POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PÚBLICA

ÍNDICE

ÍNDICE

Tabla de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN 3
3. ALCANCE 4
3.1. Alcance Subjetivo 4
3.2. Alcance Objetivo 4
4. REQUISITOS MÍNIMOS DE SEGURIDAD 5
5. PRINCIPIOS BÁSICOS 6
6. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN 7
7. MISIÓN 8
8. CUMPLIMIENTO DE ARTÍCULOS 9
9. DESARROLLO DE LA POLÍTICA 9
9.1. Primer nivel normativo: Política de Seguridad TIC. 10
9.2. Segundo nivel normativo: Normas de Seguridad de la Información. 10
9.3. Tercer nivel normativo: Procedimientos de Seguridad TIC. 10
10. ORGANIZACIÓN DE LA SEGURIDAD 11
10.1. Roles o perfiles de seguridad 11
10.2. Comité de Seguridad de la Información 11
10.3. Responsabilidades asociadas al Esquema Nacional de Seguridad 12
10.4. Procedimientos de designación 16
10.5. Matriz RACI: matriz de asignación de responsabilidades 16
11. RESOLUCIÓN DE CONFLICTOS 17
12. DATOS DE CARÁCTER PERSONAL 17
13. TERCERAS PARTES 18
14. MEJORA CONTINUA 19
15. APROBACIÓN DEL DOCUMENTO 19

PÚBLICA

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 12 de agosto de 2025 mediante acta del Presidente de la ASOCIACIÓN BARRÓ (en adelante ASOCIACIÓN BARRÓ).

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde su fecha de aprobación, y se mantendrá vigente hasta que sea sustituida por una nueva Política.

2. INTRODUCCIÓN

ASOCIACIÓN BARRÓ depende en gran medida de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, y es consciente que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan servicios públicos, y que como proveedor del sector público debe gestionar de manera adecuada estos riesgos.

El objetivo de esta gestión de riesgos es proteger los sistemas de Tecnologías de la Información y las Comunicaciones frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada por ASOCIACIÓN BARRÓ en el marco de los servicios prestados al sector público, y de manera más específica a residencias y centros sociosanitarios.

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.

PÚBLICA

Los diferentes departamentos de ASOCIACIÓN BARRÓ deben 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 la contratación de proyectos TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

3. ALCANCE

3.1. Alcance Subjetivo

Los sujetos obligados por esta Política son todo el personal de ASOCIACIÓN BARRÓ, y todas aquellas personas o entidades, tanto internas como externas, que presten servicios a ASOCIACIÓN BARRÓ, tanto en sus propias instalaciones como en remoto.

3.2. Alcance Objetivo

Esta Política se aplicará a los sistemas de información1 de ASOCIACIÓN BARRÓ que dan soporte a las actividades relacionadas con el desarrollo de programas de intervención social.

La identificación y mantenimiento del marco normativo será responsabilidad del Responsable de Seguridad de ASOCIACIÓN BARRÓ y se regulará a través del procedimiento relativo a la identificación y evaluación de requisitos legales. Se incluirán las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital o entidad que asuma esas funciones.

[1] Los sistemas de información han de entenderse en un sentido amplio como, “aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar la información”.

PÚBLICA

Asimismo, el Responsable de Seguridad de ASOCIACIÓN BARRÓ también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

4. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política de Seguridad de ASOCIACIÓN BARRÓ regula la gestión continua del proceso de seguridad. Esta Política se ha establecido de acuerdo con los principios básicos establecidos en el Capítulo II del ENS y el artículo 21 de la Directiva (UE) 2022 /2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a garantizar un nivel común de ciberseguridad en la UE (Directiva NIS 2) se desarrolla teniendo en cuenta la aplicación de los siguientes requisitos mínimos de seguridad:

a) Organización e implantación del proceso de seguridad (art.13 ENS)

b) Análisis y gestión de los riesgos (art.14 ENS y 21 a) Directiva NIS 2).

c) Gestión de personal (art.15 ENS) y prácticas básicas de ciber-higiene y formación en ciberseguridad (21 g) Directiva NIS).

d) Profesionalidad (art.16 ENS y 21 j) Directiva NIS2)

e) Autorización y control de los accesos (art.17 ENS y 21 j) ENS).

f) Protección de las instalaciones (art.18).

g) Adquisición de productos de seguridad y contratación de servicios de seguridad (art.19 ENS y 21 e) Directiva NIS 2).

h) Mínimo privilegio (art.20).

i) Integridad y actualización del sistema (art.21).

PÚBLICA

j) Protección de la información almacenada y en tránsito (art.22).

k) Prevención ante otros sistemas de información interconectados (art.23).

l) Registro de la actividad y detección de código dañino (art.24).

m) Incidentes de seguridad (art.25).

n) Continuidad de la actividad (art.26 y 21 c) Directiva NIS 2).

ñ) Mejora continua del proceso de seguridad (art.27).

