantía de la identidad de quien accede a la información y registro de las acciones realizadas
- **Cumplimiento normativo:** adecuación a la normativa vigente, incluyendo RD 311/2022 (ENS), ISO/IEC 27001:2022, RGPD y LOPDGDD

3. Alcance

Esta Política se aplica a los sistemas de información que dan soporte a los servicios de Ingeniería de Asistencia Técnica y Desarrollo de Proyectos Tecnológicos de EXCELTIC, S.L., conforme a la Declaración de Aplicabilidad vigente.

Abarca todos los activos de información asociados a dichos servicios, incluyendo:

- Sistemas, redes e infraestructuras tecnológicas (entornos físicos y en la nube)
- Datos y documentación, tanto de EXCELTIC, S.L. como de sus clientes.
- Procesos de negocio que tratan información objeto del alcance
- Personal propio, colaboradores, proveedores y terceros con acceso a la información o sistemas incluidos en el alcance.

4. Marco normativo de referencia

La presente Política se basa en los siguientes estándares y normativas de referencia:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)
- ISO/IEC 27001:2022 — Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27002:2022 Controles de seguridad de la información
- Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD).
- Guías CCN-STIC aplicables al ENS y a los sistemas del alcance
- Ley 34/2002 (LSSI), Ley 39/2015 y Ley 40/2015, en lo aplicable a los servicios prestados a las Administraciones Públicas.
- Obligaciones contractuales con clientes y otros requisitos legales aplicables

5. Principios de seguridad

La gestión de la seguridad de la información se basa en los siguientes principios:

- **Definición de objetivos anuales** alineados con el negocio y los riesgos.
- **Gestión sistemática de riesgos**, incluyendo análisis, evaluación y tratamiento continuo.
- **Implementación de controles de seguridad** en función de los riesgos detectados y conforme a la Declaración de Aplicabilidad.
- **Garantía de continuidad del negocio**, mediante planes actualizados y probados regularmente
- **Concienciación y formación del personal**, asegurando su implicación activa.
- **Notificación e investigación de incidentes**, sin tolerancia a incumplimientos legales
- **Cumplimiento de requisitos legales y contractuales**, incluyendo el ENS y la ISO 27001.
- **Revisión periódica del sistema de gestión**, asegurando su eficacia

- **Mejora continua**, mediante acciones correctivas y optimización constante.
- **Seguridad por defecto y desde el diseño**, integrada en todo el ciclo de vida de los sistemas y servicios

6. Contexto de riesgos actuales

El entorno de amenazas ha evolucionado significativamente, destacando los siguientes riesgos principales:

- **Ransomware y ciberextorsión:** especialmente relevantes en empresas tecnológicas como punto de acceso a clientes.
- **Accesos no autorizados y exposición de credenciales:** asociados al trabajo remoto y entornos híbridos.
- **Vulnerabilidades en cloud y SaaS:** necesidad de configuración segura continua.
- **Cumplimiento normativo complejo:** múltiples marcos regulatorios simultáneos (ENS, ISO 27001, RGPD).
- **Ingeniería social y phishing:** dirigidos especialmente a personal con privilegios.
- **Riesgos en la cadena de suministro:** proveedores críticos y servicios externalizados.

Estos riesgos se gestionan mediante un Sistema de Gestión de Seguridad de la Información (SGSI), con revisiones periódicas y actualización constante conforme al procedimiento de Análisis de Riesgos vigente

7. Organización de la seguridad

La responsabilidad última sobre la seguridad de la información recae en la Dirección General de EXCELTIC, S.L., que dispone los medios necesarios para el cumplimiento de esta Política. Para la organización de la seguridad conforme al ENS, se definen los siguientes roles:

Rol / Función	Deberes y responsabilidades
Responsable de la Información	Tiene la responsabilidad última sobre el uso que se hace de la información y, por tanto, de su protección. Determina los requisitos de seguridad de la información tratada y aprueba los niveles de seguridad exigibles.
Responsable del Servicio	Define los requisitos de los servicios prestados y establece los niveles de servicio aceptables Determina los requisitos de seguridad aplicables al servicio

Rol / Función	Deberes y responsabilidades
Responsable de la Seguridad	Mantiene la seguridad de la información manejada y de los servicios prestados. Supervisa la aplicación de las medidas de seguridad, la elaboración de la Declaración de Aplicabilidad y el cumplimiento del ENS y de la ISO 27001. Gestiona los incidentes de seguridad. También es responsable de la implantación, gestión y mantenimiento operativo de las medidas de seguridad técnicas
Responsable del Sistema	Desarrolla, opera y mantiene el sistema de información durante todo su ciclo de vida, incluidas sus especificaciones, instalación y verificación de su correcto funcionamiento.
Dirección	Proporciona los recursos necesarios para el Sistema de Gestión de Seguridad de la Información (SGSI), lidera y aprueba la política, revisa periódicamente su eficacia y garantiza su cumplimiento

La designación nominal de estos roles se formaliza en el apartado 8 (Comité de Seguridad) y en el documento Registro de responsables, roles y responsabilidades Las diferencias de criterio que pudieran derivar en un conflicto se tratarán en el seno del Comité de Seguridad, prevaleciendo en todo caso el criterio de la Dirección General.

