



**Expediente n.º:** 1289/2025

**Procedimiento:** Administración Electrónica

## **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

Vista las necesidades de adecuación de nuestra entidad al Esquema Nacional de Seguridad (ENS) el Ayuntamiento de Breña Baja aprueba mediante acuerdo plenario la Política de Seguridad de la Información (PSI), de conformidad de conformidad con lo dispuesto en el artículo 4 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, que atribuye a los municipios la potestad de autoorganización, entre otras, y teniendo en cuenta lo establecido en el Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica..

### **DISPONGO**

**PRIMERO.-** Aprobar la Política de Seguridad de la Información, en adelante PSI, que sigue :

#### **1 INTRODUCCIÓN**

La Política de Seguridad de la Información del Ayuntamiento de Breña Baja, en adelante la Política de Seguridad de la Información, establece el compromiso de este Ayuntamiento respecto a la seguridad de los servicios que ofrece a la ciudadanía a través de medios electrónicos y la información que gestiona en el ámbito de sus competencias, en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Canarias. Esta Política de Seguridad asegura un compromiso manifiesto de las máximas Autoridades del Ayuntamiento de Breña Baja para la difusión, consolidación y cumplimiento de la presente Política.

##### **1.1 Objetivos.**

Se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión, objetivos y estrategias establecidas por el Ayuntamiento de Breña Baja.
2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la prestación de servicios a través de medios electrónicos y a la protección de datos de carácter personal.
3. Proteger los activos de información y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales, garantizando la autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, acceso y conservación de la información mediante la prevención de riesgos, la supervisión de la actividad diaria y una respuesta adecuada y diligente ante cualquier incidente.

La Política de Seguridad de la Información es el instrumento en que se apoya el Ayuntamiento para alcanzar estos objetivos, de forma que trabajadores públicos y ciudadanos puedan acceder a los



servicios en un entorno de gestión confiable y seguro.

Para ello, el Ayuntamiento de Breña Baja ha establecido un marco de gestión de la seguridad de la información conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) y según lo establecido en la Legislación aplicable en materia de protección de datos de carácter personal vigente en la Unión Europea, en España y en la Comunidad Autónoma (en adelante, RGPD y/o LOPD), reconociendo como activos estratégicos la información que gestiona y los sistemas que la soportan y asumiendo el compromiso de cumplir los principios básicos y requisitos mínimos articulados en el ENS.

## 1.2 Principios básicos.

El Ayuntamiento de Breña Baja ha desarrollado esta Política de Seguridad de la Información partiendo de la premisa de que la seguridad de la información es un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información (art. 6.1 del ENS), siendo el análisis y gestión de los riesgos parte esencial del proceso de seguridad, por lo que debe constituirse en una actividad continua y permanentemente actualizada (art. 7.1 del ENS).

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta (art. 8.1 del ENS).

**Prevención.** El Ayuntamiento de Breña Baja debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, sus órganos directivos implementan las medidas mínimas de seguridad determinadas por el ENS, RGPD y/o LOPD así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles deben estar claramente definidos y documentados.

**Detección.** Dado que los sistemas y servicios pueden deteriorarse rápidamente debido a incidentes, que pueden ir desde una degradación hasta su detención, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

**Respuesta.** Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad (art. 8.4 del ENS).

**Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico (art. 8.5 del ENS).**

**Conservación.** Para garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

El Ayuntamiento de Breña Baja ha trazado una estrategia de protección fundamentada en múltiples líneas de defensa (art. 9.1 del ENS) integradas por medidas de naturaleza organizativa, física y lógica



(art. 9.2 del ENS).

El proceso de seguridad requiere una vigilancia continua y reevaluación periódica (art. 10 del ENS), por lo que debe ser controlado, gestionado y supervisado, promoviendo una cultura de la ciberseguridad en el Ayuntamiento.

Por último, la presente Política de seguridad establece una diferenciación de responsabilidades, definiendo los roles de responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema (art. 11.1 del ENS). Además, se delimitan las responsabilidades relacionadas con la seguridad para diferenciarlas de aquellas asociadas a la explotación de los sistemas (art 11.2 del ENS), detallando las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos (art. 11.3 del ENS).