Para dar cumplimiento a estos requisitos mínimos ASOCIACIÓN BARRÓ aplicará las medidas de seguridad en el Anexo II del EN teniendo en cuenta:

- Los activos que constituyen el sistema de información de ASOCIACIÓN BARRÓ.
- La categoría de seguridad del sistema, según lo previsto en el artículo 40.
- Las decisiones que se adopten para gestionar los riesgos identificados.

5. PRINCIPIOS BÁSICOS

La Política de Seguridad de la Información de ASOCIACIÓN BARRÓ establece los siguientes principios básicos que han de tenerse presentes en el uso de los sistemas de información:

- **Seguridad como proceso integral:** la seguridad es un proceso que comprende todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información.

- **Gestión integral basada en riesgos**: el análisis y gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y

PÚBLICA

permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos aceptables.

- **Prevención, detección, respuesta y conservación:** La seguridad del sistema de información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta.

- **Existencia de líneas de defensa**: El sistema de información de ASOCIACIÓN BARRÓ debe disponer de una estrategia de protección constituida por múltiples capas de seguridad.

- **Vigilancia continua y reevaluación periódica**: La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente permitirá medir su evolución y las medidas de seguridad se reevaluarán y actualizarán periódicamente adecuando su eficacia a la evolución de los riesgos y sistemas de protección.

6. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

ASOCIACIÓN BARRÓ establece como objetivos de Seguridad los siguientes:

- Garantizar la **protección de la información**.

- **Seguridad física:** ASOCIACIÓN BARRÓ emplaza los sistemas de información en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad.

- **Control de acceso**: ASOCIACIÓN BARRÓ limita el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de mecanismos de identificación, autenticación y autorización adaptados a la criticidad de cada activo.

PÚBLICA

- **Adquisición, desarrollo y mantenimiento de los sistemas de información**: ASOCIACIÓN BARRÓ contempla los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información.

- **Garantizar la prestación continuada de los servicios**: ASOCIACIÓN BARRÓ implanta los procedimientos adecuados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio.

- **Protección de datos**: ASOCIACIÓN BARRÓ adopta las medidas técnicas y organizativas necesarias para gestionar los riesgos derivados del tratamiento de datos personales.

- **Cumplimiento**: ASOCIACIÓN BARRÓ adopta las medidas técnicas y organizativas necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

7. MISIÓN

La misión de ASOCIACIÓN BARRÓ es acompañar, impulsar y compartir procesos socioeducativos que potencien el desarrollo personal y comunitario, para las personas y su entorno, que se encuentren en situación de desigualdad social. A través de una educación integral, participativa y en red, para una igualdad de oportunidades.

ASOCIACIÓN BARRÓ es una entidad con fuerte base social y estabilidad económica; que impulsa la inclusión activa en la sociedad donde las personas están en igualdad de oportunidades, mediante un trabajo socioeducativo y multidisciplinar que apuesta por la interculturalidad, la excelencia y el trabajo en red.

Estos son nuestros valores:

- ✓ Solidaridad activa.
- ✓ Equidad Social y apuesta por los Derechos Humanos y de la Infancia.
- ✓ Implicación.

PÚBLICA

- ✓ Interculturalidad.
- ✓ Participación.
- ✓ Reciprocidad.
- ✓ Educación integral.
- ✓ Espíritu crítico.

8. CUMPLIMIENTO DE ARTÍCULOS

Para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ASOCIACIÓN BARRÓ ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y servicios a proteger teniendo en cuenta la categoría de los sistemas afectados.

El cumplimiento del articulado del ENS se recoge detalladamente en el documento "Declaración de Aplicabilidad".

9. DESARROLLO DE LA POLÍTICA

El Comité de Seguridad de la Información de ASOCIACIÓN BARRÓ ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario, mejoras de la misma, para su aprobación por parte del Presidente de ASOCIACIÓN BARRÓ.

PÚBLICA

La presente Política de Seguridad es de obligado cumplimiento y se estructura a nivel documental, en los siguientes niveles jerárquicos:

- **Primer nivel:** Política de Seguridad de la Información.
- **Segundo nivel:** Normativas de Seguridad.
- **Tercer nivel:** Procedimientos de Seguridad.

El Responsable de Seguridad de la Información (CISO) deberá revisar al menos con periodicidad anual esta normativa, proponiendo mejoras a la misma en el caso que sea necesario.
El personal de ASOCIACIÓN BARRÓ y terceras empresas, deberán conocer además de esta Política de Seguridad, todas las normativas, procedimientos, instrucciones técnicas, u otra documentación que pueda afectar en el desempeño de sus funciones.

9.1. Primer nivel normativo: Política de Seguridad TIC.

La Política de Seguridad TIC constituye el instrumento normativo al más alto nivel en la estructura normativa de la seguridad de ASOCIACIÓN BARRÓ. Deberá ser aprobada por el Presidente de ASOCIACIÓN BARRÓ.

9.2. Segundo nivel normativo: Normas de Seguridad de la Información.

Las Normas de Seguridad TIC son instrumentos de nivel medio que abarcan un área determinada de la seguridad. El órgano responsable de su aprobación es el Comité de Seguridad de ASOCIACIÓN BARRÓ.

