Política de seguridad

Versión	Fecha	Revisado por	Aprobado por	Modificación
1	04/09/2026	Resp. Seguridad	Comité Seguridad	

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. ALCANCE 3
3. INTRODUCCIÓN 3
4. MISIÓN 4
5. PRINCIPIOS RECTORES DE LA POLÍTICA 5
6. MARCO NORMATIVO 6
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 6
Funciones y responsabilidades 7
Resolución de Conflictos 10
Procedimientos de designación 10
8. TRATAMIENTO DE DATOS PERSONALES DE LA ENTIDAD 10
9. GESTIÓN DE RIESGOS 10
10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 11
11. OBLIGACIONES DEL PERSONAL 11
12. TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES 12
13. GESTIÓN DE INCIDENTES DE SEGURIDAD 13
14. MEJORA CONTINUA 13
15. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD 13
16. HISTÓRICO DE MODIFICACIONES 14

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información ha sido aprobada por el Comité de Seguridad de la Información con fecha 4 de septiembre de 2026, siendo efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. ALCANCE

A efectos de simplificación, en el presente documento se emplea la denominación BOGAN para referirse al grupo de entidades al que pertenecen, entre otras, Agintzari, Zabalduz e Hirube.

No obstante, el alcance del Sistema de Gestión de Seguridad de la Información y del proceso de certificación conforme al Esquema Nacional de Seguridad se circunscribe exclusivamente a las entidades Agintzari, Zabalduz e Hirube, cuyos sistemas de información han sido objeto de categorización y son objeto de auditoría.

En consecuencia, esta política se aplica a los sistemas de información de Agintzari, Zabalduz e Hirube, a las personas que forman parte de dichas entidades y a los prestadores de servicios o proveedores de soluciones TIC que intervengan en dichos sistemas. La referencia a BOGAN en el resto del documento deberá entenderse limitada a este alcance, salvo que se indique expresamente lo contrario.

3. INTRODUCCIÓN

Los sistemas de información de BOGAN sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

BOGAN debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

4. MISIÓN

BOGAN tiene como objeto social impulsar, fomentar, coordinar, completar y garantizar las tareas de las cooperativas que agrupa en su seno, ofreciendo la prestación de servicios técnicos, de asesoramiento, consultoría, formación, gestión, administración, contabilidad, jurídicos, comerciales y de representación institucional tanto de la Cooperativa de Segundo Grado como de sus Cooperativas socias.

Las actividades que integran el objeto social de BOGAN habrán de ser desarrolladas, al menos en los aspectos básicos del compromiso cooperativo, directamente por la misma, y por sus cooperativas socias; sin perjuicio de ello, dichas actividades podrán ser facilitadas, completadas, coordinadas a través de otras entidades en las que la misma participe o con las que llegue a acuerdos de cooperación.

Con respecto a las cooperativas socias, la finalidad última de esta cooperativa de segundo grado reside en la consecución de la máxima eficiencia empresarial y de prestación de servicios en interés común para la sociedad, y del conjunto de entidades y servicios prestados mediante la oferta de unos servicios complementarios, la coordinación de sus actividades y la representación institucional de las mismas.

Estos servicios se prestan a través de diferentes entidades y modelos operativos, entre los que se incluyen los sistemas asociados a Zabalduz, Agintzari e Hirube, así como los servicios de soporte necesarios para su funcionamiento.

Como consecuencia de la naturaleza de su actividad, BOGAN trata información de carácter personal, en muchos casos de especial sensibilidad, asociada a procesos de intervención social, lo que exige garantizar su adecuada protección y el cumplimiento de la normativa aplicable.

La entidad asegura que todos los sistemas de información que soportan sus servicios se gestionan conforme a criterios de seguridad basados en el riesgo, garantizando la disponibilidad de los servicios, la confidencialidad e integridad de la información y la continuidad de las actividades desarrolladas, en alineación con el Esquema Nacional de Seguridad.

Los objetivos en materia de seguridad que BOGAN pretenden garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de BOGAN respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.

- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

Todo el personal de BOGAN, así como personal externo que colabore con BOGAN, tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Política de usos de medios tecnológicos, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

6. MARCO NORMATIVO

Las principales normas que afectan a esta Política son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- 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.
- 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 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.

Para más información, revisar el documento SGSI.PR11.01 Cumplimiento requisitos legales y contractuales.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Comité de Seguridad de la Información

El Comité de Seguridad es el máximo responsable de seguridad de la información y servicios. Este comité tendrá a siguiente composición:

- La persona responsable de los servicios
- La persona responsable de la información
- La persona responsable de la seguridad de la información
- La persona responsable del sistema
- La persona delegada de protección de datos

Con carácter opcional, otros miembros BOGAN podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados ya sean de carácter interno, externo o mixto.