### 1.3 Requisitos mínimos.

Con objeto de asegurar que los servicios que el Ayuntamiento ofrece a la ciudadanía cumplan los estándares establecidos en materia de seguridad, el Ayuntamiento de Breña Baja ha desarrollado esta Política de Seguridad de la Información implementando los requisitos mínimos de seguridad exigidos por el ENS en los siguientes aspectos:

- A. Organización e implantación del proceso de seguridad.
- B. Análisis y gestión de los riesgos.
- C. Gestión de personal.
- D. Profesionalidad.
- E. Autorización y control de los accesos.
- F. Protección de las instalaciones.
- G. Adquisición de productos de seguridad y contratación de servicios de seguridad.
- H. Mínimo privilegio.
- I. Integridad y actualización del sistema.
- J. Protección de la información almacenada y en tránsito.
- K. Prevención ante otros sistemas de información interconectados.
- L. Registro de la actividad y detección de código dañino.
- M. Incidentes de seguridad.
- N. Continuidad de las actividades.
- O. Mejora continua del proceso de seguridad.

## 2 ALCANCE

Esta Política de Seguridad de la Información es aplicable a todos los Departamentos Municipales del Ayuntamiento de Breña Baja, incluidas sus Direcciones Generales, Organismos Autónomos, Sociedades Municipales con mayoría de capital social municipal y demás entes que decida el pleno



municipal.

Asimismo, esta Política aplica a todos los sistemas de la información e infraestructuras de comunicación utilizadas para la realización de las funciones propias de las distintas entidades, a sus recursos y a los procesos afectados por el Real Decreto 311/2022 y la legislación aplicable de protección de datos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

La presente Política estará disponible para consulta de todos ellos a través de la Sede Electrónica del Ayuntamiento de Breña Baja.

### **3 MISIÓN**

El Ayuntamiento de Breña Baja, en el marco de sus funciones y competencias, promueve actividades y ofrece servicios públicos destinados a satisfacer las necesidades y expectativas de la ciudadanía y los diversos grupos de interés. Entre los principales objetivos que se persiguen destacan:

- Mejorar la calidad de los servicios públicos
  - Fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, generando la confianza necesaria.
- Reducir los tiempos de tramitación.
- Reducir las cargas administrativas.
- Hacer transparente la actividad de los Ayuntamientos.
- Fomentar la participación y colaboración.

La prestación de servicios debe cumplir altos estándares de calidad, garantizando en todo momento la seguridad de la información a lo largo de todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción).

### **4 MARCO NORMATIVO**

El marco normativo de las actividades del Ayuntamiento de Breña Baja en el ámbito de esta Política de Seguridad de la Información está integrado por las siguientes normas:

- El Esquema Nacional de Seguridad (ENS), regulado inicialmente por el Real Decreto 3/2010, de 8 de enero y posteriormente actualizado por Real Decreto 311/2022, de 3 de mayo, que determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.
- El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 de enero, que establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.



- Las Leyes 39/2015 y 40/2015, que regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

- La Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen de aplicación a la administración local (LRBRL).

- La Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos y garantía de los derechos digitales, que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, además de garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

- Reglamento (UE) 679/2016, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos, que establece la obligación de disponer medidas técnicas y organizativas para garantizar la confidencialidad, disponibilidad e integridad de la información. Asimismo, dispone que dichas medidas han de ser proactivas y el responsable del tratamiento ha de ser capaz de demostrar que se siguen y aplican esas medidas.

- La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022 (Directiva NIS2), relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, que amplía significativamente el alcance de la regulación anterior y establece nuevos requisitos de ciberseguridad aplicables a las administraciones públicas de nivel regional y local. Esta Directiva, pendiente de transposición al ordenamiento jurídico español, reforzará el marco normativo actual en materia de seguridad de redes y sistemas de información.

- Normas aplicables a la Administración Electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información.

## **5 ORGANIZACIÓN DE LA SEGURIDAD (Comités, Roles, Procedimientos de designación y Política de Seguridad de la Información)**

El Marco de Gobernanza municipal de la Seguridad de la Información sigue el modelo definido en la Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad: Responsabilidades y funciones. A continuación se describe la estructura organizativa de la Política de Seguridad de la Información en el Ayuntamiento de Breña Baja.

### **5.1. Pleno.**

El pleno del Ayuntamiento de Breña Baja asegura el compromiso de este Ayuntamiento en la aplicación del ENS, de la LOPD, del RGPD y/o legislación en materia de protección de datos vigente en la UE, España y en la Comunidad Autónoma.

