V. 1 | 15/05/2025

Bergarako Udala

Política de Seguridad de la Información

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día […] de […] del año […] por [*órgano que la aprueba*].

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

CONTROL DE VERSIONES

Versión	Fecha de entrada en vigor	Fecha de revisión	Motivo del cambio	Aprobación
1.1	…./…./…….		Edición inicial	[firma digital del presidente y del secretario del Comité de Seguridad]

Índice

1. Introducción

1.1 Justificación de la Política de Seguridad de la Información

La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa 'seguridad de la información' en nuestra organización, el Ayuntamiento de Bergara (en adelante, el "Ayuntamiento").

El documento ha de ser accesible por todos los miembros de la organización y está redactado de forma sencilla, precisa y comprensible.

La presente Política de Seguridad de la Información se elabora en cumplimiento de las exigencias del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad* (en adelante, el "ENS"), el cual en su *artículo 12* establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad, indicando los requisitos mínimos que debe incluir la misma.

Siendo esto así, el ENS se refiere en varios puntos a la Política de Seguridad:

En su artículo 12 se fijan los requisitos mínimos de seguridad, a saber:

> *"2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente."*

Además, en su artículo 13 se estipula que:

> *"1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.*
>
> *2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:*
>
> *a) El responsable de la información determinará los requisitos de la información tratada*
>
> *b) El responsable del servicio determinará los requisitos de los servicios prestados.*
>
> *c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.*
>
> *d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad."*

La finalidad del ENS es generar la confianza necesaria en el uso de medios electrónicos por parte de las Administraciones Públicas, a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo tanto a las citadas Administraciones Públicas, como a la ciudadanía, el ejercicio de derechos y el cumplimiento de deberes a trasvés de estos medios.

A tal efecto, la adaptación al ENS implica que el Ayuntamiento y su personal deben aplicar las medidas de seguridad exigidas en la normativa, así como realizar un seguimiento continuo de los niveles de prestaciones

de servicios, realizar el seguimiento y análisis de vulnerabilidades y preparar respuestas efectivas ante los incidentes, garantizando la continuidad de los servicios prestados.

Por todo ello, todas las áreas y departamentos del Ayuntamiento, deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa en el 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.

De igual manera, los departamentos del Ayuntamiento deben estar preparados para prevenir, detectar, responder ante incidentes y garantizar la conservación de los datos, todo ello de acuerdo al artículo 8 del ENS.

1.2 Misión y servicios prestados

El Ayuntamiento depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para la prestación de gran parte de sus servicios, es por ello que, la información tratada, constituye un activo de primer orden para la propia organización. En el mismo sentido, las citadas tecnologías de la información y comunicaciones se han hecho imprescindibles en el desempeño diario del Ayuntamiento.

Por otro lado, las indiscutibles mejoras que aportan las TIC al tratamiento de la información, vienen acompañadas de nuevos riesgos y, por lo tanto, es necesario administrar los citados sistemas con la debida diligencia, tomando las medidas adecuadas para proteger los mismos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada.

La seguridad de la información tiene como objetivo proteger la información y los servicios, garantizando la calidad de la propia información y la prestación ininterrumpida de los servicios, actuando de manera preventiva, supervisando la actividad diarios y reaccionando con presteza ante los incidentes.

El Ayuntamiento para la gestión de sus intereses y, en el ámbito de sus competencias y como Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los habitantes del municipio.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa el Ayuntamiento a través de medios electrónicos, en concreto:

- Las relaciones de carácter jurídico-económico entre la ciudadanía y el Ayuntamiento.
- La consulta por parte de la ciudadanía de la información pública administrativa y de los datos administrativos que estén en poder del Ayuntamiento.
- La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica del Ayuntamiento.
- El tratamiento de la información obtenida por el Ayuntamiento en el ejercicio de sus potestades.

2. Marco normativo y alcance

2.1 Marco normativo

En el desarrollo e implementación de la presente política de seguridad, se tendrán en cuenta las normas que regulan la actividad del Ayuntamiento en el ámbito de sus competencias, además de aquella dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, la información y los servicios.

