# Política de Seguridad

## Conforme a ENS e ISO 27001

Tipo de documento: Público

Berger Levrault

# Índice



# 1. Introducción

La Alta Dirección ha considerado necesario incluir una declaración única y extensible a toda la entidad, relativa a necesidad de gestionar la seguridad como un todo, transversal en toda la organización, en cada área y en cada proceso –interno y externo–, como una cuestión estratégica de la organización.

La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) está condicionada a las necesidades de negocio y a las líneas marcadas por los objetivos organizacionales, entre los que se encuentran actualmente, los objetivos de seguridad. Todos los procesos internos y externos quedan adscritos y afectos a la presente Política de Seguridad, o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La organización ha considerado preciso plasmar la política en un documento escrito que encabezara cuantos procesos de seguridad se integren en los procesos de trabajo y en los objetivos de negocio.

La organización debe cerciorarse de que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema y de la información, desde el diseño de un producto o un servicio hasta su retirada. Incluyendo las diferentes fases de desarrollo o adquisición y la propia producción o explotación. El sistema deberá estar diseñado para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad.

A lo largo del presente documento se integran de manera clara:

a) Los objetivos de negocio de la organización.
b) El marco legal y regulatorio aplicable y afecto.
c) Los roles o funciones de seguridad.
d) La estructura del órgano para la gestión y coordinación de la seguridad.
e) Las directrices para la estructuración del sistema.

Todo el sistema está estructurado y cumple las premisas derivadas de una gestión de información documentada y como tal debe adecuarse y seguirse.

## 1.1 Normativa aplicable

La seguridad de la organización considerada en el presente documento de alto nivel está alineada con:

- Norma UNE ISO/IEC 27001:2017.
- Real Decreto por el que se regula el Esquema Nacional de Seguridad (en adelante, "ENS").
- La seguridad de la información personal, derivada del Reglamento (UE) 2016/679 de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- La Directiva (UE) 2016/1148 (Directiva NIS), el Real Decreto-ley 12/2018 (Ley NIS) y el Real Decreto 43/2021 (Reglamento NIS) sobre seguridad de redes y sistemas de información.
- [1]Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

También quedan implicadas el resto de las normas del sector, normas internacionales, comunitarias, nacionales, autonómicas y locales que sean de aplicación, que se detallan en el proceso de normativa aplicable de la organización.

## 1.2 Estándar de seguridad de la información

La dirección ha considerado emplear estándares de seguridad para alinear los procesos y la seguridad del sistema de información, tomando como referencia el ENS y la norma UNE ISO/IEC 27001:2017, junto con otras normas de uso no obligatorias pero de referencia, y específicamente la serie de Guías 800 publicadas por el Centro Cristológico Nacional CCN-CERT.

En base a ello, se ha desarrollado un sistema paralelo a otros estándares de los que se beneficiará cuando los estándares sean compatibles con los requisitos propios de un Sistema de Gestión de la Seguridad de la Información, considerando las particularidades del negocio de la organización y del cliente tipo existente al que se dirige el proceso de venta.

[1] Se considera la colaboración con el sector público para dar cumplimiento a la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

El sistema debe ser administrado con diligencia, tomando las medidas adecuadas para proteger la información frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información.

Para defenderse de las amenazas, se requiere una estrategia de seguridad que se adapte a los cambios en las condiciones del entorno para garantizar la seguridad de nuestro sistema y el adecuado servicio prestado de manera continua. Esto implica que todos los recursos deben disponer y aplicar aquellas medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II del ENS, en solitario o en conjunto con aquellos controles paralelos y de análoga naturaleza que pudiera decidir la organización. Estos controles se detallan en la declaración de aplicabilidad de la organización, aprobada y en vigor.

La organización considera la necesidad de someterse a una revisión de conformidad que implica una declaración o certificación de un tercero externo independiente, que permita acreditar la alineación del sistema de gestión implantado a la norma ENS y a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

# 2. Objetivo de la Política de Seguridad de la Información

El objetivo de la Política de Seguridad es la protección de los activos que soportan el sistema de información de la organización y los procesos internos implicados en los servicios declarados, quedando afectadas las tres dimensiones de seguridad –confidencialidad, integridad y disponibilidad–, y cuando fuera preciso, incorporando otras dimensiones –autenticidad y trazabilidad– (por requerimiento legal y por decisión de la Alta Dirección), quedando alineada plenamente con los objetivos de negocio e integrándose en la estrategia de la empresa.