Este compromiso se manifiesta mediante la aprobación de la presente Política de Seguridad de la



Información, así como de todas aquellas modificaciones o actualizaciones de la misma que el Comité de Seguridad de la Información pueda proponer, en el ámbito de sus competencias.

## 5.2. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información estará compuesto por:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de Seguridad
- Delegado de Protección de Datos
- Responsable del Sistema
- Administrador de la Seguridad del Sistema
- Vocales (Según necesidad)

La composición y responsabilidades del Comité se establecerán por acuerdo del pleno, a quién reportará a fin de informar regularmente del estado de la seguridad de la información. Sus funciones serán:

- Coordinar todas las funciones de seguridad de la Organización.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación unificada y consistente en el caso de que deban ser activados.
- Elaborar la Política de Seguridad, que será aprobada por el Alcalde.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. El responsable de seguridad se encargará de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Atender a las inquietudes del Alcalde y transmitírselas al Responsable de Seguridad. De este último, recabar respuestas y soluciones que, una vez coordinadas, son notificadas al Alcalde.
- Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes, se consolidan y resumen para el Alcalde.
- Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad.
- Definir, dentro de la Política de Seguridad, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.

El Comité de Seguridad de la Información elegirá de entre sus miembros un director que será el encargado de coordinar su funcionamiento.

## 5.3 Responsable de la Información

Será designado por el pleno del Ayuntamiento de Breña Baja. Sus funciones y responsabilidades son:



- Velar por el buen uso de la información y, por tanto, de su protección.
  - Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información tratada en materia de seguridad.
- Determinar los niveles de seguridad de la información.

#### 5.4 Responsable de los Servicios

Será designado por el pleno del Ayuntamiento de Breña Baja. Sus funciones y responsabilidades son:

- Establecer los requisitos del servicio prestado en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
  - Determinar los niveles de seguridad de los servicios y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 40 del ENS.

#### 5.5. Responsable de Seguridad.

Será designado por el pleno del Ayuntamiento de Breña Baja, siendo el encargado de establecer las medidas necesarias para cumplir los requisitos de seguridad establecidos por el responsable de la información y de los servicios manejados por el sistema.

Teniendo en cuenta la complejidad organizativa y funcional de los medios electrónicos utilizados por el Ayuntamiento de Breña Baja, en ejercicio de la potestad de autoorganización de la Administración municipal, el Responsable de Seguridad podrá asignar diversos cometidos a unidades orgánicas o empleados públicos, o especializar funciones por razones técnicas u organizativas. Esta asignación no supondrá en ningún caso una delegación de las competencias que le corresponden.

Sus responsabilidades y, en su caso, de las unidades o empleados especializados, son las siguientes:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Analizar y elevar al Comité de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.
- Determinar la categoría de seguridad del sistema de información, valorando el impacto que tendría un incidente que afectase a la seguridad de la información, conforme con lo establecido en el artículo 40 del ENS.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, formalizándolas en el documento Declaración de Aplicabilidad.
- Realizar el seguimiento y control del estado de seguridad de los sistemas de información verificando, a través del seguimiento y control de los riesgos, que las medidas de seguridad son adecuadas para garantizar que se satisfacen los requisitos de seguridad.
  - Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.
  - Realizar los preceptivos análisis de riesgos.
  - Valorar los riesgos residuales respecto de la información calculada en el análisis de riesgos.
  - Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta



su resolución.

- Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.
- Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
- Analizar los informes de auditoría y presentar sus conclusiones al responsable del sistema.

## 5.6. Delegado de Protección de Datos

Será designado por el Ayuntamiento de Breña Baja. Sus responsabilidades, funciones y tareas son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o del Estado.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o del Estado y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
  - Identificación de las bases jurídicas de los tratamientos.
  - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
  - Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico distintas de las establecidas por la normativa general de protección de datos.
  - Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
    - Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
    - Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
    - Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
  - Diseño e implantación de políticas de protección de datos.
  - Auditoría de protección de datos.
  - Establecimiento y gestión de los registros de actividades de tratamiento.
  - Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
  - Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
  - Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de



notificación a las autoridades de supervisión y a los afectados.

- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
  - Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

#### 5.7. Responsable del Sistema.

Será nombrado por el pleno del Ayuntamiento de Breña Baja. Sus responsabilidades son las siguientes:

- Mantener los niveles de seguridad del servicio electrónico actualizados.
- Desarrollar la forma concreta de implementar la seguridad en el sistema y la supervisión de la operación diaria del mismo (Procedimientos Operativos).
- Seleccionar las salvaguardas y medidas correctoras que se deban implantar.
- Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
- Suspender, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.
  - Dar publicidad, en los correspondientes portales de internet o sedes electrónicas, a las declaraciones y certificaciones de conformidad con el ENS.

El Responsable del Sistema remitirá al Responsable de Seguridad el resultado de las tareas realizadas en el ámbito de estas responsabilidades, al menos una vez al año o a petición del mismo, reportando el resultado en formato adecuado para una integración de la información.

#### 5.8 Administrador de la Seguridad del Sistema.

Será nombrado por el pleno del Ayuntamiento de Breña Baja. Sus responsabilidades son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización para asegurar que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aplicar cambios en la configuración vigente del Sistema de Información.



- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
  - Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
  - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

## 5.9 Resolución de conflictos.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información del Ayuntamiento de Breña Baja, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad, elevándose para su resolución al Comité de Seguridad de la Información en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

## 6 DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Breña Baja trata datos de carácter personal. La clasificación de la información de carácter personal viene establecida en el Reglamento General de Protección de Datos (RGPD), complementado por la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así como las medidas de seguridad adoptadas derivadas de la evaluación de impacto y análisis de riesgo realizado sobre los tratamientos.

Todos los sistemas de información del Ayuntamiento de Breña Baja se ajustan a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades de Tratamiento.

Para garantizar dicha protección, se han adoptado las medidas de seguridad aplicables a los datos de carácter personal previstas en el ENS.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con el ayuntamiento.

## 7 GESTIÓN DE RIESGOS



El Análisis de Riesgos, evaluando las amenazas y los riesgos a los que están expuestos la información, los servicios y sistemas del Ayuntamiento de Breña Baja, se realizará:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo IV del Real Decreto 311/2022, de 3 de mayo, y del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y/o Legislación aplicable en materia de protección de datos de carácter personal vigente.
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal la información recopilada de fuentes de reconocido prestigio como el CCN-CERT.

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 de la Información, asimismo, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia, mediante rangos, para los diferentes tipos de información manejados y los diferentes servicios prestados.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El Comité de Seguridad de la Información trasladará al pleno municipal de las necesidades de inversión en materia de seguridad detectadas mediante dichos análisis.

## **8 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

### **8.1 Autorización y control de accesos**

El acceso a los sistemas de información del Ayuntamiento de Breña Baja será de uso público o estará restringido a personal formalmente autorizado. En este segundo supuesto, se deberá limitar el acceso mediante técnicas que aseguren la inequívoca identificación de los usuarios a través de su autenticación (identificación a través de una posesión o de un conocimiento exclusivo) y autorización (comprobación de los permisos de acceso a la información o al servicio). Ello con independencia de la red o el dispositivo desde el que se acceda.



Las aplicaciones deberán contar con roles y permisos de acceso que implementen el principio de privilegio mínimo, facilitando el acceso de los usuarios a la información y funcionalidades necesarias pero limitando aquellas innecesarias para el desempeño de sus funciones.

## 8.2 Registro de actividad y detección de código dañino

Se registrarán las actividades 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. Por ello, el acceso a toda la información y a los servicios (incluido el acceso a Internet o cualquier otra comunicación por parte de los usuarios) será monitorizado y restringido en función de las necesidades del puesto de trabajo. Esta capacidad de monitorización del uso seguro resulta indispensable para 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 redes y sistemas de información del ayuntamiento.

## 8.3 Protección física de las instalaciones

El Ayuntamiento de Breña Baja implantará las medidas necesarias que impidan el acceso de personal no autorizado a sus instalaciones con el fin de evitar situaciones de sustracción o modificación de los sistemas de información del ayuntamiento y sus datos.

Se controlará el acceso de personas ajenas al ayuntamiento, que serán identificadas y deberán contar con una autorización formal.

Los sistemas de procesado se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Se deberán registrar las visitas de terceros que serán acompañados por personal autorizado del Ayuntamiento de Breña Baja.