Concretamente, el marco normativo aplicable está integrado por las siguientes normas:

- El *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* , el cual fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

- El *Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica*, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

- 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 (en adelante, el “RGPD”).

- La *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitale*s (en adelante, la “LOPDGDD”).

- La *Ley 39/2015, de 1 de octubre,* del Procedimiento Administrativo Común de las Administraciones Públicas.

- La *Ley 40/2015, de 1 de octubre,* de Régimen Jurídico del Sector Público.

- *Real Decreto 203/2021, de 30 de marzo*, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

- La *Ley 7/1985, de 2 de abril,* Reguladora de las Bases del Régimen Local*, modificada por la ley 11/1999*, de 21 de abril.

- La *Ley 57/2003, de 16 de diciembre,* de medidas para la modernización del gobierno local.

- El *Real Decreto Legislativo 1/1996, de 12 de abril*, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. .

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- La *Ley 19/2013, de 9 de diciembre,* de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- *Ley 34/2002, de 11 de julio,* de servicios de la sociedad de la información y de comercio electrónico.

- *Ley 37/2007, de 16 de noviembre,* sobre reutilización de la información del sector público.

- *Ley 25/2007, de 18 de octubre,* de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- *Ley 56/2007, de 28 de diciembre*, de Medidas de Impulso de la Sociedad de la Información.

- *Ley 9/2014, de 9 de mayo,* General de Telecomunicaciones.

- *Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público,* por la que se transponen al ordenamiento jurídico español las *Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.* .

- *Real Decreto-ley 14/2019, de 31 de octubre*, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

- El *Real Decreto 1553/2005, de 23 de diciembre*, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

- *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.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento.

Será responsabilidad del Ayuntamiento mantener actualizado un Anexo con la normativa actualizada incluidas las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas.

Así mismo, el Ayuntamiento, también será responsable de identificar las guías de seguridad del Centro Criptológico Nacional (CCN-CERT), que sean de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

2.2 Alcance

La presente Política de Seguridad es de aplicación a todos los sistemas TIC del Ayuntamiento, a todo el personal del mismo, sin que medie ninguna excepción, a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos y/o acuerdos.

3. Organización de la seguridad

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada una de las personas usuarias de los sistemas de información del Ayuntamiento son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones, tal como indica el artículo 13 del ENS.

Para una mejor respuesta a incidentes de seguridad, el Ayuntamiento mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

3.1 Estructura de Seguridad

Podemos distinguir tres (3) niveles en el organigrama del Ayuntamiento, los cuales ostentarán diferentes bloques de responsabilidad:

Nivel – Gobierno

Entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que se alcancen.

Sobre este nivel, recae la responsabilidad legal, así como la responsabilidad de especificar las necesidades.

Nivel – Supervisión

Servicios que entienden qué hace cada unidad de gestión y cómo las diferentes unidades se coordinan entre sí para alcanzar los objetivos marcados.

Nivel – Operacional

Se centra en una actividad concreta y controla cómo se hacen las cosas.

3.2 Definición de roles

En la misma línea, según detalla el *Anexo II del ENS, en su sección 3.1*, la Política de Seguridad **debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todo el personal de la organización administrativa**.

En este sentido, se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información por cada nivel:

Nivel de Gobierno:

3.2.1 Responsable de la Información y de Servicios

El Responsable de la Información y de Servicios será el\la Alcalde\Alcaldesa del Ayuntamiento.

El Responsable de la Información y de Servicios establecerá los requisitos sobre la información proporcionada a través de los servicios del Ayuntamiento y, por tanto, tendrá la última palabra a la hora de decidir el tipo de información accesible y el uso que se le pueda dar, en virtud de la reglamentación vigente y de las buenas prácticas en materia de Protección de Datos.

Le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los tratamientos de datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Aceptar los niveles de riesgo residual que afecten a la información.

- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información y de Servicios, se realizará a propuesta de la Comisión de Seguridad de la Información.

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

- Determinar el funcionamiento del Comité de Seguridad de la Información y asignar los roles previstos por el SEN.