La organización declara como servicios aquellos que se desarrollan de manera externa a un cliente, agrupándose en: diseño y desarrollo de software, consultoría de producto o software, implantación de producto o software, formación a usuario final, vigilancia y mejora y soporte.

**Diseño y desarrollo de software:**

- Análisis de requisitos
- Diseño y arquitectura
- Programación
- Pruebas
- Certificación
- Documentación
- Mantenimiento

**Consultoría para el asesoramiento personalizado en soluciones y/o software**

**Implantación de productos / software:**

- Lanzamiento y toma de requisitos
- Integración sistema interno (análisis, pruebas, migración, producción)
- Conexiones in situ / en remoto
- Cierre y aceptación

**Hosting (gestionado):**

- Sistema de copias de seguridad y pruebas de restauración
- Acciones preventivas y reactivas sobre el hosting

**Formación (usuarios del sistema)**

**Servicio de vigilancia (actualizaciones y versiones mejoradas)**

**Actividades de soporte y mantenimiento**

- Gestión de comunicación (llamada, correo o web-chat)
- Resolución de la incidencia (con / sin conexión en remoto)
- Informes de mediciones, indicadores y tendencias.

## 2.1 Objetivos de seguridad de la información

Los objetivos de seguridad de la Información, definidos por Berger-Levrault España para todas las empresas del grupo, han sido desarrollados y aprobados por la dirección, considerando los requerimientos identificados de las

partes interesadas (internas y externas), el cumplimiento legal, la gestión de los riesgos y el cumplimiento de los requisitos de seguridad establecidos por la alta dirección y detallados en la declaración de aplicabilidad.

La organización ha establecido los siguientes **objetivos clave** de la seguridad de la información:

1. **Mantener el pleno cumplimiento legal,** alineando los procesos y los servicios, a la normativa vigente en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (administración pública), a la información implicada (*pública, restringida o secreta*) o en general a la seguridad de la información y/o servicio.
2. **Mantener una alineación del sistema de gestión de seguridad a la norma de referencia** (ENS y estándar UNE ISO/IEC 27001:2017), estructurando la gestión eficiente y eficaz de la seguridad de acuerdo a aquella y a las buenas prácticas del sector (incluyendo las Guías publicadas por el CCN-CERT), conformes con la misma.
3. **Establecer y difundir los roles y responsabilidades** relacionados con la Seguridad de la Información.
4. **Sensibilizar y concienciar** de manera estable y permanente al usuario de la organización mediante el impulso de acciones por la dirección y la ejemplificación de la misma en las tareas de seguridad más críticas.
5. **Fomentar y mantener una buena reputación de la organización,** en relación a los servicios y la seguridad desarrollados.
6. **Disponer de respuestas a los incidentes de seguridad**, mediante respuesta activa –reactiva y proactiva– y acciones preventivas y detectivas, y cuando fuera preciso acciones de respuesta y recuperación, adecuadas y detalladas.
7. **Asegurar que los activos de la organización sólo sean utilizados por usuarios autorizados** en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
8. **Proteger la información** interna y la relacionada con la prestación de los servicios / clientes, considerando las dimensiones de:
    - **Confidencialidad:** Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - **Integridad:** Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - **Disponibilidad:** La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
    - **Trazabilidad:** Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
    - **Autenticidad:** Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

# 3. Principios de seguridad

La dirección ha aprobado el desarrollo de una estrategia de seguridad materializada en una gestión que ha sido diseñada / establecida, implementada, mantenida y mejorada, conforme al ciclo de Deming, a los efectos de lo dispuesto en el estándar UNE-EN ISO/IEC 27001:2017 y considerando lo establecido en el control [org.1] del ENS.

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

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por la dirección. Todo el sistema estará enmarcado por los principios de seguridad.

El sistema puede apoyarse en otros sistemas de gestión, como el desarrollado para la calidad del producto o servicio conforme al estándar UNE-EN ISO 9001:2015. El sistema llamará a los procesos o procedimiento que desarrollen los principios, los requisitos o los controles de seguridad y trazará la correspondencia.

