POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE EIBAR

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado mediante Resolución de Alcaldía, de 15 de febrero de 2019. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y estará vigente hasta que sea reemplazada por una nueva.

La entrada en vigor de la presente Política de Seguridad de la Información del Ayuntamiento de Eibar supone la derogación de cualquier otra que existiera a nivel de las diferentes áreas, unidades y servicios municipales.

2. INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento de Eibar, conocedora de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso “su propia Información” es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todas las áreas, unidades y servicios del Ayuntamiento de Eibar, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el Ayuntamiento de Eibar, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

3. OBJETIVO

La Política de Seguridad de la Información del Ayuntamiento de Eibar, en adelante la Política de Seguridad de la Información, identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

La Política de Seguridad de la Información es el instrumento en que se apoya el Ayuntamiento de Eibar para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el Ayuntamiento de Eibar.

4. ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para las áreas, servicios y unidades del Ayuntamiento de Eibar a sus recursos y a los procesos afectados por el ENS, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.
Todos los miembros del Ayuntamiento de Eibar, afectados por el alcance del ENS tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. MISIÓN DEL AYUNTAMIENTO DE EIBAR

El Ayuntamiento de Eibar, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la ciudadanía. Para ello pone a disposición de la misma la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadanía y Ayuntamiento en esta relación.

6. PRINCIPIOS Y DIRECTRICES

Los principios y directrices que deben de contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, y/o a los servicios que se prestan.

Prevención.

El Ayuntamiento de Eibar 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 3/2010, de 8 de enero, 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 de Eibar:

- 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.

Detección.

El Ayuntamiento de Eibar 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 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los/as responsables regularmente.

Respuesta.

Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

Recuperación.

Para garantizar la disponibilidad de los servicios, el Ayuntamiento de Eibar 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 el Documento de Seguridad del Ayuntamiento de Eibar.

7. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Eibar, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, está integrado por las siguientes normas:

a) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
b) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas cuando entre en vigor.
c) Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público cuando entre en vigor.
d) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
e) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
f) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
g) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
h) Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
i) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
j) Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido del Estatuto Básico del Empleado Público.
k) Ley 59/2003, de 19 de diciembre, de firma electrónica.

l) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
m) Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

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

8. 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 uno de los/as usuarios/as de los sistemas de información del Ayuntamiento de Eibar son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Para una mejor respuesta a incidentes de seguridad, el Ayuntamiento de Eibar 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.

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, definidas y documentadas.

8.1. Comités: funciones y responsabilidades

El Comité de Seguridad estará constituido por los siguientes cargos y personas:

- Presidente/a: El/la concejal/a Delegado/a de Delegación de Gobierno Abierto.
- Secretaria/o: El/la técnico/a de Organización.
- Responsable de Seguridad del ENS: El/la el/la Secretario/a general del Ayuntamiento de Eibar.
- Responsable de Sistemas del ENS: El/la responsable del departamento de Informática.
- Responsable del Servicio: El/la el/la directora/a de Organización y Personal.
- Responsable de Información: El/la el/la técnico/a de Organización.

El Comité de Seguridad de la Información podrá convocar a las personas responsables de Seguridad de ENS de cada área municipal en función de las necesidades.

Las reuniones ordinarias del Comité de Seguridad de la Información tendrán una periodicidad anual.

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.
- 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 de Eibar.
- 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 de carácter personal.
- 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 que permitan verificar el cumplimiento de las obligaciones del Ayuntamiento en materia de seguridad.

8.2. Roles: funciones y responsabilidades

Los roles fundamentales en la Seguridad de la Información son los siguientes:

- Responsable del servicio, que será desempeñado por el/la directora/a de Organización y Personal.
- Responsable de seguridad del ENS, que será desempeñado por el/la Secretario/a general del Ayuntamiento de Eibar.
- Responsable de información, que se desempeñará por el/la técnico/a de Organización.
- Responsable de Sistema del ENS: El/la responsable del departamento de Informática.

A continuación se detallan y se establecen las funciones y responsabilidades de cada una de las figuras:

- La persona Responsable del Servicio, determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El/la Responsable de la Información, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El/la Responsable de Seguridad ENS, su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho.
- El/la Responsable del Sistema, es el/la encargado/a de las operaciones del sistema.

Las políticas y roles de seguridad de protección de datos residen en la Comisión de Seguridad.

8.3. Procedimientos de designación

El Ayuntamiento de Eibar procederá a realizar la constitución del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 4 años o cuando los puestos queden vacantes.

9. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Eibar solo recogerá 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. Estas medidas estarán recogidas en el Documento de Seguridad aprobado mediante Resolución de Alcaldía.

10. OBLIGACIONES 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 de Eibar 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, unidades y servicios municipales y los Organismos Autónomos.

11. GESTIÓN DE RIESGOS

La gestión de riesgos es parte esencial del proceso de seguridad y debe realizarse de manera continua sobre los sistemas de información, con el objetivo de mantener los entornos controlados y de minimizar los riesgos hasta niveles aceptables.

Las personas Responsables de la Información y de los Servicios responden de los riesgos sobre la información y los servicios, respectivamente, y asegurarán su seguimiento y control, sin perjuicio de la posibilidad de delegar estas tareas. Para ello, podrán contar en el proceso con la participación y asesoramiento de quienes sean Responsable de la Seguridad y Responsable de los Sistemas.

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 de Eibar, 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.

Dicho análisis se repetirá:

- Regularmente, al menos una vez cada dos años.
- Cuando cambie sustancialmente la información manejada o los servicios prestados.
- Cuando ocurra un incidente grave de seguridad o se descubran y reporten vulnerabilidades graves.

12. TERCERAS PARTES

Cuando el Ayuntamiento de Eibar preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la 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 Eibar 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 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.

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 ENS 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.

13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 de Eibar en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros 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 www.eibar.eus/documentodeseguridad.