9.3. Tercer nivel normativo: Procedimientos de Seguridad TIC.

Los Procedimientos de Seguridad TIC son instrumentos de nivel inferior, redactados con un mayor nivel de detalle, aplicables a un ámbito específico. El Responsable de su aprobación es el Responsable de Seguridad.

PÚBLICA

10. ORGANIZACIÓN DE LA SEGURIDAD

10.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- **Responsable de Información:** Juan Daniel Molano Villar
- **Responsable de los Servicios:** Juan Daniel Molano Villar
- **Responsable de Seguridad:** Raquel Baena Fernández
- **Responsable del Sistema:** Malena Chamorro de la Cruz

10.2. Comité de Seguridad de la Información

ASOCIACIÓN BARRÓ ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

- Presidente: Presidente de ASOCIACIÓN BARRÓ.
- Miembros:
  - ✓ Responsable del Servicio
  - ✓ Responsable del Sistema.
  - ✓ Responsable de Seguridad

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

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias de ASOCIACIÓN BARRÓ o de forma remota con periodicidad semestral previa convocatoria al efecto realizada por el Director General de dicho Comité. En todo caso, el Comité podrá celebrar reuniones extraordinarias cuando existan circunstancias que lo requieran.

PÚBLICA

10.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo II del ENS previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad (CISO/ RSF)

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Gestionar, supervisar y mantener la seguridad física de las instalaciones de ASOCIACIÓN BARRÓ.
- Promover la formación y concienciación en materia de seguridad.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- 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.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.

PÚBLICA

- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Implantar y gestionar los Sistemas de Información de ASOCIACIÓN BARRÓ durante todo su ciclo de vida, incluyendo la implantación de los controles de ciberseguridad, así como su operación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Colaborar con el Responsable de Seguridad para la investigación y resolución de ciberincidentes que afecten a los Sistemas de Información de ASOCIACIÓN BARRÓ y aplicar el conocimiento obtenido del análisis de los ciberincidentes que hayan tenido lugar para reducir la probabilidad o el impacto de incidentes en el futuro.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
  - ✓ La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
  - ✓ La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
  - ✓ Aprobar los cambios en la configuración vigente del Sistema de Información.

PÚBLICA

- ✓ Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- ✓ Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- ✓ Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- ✓ Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- ✓ Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

PÚBLICA

- ✓ Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- ✓ Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

- ✓ Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- ✓ Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.

- ✓ Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

- ✓ Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.

- ✓ Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.

- ✓ Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

- ✓ Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.

PÚBLICA

- ✓ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

- ✓ Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

10.4. 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 ha sido realizada por el Presidente de ASOCIACIÓN BARRÓ y comunicada a las partes interesadas.

Los miembros del Comité, así como los roles de seguridad serán revisados cada tres años o con ocasión de vacante.

10.5. Matriz RACI: matriz de asignación de responsabilidades

Tarea	DG	RI	RS	CISO/RSF	CIO
Política de Seguridad	A	C	C	R	C
Determinación de la categoría del Sistema	C	C		A/R	C
Análisis de Riesgos		I	R	A/R	R
Declaración de aplicabilidad		I	R	A/R	R
Normas y procedimientos de S.I		I		A/R	R
Respuesta incidentes de seguridad	I	I	C	A/R	R
Seguridad del ciclo de vida de los servicios y sistemas de información				C	A/R
A: Accountable (toma la decisión, autoriza y aprueba. **R: Responsible (es responsable de la realización del trabajo**		**C: Consulted (se le consulta antes de tomar la decisión).** **I: Informed (se le informa de las decisiones tomadas)**			

PÚBLICA

11. RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad de la Información de ASOCIACIÓN BARRÓ se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

12. DATOS DE CARÁCTER PERSONAL

ASOCIACIÓN BARRÓ solo tratará datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso conforme a la Política de Protección de Datos Personales aprobada por la Presidencia de ASOCIACIÓN BARRÓ.

De conformidad con el 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) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

PÚBLICA

13. TERCERAS PARTES

Cuando preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. ASOCIACIÓN BARRÓ definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que ASOCIACIÓN BARRÓ lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando ASOCIACIÓN BARRÓ utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad establecidas en la disposición adicional segunda del Real Decreto 311/2022, y en consideración 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, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se

PÚBLICA

requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

14. MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a actualización permanente. Por ello, es necesario que ASOCIACIÓN BARRÓ implante un proceso de mejora continua que comportará entre otras acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas y externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de normas y procedimientos.

Para ASOCIACIÓN BARRÓ, la gestión adecuada de la seguridad de la información constituye un reto continuo y colectivo, necesario para la continuidad de la Entidad.

15. APROBACIÓN DEL DOCUMENTO

Declaro aprobada la Política de Seguridad de la Información de ASOCIACIÓN BARRÓ que se recoge en este documento, debiendo ser comunicada para el conocimiento general de todos los empleados de la entidad, lo que facilitará su cumplimiento y seguimiento.

12 de agosto de 2025 Presidente de ASOCIACIÓN BARRÓ

PÚBLICA