**La dirección ha establecido como requerimiento de seguridad el pleno cumplimiento de las obligaciones legales y contractuales ligadas a la información y a los servicios. Los requisitos serán identificados y organizados para su correcta gestión.**

## 3.1 Organización e implantación del proceso de seguridad

La seguridad deberá comprometer a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

### 3.1.1 La Dirección

La Dirección será quien lidere la organización y promueva la cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso desarrollado o servicio a terceros. Con carácter general se deriva la seguridad al Comité de Seguridad.

### 3.1.2 El Comité de Seguridad

En el Comité de Seguridad podrán integrarse los Responsables de áreas o departamentos, Responsables de Producto(s), Responsables de clientes o de contratos, Responsable de Sistemas, Coordinador de IT y Responsable de Calidad. El Comité de Seguridad reportará sus actividades a la Dirección General. De entre todos los integrantes se designa un Responsable de Seguridad y del Comité, que aceptará su cargo y sus responsabilidades (según modelo ACTA) y podrá apoyarse en uno o varios delegados. El cargo de Responsable podrá segregarse en uno o varios Responsables de Seguridad. La designación de roles se ha establecido a la luz del principio de separación de funciones. Las designaciones serán revisadas en el ciclo de dos años, iniciándose el cómputo del plazo en el proceso de declaración o certificación de conformidad del sistema con respecto al ENS.

Si los incidentes de seguridad, una vez registrado y valorados en el Registro de Aprendizaje de Incidentes de Seguridad, tienen impacto en cliente y además una prioridad crítica se convocará al Comité de Seguridad.

Atendiendo a las necesidades, se convocará a todos o a algunos de los participantes en el Comité de Seguridad de la Información.

El Comité de Seguridad podrá formar parte de otros Comités de Gestión, pero será el responsable de coordinar, evaluar y proponer mejoras para la Seguridad de Información y Servicios.

Las **reuniones** del comité y sus puntos concretos serán recogidas en actas en las que se incluirán los acuerdos más característicos, así como las acciones que deberán llevarse a cabo para cumplir con los objetivos de seguridad. La convocatoria se podrá realizar por el Responsable de Seguridad, el Responsable del Sistema o sus delegados, con al menos una semana de antelación para convocatorias ordinales. Para convocatorias extraordinarias que puedan tener carácter urgente, el plazo de convocatoria podrá ser inferior al de las convocatorias ordinarias.

**La seguridad del sistema será revisada** por el Comité, de conformidad a los requisitos, la política y los procedimientos aprobados por la dirección. Las revisiones serán por parte de la dirección y por revisiones internas o auditorias del sistema.

La seguridad del sistema se documentará mediante procedimientos de operación que serán puestos a disposición de los usuarios implicados en el mismo.

Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados.

Se documentarán los acuerdos con proveedores y colaboradores formando parte del sistema. La cadena de suministro será controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudieran tener el sistema.

Las comunicaciones serán gestionadas, desde entornos de redes a intercambios operativos incluidos en los procesos. Se incluirá cuando sea necesario, el cifrado o el control de comunicaciones de mensajería instantánea.

Para soportar esta política general, se establecerán políticas de seguridad, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio de las empresas pertenecientes al grupo BLE, si procede.

## 3.2 Análisis y gestión de los riesgos

La gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado en el seno de la organización, bajo el liderazgo de la dirección.

La gestión de riesgos permitirá el mantenimiento de un entorno de seguridad diferencial controlado, minimizando los riesgos hasta niveles aceptables para la dirección. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de la información, los riesgos a los que estén expuestos y las medidas de seguridad.

La gestión de riesgos se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en una metodología detallada y documentada que permita la repetición de la medición y análisis. Esta metodología permitirá que se repita el Análisis de Riesgo a intervalos planificados y al menos una vez al año, salvo que no hubiera modificaciones y cada vez que el sistema tenga cambios sustanciales, o cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

## 3.3 Gestión de personal y profesionalidad

Todo el personal relacionado con el sistema y con la información deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, debiendo ser controlados y sus acciones supervisadas para verificar que se siguen los procedimientos de seguridad y la aplicación de los principios de seguridad en el desempeño de sus funciones. El personal conocerá la presente política y deberá disponer de los medios necesarios para cumplir lo establecido en ella.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe 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 determinada actividad.

La responsabilidad será exigible mediante un procedimiento disciplinario que, como las pautas de seguridad, conocerá previamente el usuario.