El secretario o la secretaria del Comité de Seguridad será la persona responsable del sistema, que se encargará de convocar las reuniones del Comité y levantar acta de ellas.

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.
- Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la información
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Funciones y responsabilidades

Responsable de la Información

Serán funciones del responsable de la Información:

- Establecer y mantener actualizada la clasificación de la información tratada en los sistemas, atendiendo a su nivel de sensibilidad.
- Definir los requisitos de seguridad necesarios para la información en función de su clasificación y asegurarse de que sean implementados en los sistemas correspondientes.
- Supervisar la seguridad de la información gestionada en el sistema, colaborando con el Responsable del Sistema y el Responsable de Seguridad.
- Garantizar que la gestión de la información se ajusta a las disposiciones legales, reglamentarias y organizativas aplicables.

- Participar en la identificación, gestión y resolución de incidentes de seguridad relacionados con la información.

Responsable del Servicio

Serán funciones del responsable del servicio:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los Servicios.
- Supervisar el desarrollo, mantenimiento y operación del servicio, verificando que se ajusta a los niveles de seguridad acordados.
- Coordinarse con el responsable de Seguridad, el responsable del Sistema y el Responsable de la Información para garantizar una gestión integral de la seguridad en el servicio.
- Participar en la identificación y resolución de incidentes de seguridad que afecten al servicio, y reportar dichos incidentes según los procedimientos establecidos.
- Asegurar que el servicio cumple con las normativas internas y externas aplicables.
- Colaborar en la identificación, análisis y gestión de los riesgos que puedan afectar al servicio, informando de forma oportuna sobre aquellos que puedan tener un impacto significativo.

Responsable de la Seguridad

Serán funciones del Responsable de Seguridad:

- Determinar las medias de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
- Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio
- Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
- Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
- Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.
- Aprobar los procedimientos de seguridad que forman parte del mapa normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Realizar el análisis y evaluación de Riesgos de los activos de BOGAN, junto con los responsables de los mismos.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Hacer seguimiento del cumplimiento de las medidas y normas de seguridad y acuerdos de nivel de servicio por parte de los proveedores de servicios TIC
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

- Análisis de los informes de Auditoria de primera, segunda o tercera parte que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información
- En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.

Responsable de Sistema

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Adopción de las medidas correctoras derivadas de las auditorías de seguridad
- Definir la topología y la gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Elaborar los procedimientos operativos necesarios.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el responsable del Seguridad y/o Comité de Seguridad TIC.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al responsable de Seguridad o a quién éste determine.
- Implantar los planes de continuidad del servicio, asesorado por la persona Responsable de Seguridad.
- En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a BOGAN, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de BOGAN, en materia de protección de datos, 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 supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento. Recabar información para supervisar el registro de las operaciones de tratamiento.
    - Asesorar en el principio de la protección de datos por diseño y por defecto.
    - Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
    - Priorizar actividades en base a los riesgos.
    - Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

Resolución de Conflictos

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias

Procedimientos de designación

- La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por presidencia del Consejo Rector de Bogan.
- Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento.

8. TRATAMIENTO DE DATOS PERSONALES DE LA ENTIDAD

BOGAN trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. BOGAN deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

9. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas).

Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma. El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información y Manual del Sistema Gestión Seguridad de la Información

b) Segundo nivel normativo: constituido la Política de Uso de medios tecnológicos para el correcto uso de los sistemas de información

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Comité de Seguridad la aprobación de la Política de Seguridad de la Información, la Política de Uso de medios tecnológicos y de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

11. OBLIGACIONES DEL PERSONAL

Todas las personas usuarias de los sistemas de la información de BOGAN tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Política de Uso de medios tecnológicos, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a las personas afectadas.

Se establecerá un programa de concienciación continua para atender a todos las personas usuarias de los sistemas de la información, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que a necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto se es su primera asignación o se trata de un cambio de puesto de trabajo o de responsabilidades en este.

El manifiesto incumplimiento de la Política de Seguridad de la Información o de la normativa y los procedimientos derivados de ellas, pueden llevar al inicio de medidas disciplinarias adecuadas y, se es el caso, a otras medidas legales de aplicación.

12. TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando BOGAN preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando BOGAN utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II del Real Decreto 311/2022 y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que BOGAN pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad,

que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD

BOGAN dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.
Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14. MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

15. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

16. HISTÓRICO DE MODIFICACIONES

Versión	Fecha	Revisado por	Aprobado por	Modificación
1	04/09/2026	Resp. Seguridad	Comité Seguridad	Edición inicial