- Aprobación del plan de mejora.

Nivel Supervisión:

3.2.2 Responsable de Seguridad

El\la Responsable de Digitalización y Organización del Ayuntamiento, tendrá el rol de Responsable de Seguridad del Ayuntamiento, teniendo por funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.
- Realizar las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de la Seguridad de la Información dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de monitorización y auditoría de los estados de seguridad de los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el Comité de Seguridad incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por los Responsables de los Sistemas cuando en virtud del contenido no requiera la aprobación del Comité de Seguridad.
- Proponer la redacción de aquella normativa de seguridad del Ayuntamiento que considere necesario formalizar.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema
- 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.
- 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.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo a la puesta en marcha de un nuevo servicio vinculado al ENS.

Nivel Operacional

3.2.3 Responsable de Sistemas

El\la técnico\a de Informática tendrá el rol de Responsable de Sistemas del Ayuntamiento, teniendo por funciones las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Verificar la aplicación de los procedimientos operativos de seguridad en los sistemas de información.
- 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
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para que la seguridad no esté comprometida y que en todo momento se ajusten a los procedimientos establecidos.
- Supervisar el estado de la seguridad de los sistemas.
- Informar al Responsable de Seguridad sobre 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.
- Asesorar al Responsables de Seguridad para cumplir los requisitos de seguridad establecidos.

3.2 Comité de Seguridad de la Información

El Comité de la Seguridad de la Información (en adelante, el “Comité de Seguridad”), coordina la seguridad de la información a nivel de organización.

Podrán convocarse reuniones extraordinarias cada vez que las necesidades o las circunstancias así lo exijan.

El **Comité de Seguridad** tendrá las siguientes funciones:

- **Atender las inquietudes, en materia de Seguridad de la Información**, del Ayuntamiento y de las diferentes áreas, unidades y servicios informando regularmente del estado de la Seguridad de la Información a la Alcaldía.

- **Asesorar en materia de Seguridad de la Información**, siempre y cuando le sea requerido y tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

    - Grupos de trabajo especializados internos, externos o mixtos.
    - Asesoría interna y/o externa

- **Resolver los conflictos de responsabilidad que puedan aparecer entre los/as diferentes responsables** y/o entre diferentes Áreas/Unidades/Servicios del Ayuntamiento, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- **Recoger las funciones y obligaciones de los/as Responsables de la Información y los Servicios ENS, en aquellas acciones transversales**, en las que le sea solicitado y/o se considere necesario.

- **Promover la mejora continua del sistema de gestión de la Seguridad de la Información**. Para ello se encargará de:

    - Coordinar los esfuerzos de las diferentes áreas/unidades/servicios 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 del Ayuntamiento, 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 (Privacy by Design). 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 el Ayuntamiento 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 Superior del Ayuntamiento.

- **Elaborar la normativa de Seguridad de la Información** para su aprobación en coordinación con el Ayuntamiento.

- **Verificar la idoneidad de los procedimientos de seguridad de la información** y demás documentación.

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

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

- **Promover la realización de las auditorías periódicas ENS y LOPDGDD** que permitan verificar el cumplimiento de las obligaciones del Ayuntamiento en materia de seguridad.

Los roles previstos por el ENS y el reglamento de funcionamiento de la Comisión se determinarán y aprobarán por Decreto de Alcalde.

4. Datos personales

El Ayuntamiento realiza tratamientos en los que emplea datos personales adoptando las pertinentes medidas de seguridad para cumplir con las directrices del RGPD y las indicaciones de la persona DPD. Asimismo, de esta forma se garantiza que se mantiene la suficiente diligencia para cumplir con el principio de responsabilidad proactiva y *accountability* que establece la actual normativa de seguridad.

El Ayuntamiento sólo recogerá datos personales 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, los cuales se registraran en el Registro de Actividades del Tratamiento del propio Ayuntamiento.

Cada departamento municipal se encargará de gestionar y mantener la seguridad referente a los datos personales incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos personales recogidos en el mencionado Registro de Actividades del Tratamiento.