El usuario con acceso concedido al sistema pueda o no desarrollar acciones, estará sometido a secreto y reserva, aun cuando finalice su relación con la organización.

La seguridad de los sistemas estará gestionada en todas sus magnitudes, por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: diseño, desarrollo, instalación, mantenimiento, gestión de incidencias y desmantelamiento. Se considerará como recurso a todo usuario propio o de un tercero. Se establecerá un programa de concienciación y capacitación según necesidades, de manera continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Los recursos serán gestionados conforme a la política de recursos humanos aprobada.

## 3.4 Autorización y control de los accesos

La organización ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados, restringiendo el acceso a las funciones permitidas.

## 3.5 Protección de las instalaciones

La organización prevendrá los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Los activos se protegerán frente a actos vandálicos y especialmente frente a robos o interrupciones.

En las Políticas de Personal se recoge el uso aceptable de activos en la organización y especialmente de uso, reutilización o retirada de activos. Se contempla la autorización de uso de equipos o dispositivos propios de usuarios, ligados a la organización por vínculo profesional, siempre que se mantengan las medidas de seguridad aprobadas por la dirección.

Todos los puestos estarán alineados con la política de seguridad, con independencia de si se desarrollan funciones en áreas controladas por la organización o no.

## 3.6 Adquisición de productos y contratación de servicios de seguridad.

La organización tendrá en cuenta, para la adquisición de productos, que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 (también conocida como Common Criteria) u otras de naturaleza y calidad análogas.

## 3.7 Seguridad por defecto (Mínimo privilegio)

**La seguridad se entenderá como un proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

**Las funciones de operación, administración y registro de actividad** serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

**El uso del sistema será sencillo y seguro**, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Para mantener el proceso de seguridad integral, se realizará una **gestión de los activos** –de la información–, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad, implicando la trazabilidad y la autenticación. La clasificación conllevará necesariamente una política de inventariado, etiquetado y manipulación, gestionado de conformidad a su naturaleza y con identificación del responsable.

Se deberá conocer en todo momento el **estado de seguridad del sistema o de sus componentes**, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

## 3.8 Integridad y actualización del sistema

La organización ha implementado controles y evaluaciones regulares de la seguridad (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal. Asimismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

## 3.9 Protección de la información almacenada y en tránsito

La organización ha implementado mecanismos para proteger la información almacenada o en tránsito especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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

## 3.10 Prevención ante otros sistemas de información interconectados

La organización ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

## 3.11 Registro de actividad y detección de código dañino

La organización ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente 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 laboral, y demás disposiciones que resulten de aplicación.

Se implementan medidas para analizar las comunicaciones entrantes y salientes, 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.

## 3.12 Incidentes de seguridad

Se dispondrá de procedimiento(s) de gestión de incidentes de seguridad en el sistema. El proceso de gestión de incidentes incluirá la detección y notificación de las incidencias, los criterios de clasificación, los procedimientos de análisis y resolución, así los cauces de comunicación a las partes interesadas –especialmente cuando afecta a terceros– y el registro de las actuaciones ejecutadas.

La gestión de incidencias servirá al sistema para la mejora continua y para el control de tendencias relacionadas con la seguridad.

Los incidentes de seguridad permitirán la recopilación de evidencias, de manera que se podrá identificar, documentar la recogida, la adquisición y preservación de la información.

Existirá un registro de incidentes de seguridad que permitirá la evaluación de los mismos, de sus tiempos de resolución y de las tendencias.

## 3.13 Continuidad de la actividad

La continuidad formará parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización dispondrá de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Cuando sea necesario por ser requisito legal, la entidad realizará un análisis de impacto y detallará un procedimiento de continuidad con sus correspondientes pruebas. Se podrá desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.

### 3.14 Mejora continua del proceso de seguridad

La organización actualizará y mejorará de forma continua el proceso de seguridad integral implantado, en línea a los requisitos de las normas de seguridad implantadas.

### 3.15 Seguridad con terceras partes

La entidad desarrollará los servicios conforme a la presente política y cuando se trate de Administraciones Públicas, les hará participes de la presente, y de cuantos procesos y procedimientos afecten a la seguridad de la información y /o servicio.