8. Comité de seguridad de la información

El Comité de Seguridad de la Información es el órgano con mayor responsabilidad dentro del SGSI; en él se acuerdan todas las decisiones relevantes relacionadas con la seguridad de la información Actúa con autonomía ejecutiva y no subordina su actividad a ningún otro elemento de la empresa.

La composición actual del Comité de Seguridad es la siguiente:

Cargo
Responsable de Seguridad
Responsable del Sistema
Responsable del Servicio
Responsable de la Información

El Comité se reúne con una periodicidad mínima semestral (y siempre que sea necesario ante un incidente grave o un cambio significativo del contexto), levanta acta de sus acuerdos y

aprueba las decisiones por mayoría El procedimiento para la designación, renovación y cese de sus miembros es la ratificación por el propio Comité.

9. Gestión de riesgos

Todos los sistemas incluidos en el alcance de esta Política están sujetos a un análisis de riesgos, que identifica y evalúa las amenazas y vulnerabilidades a las que están expuestos Este análisis se revisa:

- Al menos una vez al año.
- Cuando cambie significativamente la información manejada o los servicios prestados
- Cuando se produzca un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves que afecten a los sistemas del alcance

La metodología aplicada es la establecida en el procedimiento Análisis de Riesgos, alineado con los requisitos del ENS y de la ISO 27001:2022. El Comité de Seguridad establece valoraciones de referencia comunes para los tipos de información y servicios, y dinamiza los recursos necesarios para el tratamiento de los riesgos identificados Los análisis de riesgos están unificados sobre el mismo inventario de activos

10. Gestión de personal y concienciación

Todos los miembros de EXCELTIC, S.L. tienen la obligación de conocer y cumplir esta Política de Seguridad y la Normativa de Seguridad complementaria. El Comité de Seguridad garantiza que esta información llega a todo el personal afectado

En materia de formación y concienciación:

- Todo el personal atiende al menos una sesión anual de concienciación en materia de seguridad de la información
- Se establece un programa continuo de concienciación que atiende especialmente al personal de nueva incorporación.
- El personal con responsabilidad en el uso, operación o administración de sistemas TIC recibe formación específica antes de asumir sus funciones o ante cambios significativos del puesto.
- Recursos Humanos incluye funciones de seguridad en las descripciones de puesto, gestiona los compromisos de confidencialidad y coordina la capacitación del personal

Todo el personal tiene la obligación de notificar, a través de los canales establecidos, las debilidades e incidentes de seguridad de la información que detecte.

11. Responsabilidades generales

La seguridad de la información es una responsabilidad compartida por toda la organización:

- **Dirección:** Aprueba la Política y garantiza la disponibilidad de recursos.
- **Responsables de área y mandos intermedios:** aseguran el cumplimiento dentro de sus equipos y del personal a su cargo
- **Responsable de Seguridad:** asesora, supervisa y mantiene las medidas de seguridad y coordina la respuesta a incidentes.
- **Empleados, colaboradores y terceros:** deben proteger la información a la que acceden, no hacer uso indebido de ella y notificar incidentes o debilidades.

El cumplimiento de esta Política es obligatorio para todo el personal interno, proveedores, colaboradores y visitantes, así como el estricto cumplimiento de las leyes y obligaciones contractuales aplicables Los incumplimientos se tratarán conforme al régimen disciplinario vigente

12. Revisión por la dirección

La Dirección revisa la política del SGSI al menos una vez al año para garantizar su idoneidad, adecuación y eficacia. La revisión incluye:

- Seguimiento de acciones previas.
- Cambios en el contexto organizativo.
- Resultados de la evaluación y tratamiento de riesgos.
- Resultados de auditorías internas y externas, e indicadores del SGSI
- Cumplimiento normativo y estado de la Declaración de Aplicabilidad.
- Incidentes de seguridad y acciones derivadas.
- Identificación de oportunidades de mejora.

13. Mejora continua

EXCELTIC, S L establece un proceso de mejora continua del SGSI, aplicando los criterios y la metodología establecidos en la ISO/IEC 27001:2022 y en el ENS (RD 311/2022). Este proceso se apoya en el ciclo PDCA (Plan-Do-Check-Act), en los resultados de auditorías internas y externas,

en el tratamiento de no conformidades y acciones correctivas, y en la actualización periódica del análisis de riesgos y de la Declaración de Aplicabilidad.

Aprobación: la presente Política es aprobada por la Dirección General de EXCELTIC, S.L. y entra en vigor desde la fecha de su firma, permaneciendo vigente hasta que sea reemplazada por una nueva versión. Su revisión es, como mínimo, anual.