## 8.4 Mínimo privilegio, seguridad por defecto y mínima funcionalidad

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

Para ello, los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, es decir:

- a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
- b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.
- c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

Asimismo, se aplicará la regla de la mínima funcionalidad, es decir:

- a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.
- b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.



Además, se asegurará que las funciones de operación, administración y registro de actividad sólo son accesibles por las personas desde emplazamientos o equipos autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

#### 8.5 Instalación y mantenimiento de los sistemas de información

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

La adquisición y puesta en producción de un nuevo sistema de información deberá venir precedida de su autorización formal, siguiendo la normativa de gestión del cambio del Ayuntamiento de Breña Baja.

Durante la vida útil de los sistemas de información del ayuntamiento, éstos serán mantenidos de manera que se asegure que cumplen con los niveles de operatividad con los que fueron planeados. Además, se seguirán las recomendaciones de fabricantes en cuanto a la actualización de elementos de seguridad.

#### 8.6 Seguridad de las comunicaciones

Se permitirán las comunicaciones necesarias para las funciones propias del Ayuntamiento de Breña Baja y sólo éstas, basándose siempre en el principio de la seguridad por defecto. Por ello, la red de comunicaciones del Ayuntamiento de Breña Baja contará con las medidas de seguridad técnicas necesarias para impedir accesos no permitidos a sus sistemas de información.

Se prestará especial protección (incluidas técnicas de cifrado) a aquellas conexiones entre sistemas del Ayuntamiento de Breña Baja y otras entidades, realizadas a través de redes de públicas.

#### 8.7 Copias de seguridad y continuidad de las actividades

Los sistemas de información del ayuntamiento dispondrán de copias de seguridad para garantizar sus necesidades de disponibilidad, en caso de fallos en los sistemas principales.

Habrán procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro, preferiblemente fuera de las instalaciones de la organización.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Se establecerán los planes que garanticen la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

#### 8.8 Seguridad en información almacenada en sistemas portátiles, soportes extraíbles y sistemas externos



Como parte de los planes de continuidad se pueden definir réplicas en otras sedes y en soportes extraíbles. Estas copias se deben limitar a las necesidades de recuperación y los riesgos definidos en cada sistema. La custodia de estas réplicas y soportes para el almacenamiento y transporte de información deberá garantizar las mismas condiciones que el sistema original o de producción. Igualmente la información podrá replicarse o contenerse en sistemas portátiles si se garantizan los mismos principios que sobre sistemas fijos.

#### 8.9 Gestión de incidentes de seguridad

El Ayuntamiento de Breña Baja establecerá un mecanismo para la actuación en caso de incidentes de seguridad. Se ejecutarán los planes de formación y concienciación para su detección y comunicación.

Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

El Ayuntamiento de Breña Baja establecerá un sistema de detección y reacción frente a código dañino, basado en el uso obligatorio de una herramienta de antivirus.

#### 8.10 Formación y concienciación

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Ayuntamiento de Breña Baja, así como a la difusión entre los mismos de la Política de Seguridad de la Información y de su desarrollo normativo.

A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ayuntamiento de Breña Baja.

### 9 OBLIGACIONES DEL PERSONAL

Todos los miembros de la organización municipal y las empresas y personas terceras que realicen servicios de cualquier clase contratados por el Ayuntamiento de Breña Baja o que de alguna manera se presten bajo el control y/o la dirección del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, que será trasladada a través de los Departamentos Municipales quienes deberán disponer los medios necesarios para que ésta llegue a los afectados.

Se establecerá un programa de concienciación continua dirigido a todos los miembros del Ayuntamiento de Breña Baja, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

### 10 TERCERAS PARTES

Cuando el Ayuntamiento de Breña Baja utilice servicios o maneje información de terceros, les hará



partícipes de esta Política de Seguridad de la Información. El Comité de Seguridad de la Información establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Breña Baja preste servicios a otros organismos o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información. Dicha 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 exigirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando el Ayuntamiento de Breña Baja preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para el reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Breña Baja utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañan a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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 de seguir adelante.

## **11 REVISIÓN**

El Comité de Seguridad de la Información revisará anualmente la Política de Seguridad de la Información o cuando exista un cambio significativo que obligue a ello. La propuesta de revisión, en su caso, será aprobada por el pleno del Ayuntamiento de Breña Baja y difundida para que la conozcan todas las partes afectadas.

**DOCUMENTO FIRMADO ELECTRÓNICAMENTE**