Cuando se establezca una cadena de suministro en la gestión o administración de soluciones a terceros, se mantendrá la presente política aplicable a todos los eslabones presentes. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en la misma, se requerirá un informe del Responsable de Seguridad que revise y concrete los riesgos en que se incurre y la forma de tratarlos.

Cualquier 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.

# 4. Alcance

La presente política afecta a toda la organización, y colaboradores externos si procede, y en concreto, al sistema de información que soporta los servicios identificados y los procesos tanto internos como externos, que son necesarios para desarrollar y cumplir con los objetivos de negocio.

La política de seguridad de la información se aplicará **a toda la información** del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, **a todo el personal** de las distintas empresas de BLE. y también terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como **a cualquier activo** de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad, de manera que cuando el sistema se encuentre en fase de actualización, el activo no registrado se vea obligado por la política.

En el ámbito del Esquema Nacional de Seguridad, será considerado alcance del sistema para Aytos Soluciones Informáticas y ABS Informática:

> ***"Sistema de información propiedad de AYTOS SOLUCIONES INFORMÁTICAS S.L.U., para la provisión, migración, administración, mantenimiento y soporte de software en la modalidad On-Premise y en modalidad Software como Servicio (SaaS), conforme a las disposiciones del Real Decreto 3/2010, catálogo de servicios y Declaración de Aplicabilidad vigente."***
>
> ***"Sistema de información propiedad de ABS INFORMÁTICA S.L.U., para la provisión, migración, administración, mantenimiento y soporte de software en la modalidad On-Premise y en modalidad Software como Servicio (SaaS), conforme a las disposiciones del Real Decreto 3/2010, catálogo de servicios y Declaración de Aplicabilidad vigente***."

Este alcance se completa con un anexo al certificado, que recogerá el listado de servicios afectados.

Y en el ámbito de la ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información, será considerado el alcance del sistema para Berger-Levrault España (Aytos Soluciones Informáticas y ABS Informática):

> ***"Los sistemas de información que dan soporte a las actividades de desarrollo, comercialización, consultoría y soportes relacionados con:***
> • ***Soluciones de sede electrónica.*** *Carpeta ciudadana, registro telemático, trámites electrónicos, portales de proveedores y portales del contribuyente y del empleado, perfiles y notificaciones.*
> • ***Sistema de gestión de expedientes.*** *Contratación, gestor documental, archivo y notificaciones electrónicas, firmas y BPM.*
> • ***Soluciones internas****. Gestiones económica financiera, gestión patrimonial, gestión tributaria y de recaudación, nóminas y gestión de recursos humanos.*
> • ***Soluciones transversales.*** *Territorio, padrón, tributos, registros, subvenciones.*
> • ***Soluciones móviles.***
> • ***Soluciones geolocalización.***
> ***En modalidad Software como Servicio (SaaS) e instalaciones en clientes (On-Premise); de acuerdo al documento de aplicabilidad vigente a la fecha de emisión del certificado.****"*

Esta política será accesible a todos los miembros de la organización, mediante su publicación en la intranet y en la web de Berger-Levrault para colaboradores externos.

# 5. Cumplimiento

La Política de Seguridad de la Información tendrá vigencia una vez aprobada por el Director General y puesta en conocimiento de todo el personal de la organización afectado, incluidos aquellos externos a los que sea de aplicación. La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente a la organización.

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario para personal de la organización, basándose en los convenios laborales colectivos que sean de aplicación. En el caso de los proveedores y colaboradores externos se aplicará lo establecido en los contratos vigentes.

La organización establece el correo seguridad.sgi-es@berger-levrault.com como canal de comunicación por parte del personal de Berger-Levrault España para cualquier incumplimiento de la presente Política de Seguridad.

# 6. Aprobación del Director General

El Director General de Berger-Levrault España, asume el compromiso de proveer todos los recursos y medios para la operación y mejora del Sistema de Seguridad de la Información, de las Políticas, Procedimientos, Instrucciones y Normas desarrolladas al efecto y del compromiso de velar por su cumplimiento.

El Director General demostrará su compromiso, mediante la:

- Revisión y aprobación de las Políticas de Seguridad de la Información.
- Participación en el desarrollo de una cultura de Seguridad.
- Divulgación del sistema.
- La asignación efectiva de recursos, conforme se produzcan crecimientos y aumentos de volumen del negocio.

Es aprobada en Écija a 27 de octubre de 2022 y se publica para su correcta difusión.