5. Gestión de riesgos

5.1 Justificación

Todos los sistemas sujetos a esta Política de Seguridad realizarán un proceso de análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. El gobierno y la gestión de la seguridad de la información se guiarán por los resultados de los procesos de análisis y gestión de riesgos. Este análisis se repetirá:

- Al menos cada año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

5.2 Criterios de evaluación de riesgos

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a la ciudadanía.

5.3 Directrices de tratamiento

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.

5.4 Riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad.

Los niveles de riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad al Comité de Seguridad, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

5.5 Realización o actualización de evaluaciones de riesgos

Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y, en especial, las Guías elaboradas por el Centro Criptológico Nacional (CCN). Esta evaluación de los riesgos se repetirá regularmente para los sistemas de información teniendo en cuenta las recomendaciones formuladas por dicho Centro.

Existe un compromiso por parte del Ayuntamiento, y una obligación por parte de los/as Responsables de la Información, de realizar análisis de riesgos y atender a sus conclusiones. Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos los activos.

De igual manera, el análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 10 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

6. Gestión de incidentes de seguridad

6.1 Prevención

El Ayuntamiento 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 deben implementar las medidas mínimas de seguridad determinadas por el ENS regulado mediante Real Decreto 311/2022, de 3 de mayo, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el Ayuntamiento:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Establece áreas seguras para los sistemas de información crítica o confidencial.

6.2 Monitorización y detección

El Ayuntamiento establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS (existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los/as responsables regularmente.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

6.3 Respuesta

El Ayuntamiento establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

6.4 Recuperación

Para garantizar la disponibilidad de los servicios, el Ayuntamiento dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos. Se trata de los procedimientos y las normas contenidos en la Documentación de Seguridad del Ayuntamiento.

7. Obligaciones y responsabilidades del personal

Todo el personal con acceso a los sistemas de información tiene el deber de conocer y cumplir la Política de seguridad de la información y la normativa de seguridad derivada que se establezca.

A tal efecto, la Política de seguridad de la información será comunicada a todas las personas usuarias de los sistemas de información incluidos en el ámbito de la Administración Electrónica, de manera pertinente, accesible y comprensible. Su incumplimiento podrá ser sancionado de conformidad con la normativa disciplinaria correspondiente.

Asimismo, el personal perteneciente a empresas externas subcontratadas que tengan acceso a la documentación o información asociada a alguno de los servicios del Ayuntamiento tiene la obligación de conocer y cumplir esta Política de seguridad de la información.

Todo personal que emplee sistemas de tecnologías de la información y las comunicaciones recibirá formación para el manejo seguro de dichos sistemas. Se deberán establecer los procedimientos de control que garanticen el cumplimiento efectivo de esta Política, que serán efectuados por las áreas, departamentos y servicios municipales y los Organismos Autónomos

A continuación, se detallan las **responsabilidades** de todo el personal empleado de la entidad:

- La persona empleada se ha de responsabilizar de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber de las personas trabajadoras.
- La persona empleada se ha de responsabilizar de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- La persona empleada se ha de responsabilizar siempre que abandone el puesto de trabajo de cerrar su sesión o bloquear el equipo con contraseña.
- La persona empleada se ha de responsabilizar de guardar copias de todos los correos que incluyan anexos con datos personales vinculados a la entidad.
- Tendrá la obligación de cumplir la política de **mesa limpia**.

En el mismo sentido, los sistemas de información y la propia información solamente van a poder ser utilizados por las personas empleadas para los fines para los que inicialmente han sido creados y puestos en conocimiento de dichas personas.

De esta forma, **no se considera aceptable**:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual, así como la difusión de datos personales ni confidencial perteneciente a la entidad. Se está obligado a guardar secreto de la información incluso terminada la relación laboral.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad de las personas usuarias.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.

- Corromper o destruir datos de otras personas usuarias o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

8. Terceras partes

Cuando el Ayuntamiento 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 la coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento 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. 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 garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, 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 ENS cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el ENS, 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 de el/la 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/as responsables de la información y los servicios afectados antes de seguir adelante.

9. Desarrollo de la Política de Seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad a intervalos planificados, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La normativa de seguridad está a disposición de todo el personal de la organización que necesite conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones y cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

9.1 Seguridad de la gestión de recursos humanos

La seguridad ligada al personal es primordial para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios. Es por ello que los responsables de recursos humanos deben prestar atención a lo establecido en el ENS y en la presente Política de Seguridad, adoptando las medidas de seguridad oportunas, tales como la firma de un acuerdo de confidencialidad para todas las personas empleadas para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deben ser comunicadas regularmente a todas las personas trabajadoras y terceros si procede. Cuando se termine la relación laboral o contractual de las personas empleadas o personal externo, se les retiran los permisos de acceso a las instalaciones y la información y se les pide que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

9.2 Seguridad física y del entorno

Las instalaciones físicas pueden contar con diferentes tipos de medidas de protección: obstáculos físicos, medidas técnicas de vigilancia, sistemas de inteligencia y vigilantes y/o personal de seguridad.

Para asegurar la eficacia de la seguridad lógica se debe partir de la correcta seguridad física, ya que únicamente es esta la forma de evitar intromisiones, daños o accesos no autorizados.

Para ello, el Ayuntamiento garantiza el acceso autorizado a las instalaciones y cuenta con barreras físicas para asegurar los recursos que éstas alberguen.

9.3 Gestión de las comunicaciones y operaciones

El Ayuntamiento evita que se dé un uso malicioso de la red, y para ello controla el acceso a los servicios de redes tanto internas como externas, de forma que las personas usuarias no pongan en riesgo los servicios en cuestión. En este sentido, se hace uso de procedimientos de autorización para saber quién puede acceder a los recursos de la red, y de procedimientos de gestión para proteger los accesos a la red.

Todos los procedimientos que se deban llevar a cabo se encuentran debidamente documentados, y serán revisados, y, convenientemente modificados, en caso de que se produzcan cambios significativos de aquéllos establecidos inicialmente.

Hay procedimientos para la realización de copias de seguridad que se archivan para recuperar los datos en caso de incidencia. Por tanto, los datos son guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente. Si la información se guarda en el disco duro de un PC, la persona usuaria asignada a dicho PC es la responsable de realizar las copias de seguridad. Estas copias están claramente identificadas y se guardan en sitio seguro.

10. Control de accesos

El acceso al sistema de información, se controla y limita a las personas usuarias, procesos, dispositivos y otros sistemas de información, debidamente autorizadas, restringiendo el acceso a las funciones permitidas. Únicamente así cabe asegurar la protección de la información frente a accesos no autorizados. Es el Responsable del Servicio quien se ocupa de definir las necesidades de acceso a la información distinguiendo entre las relativas al conjunto de áreas y las relativas a cada persona usuaria.

Únicamente se facilita al personal la información pertinente para el desarrollo de la actividad a realizar. El Ayuntamiento ha de vigilar en todo momento que la seguridad de los recursos está asegurada.

10.1 Responsabilidad de las personas usuarias

El personal del Ayuntamiento debe actuar de forma preventiva para evitar y reducir los riesgos de los accesos no autorizados y de posibles daños. Para ello, las personas usuarias deben, entre otros:

- Mantener despejados de papeles y otros medios de almacenamiento de información.
- Guardar en espacios cerrados la información (especialmente fuera del horario laboral).
- Configurar los equipos informáticos para que queden bloqueados cuando la persona usuaria no se encuentra en su puesto de trabajo.
- Proteger los puntos de entrada y salida de correo, máquinas fax e impresoras, escáneres etc.

11. Documentación complementaria

Esta Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, Decálogo de Buenas Prácticas, etc.).

Del mismo modo, esta Política de Seguridad de la Información complementa las políticas de seguridad del Ayuntamiento en materia de protección de datos personales.

La Normativa de Seguridad estará a disposición de todo el personal de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Estará disponible para su consulta en: https://www.bergara.eus/es/Informacion-legal