Política de Seguridad de Zarauzko Udala

Contenido

1 APROBACIÓN Y ENTRADA EN VIGOR 3
2 OBJETIVOS Y MISIÓN DE ZARAUZKO UDALA 4
3 OBJETIVOS Y MISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 5
4 ALCANCE 8
5 MARCO NORMATIVO 10
6 REVISIÓN DE LA POLÍTICA 12
7 PRINCIPIOS Y DIRECTRICES EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. 13
7.1 Seguridad integral. 13
7.2 Gestión de riesgos. 13
7.3 Prevención, reacción y recuperación. 13
7.4 Líneas de defensa. 15
7.5 Reevaluación periódica. 15
7.6 La seguridad como función diferenciada. 16
8 ORGANIZACIÓN DE LA SEGURIDAD 17
8.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES 17
8.1.1 Pleno del Ayuntamiento. 18
8.1.2 Comité de Seguridad Corporativa. 18
8.2 ROLES: FUNCIONES Y RESPONSABILIDADES 20
8.2.1 Comité de Seguridad Corporativa 21
8.2.2 Responsable del Servicio: 21
8.2.3 Responsable de la Información: 21
8.2.4 Responsable de Seguridad: 22
8.2.5 Responsable del Sistema: 23
8.2.6 Administrador de la Seguridad del Sistema 24
8.2.7 Responsable del tratamiento 25
8.2.8 Delegado de Protección de Datos 26
9 ANÁLISIS Y GESTIÓN DE RIESGOS 27
10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 28
10.1 Instrumentos de desarrollo 28
10.2 Aprobación de las normas de seguridad 29
10.3 Sanciones previstas por incumplimiento 29
11 CLASIFICACIÓN DE LA INFORMACIÓN 30
12 DATOS DE CARÁCTER PERSONAL 31
13 CONCIENCIACIÓN Y FORMACIÓN. 32
14 OBLIGACIONES DEL PERSONAL 33
15 TERCERAS PARTES 34
HISTORIAL DE MODIFICACIONES 35

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado por el *Comité de Seguridad Corporativa*, y aprobado por el Pleno de Zarauzko Udala.

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

La entrada en vigor de la presente Política de Seguridad de la Información de Zarauzko Udala supone la derogación de cualquier otra que existiera a nivel de los diferentes departamentos municipales.

Zarauzko Udala mantendrá en su sede electrónica la versión actualizada del documento de Política de Seguridad de la Información.

2 OBJETIVOS Y MISIÓN DE ZARAUZKO UDALA

Zarauzko Udala, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la ciudadanía. Asimismo, se desea potenciar el uso de las nuevas tecnologías en Zarauzko Udala y en la propia 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.

Los principales objetivos que se persiguen entre otros son:

- Fomentar la relación electrónica de la ciudadanía con Zarauzko Udala.
- Crear la confianza necesaria entre ciudadano y Zarauzko Udala en esta relación.

Para ejercer las competencias municipales Zarauzko Udala hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

3 OBJETIVOS Y MISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo del presente documento, pretende determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refieren las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Zarauzko Udala ha establecido un marco de gestión de la seguridad de la información según lo establecido por 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, reconociendo así como activos estratégicos la información y los sistemas que la soportan, y el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

La misión de la implantación de este marco de referencia es el asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de Zarauzko Udala.

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 Zarauzko Udala.

El marco de gestión de seguridad de la información abarca igualmente la protección de datos de carácter personal y tiene en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD, así como lo contemplado en la legislación de carácter nacional en dicha materia.

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

- Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por Zarauzko Udala.

- 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 protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

- Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

- Proteger los recursos de información de Zarauzko Udala y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y legalidad de la información.

Esta Política de Seguridad asegura un compromiso manifiesto de las máximas Autoridades de Zarauzko Udala, para la difusión, consolidación y cumplimiento de la presente Política.

4 ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para todos los Departamentos Municipales de Zarauzko Udala, entendiendo por Departamentos Municipales a sus Áreas y Distritos, sus Sociedades Mercantiles (Zarautz-Lur) y demás entes que decida la Junta de Gobierno Local; 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 o acuerdos con terceros.

Se determinará el alcance desde un doble punto de vista, el organizativo por un lado y el relativo a sistemas de información o alcance funcional.

En cuanto a este último, esta Política se aplicará a los sistemas de información de Zarauzko Udala, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo. Existen recursos que se utilizan para las relaciones entre administraciones y ciudadanos que han sido creadas y siguen siendo mantenidas por empresas privadas. Son aplicaciones y páginas web cuyo desarrollo ha sido encargado a éstas por diferentes departamentos e incluso organismos municipales. En lo que a éstos se refiere, se deberán incluir dentro del ámbito de la ENS, y se deberá notificar a estas empresas los criterios de seguridad por los que se rige Zarauzko Udala, sus organismos autónomos y sus sociedades públicas a fin de que adecuen los recursos a estos requisitos de seguridad.

En lo que al punto de vista organizativo se refiere, y en lo relativo al ENS, las obligaciones del mismo vinculan directamente a Zarauzko Udala y sus sociedades.

Este esfuerzo de integración se debe a cuatro factores:

- Estas sociedades están ofreciendo servicios y trámites que parten de

competencias propias municipales por lo que resulta obligatorio asegurarse de la seguridad de los sistemas y de la protección de datos.

- En caso de que haya incidencias de seguridad, la responsabilidad última recae sobre el propio Ayuntamiento.
- Fijar unas normas, unos criterios y unas responsabilidades compartidas en materia de seguridad de la información contribuye a una mayor cohesión y a un mejor servicio.
- El ciudadano percibe la presencia de Zarauzko Udala en estas sociedades, y atribuye la responsabilidad última de su actuación a éste.

Todos los miembros de Zarauzko Udala, afectados por el alcance del ENS tienen la obligación de conocer y cumplir esta Política de Seguridad, así como la Normativa de seguridad que la complementa, siendo responsabilidad del Comité de Seguridad Corporativa disponer los medios necesarios para que la información llegue al personal afectado.

5 MARCO NORMATIVO

El marco normativo de las actividades de Zarauzko Udala en el ámbito de la Política de Seguridad de la Información está integrado por las siguientes normas:

- Ley 7/1985, Reguladora de las Bases del Régimen Local.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 33/2003, del Patrimonio de las Administraciones Públicas.
- Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación del 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.

- Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.
- Ley 27/2013, de Racionalización y Sostenibilidad de la Administración Local
- Ley 9/2014, General de Telecomunicaciones.
- Real Decreto 8/2014, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 18/2014, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de Régimen Jurídico del Sector Público.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de Zarauzko Udala en el ámbito de sus competencias y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por la Corporación igualmente en el ejercicio de sus competencias.

6 REVISIÓN DE LA POLÍTICA

Esta Política ha sido propuesta y revisada por el **Comité de Seguridad Corporativa** de Zarauzko Udala, aprobado mediante Decreto Núm. 1503 de 25 de octubre de 2018, para que la conozcan todas las partes afectadas.

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización municipal, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la organización.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Pleno del Ayuntamiento para resolución de los mismos, previo informe propuesta del Comité de Seguridad Corporativa.

7 PRINCIPIOS Y DIRECTRICES EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

7.1 Seguridad integral.

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

7.2 Gestión de riesgos.

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

7.3 Prevención, reacción y recuperación.

La seguridad del sistema debe contemplar aspectos de prevención, detección, respuesta y recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

Zarauzko Udala 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 responsables deben implementar las medidas mínimas de seguridad determinadas por el ENS y por el RLOPD para tratamientos automatizados.

Así mismo deberán tenerse en cuenta las medidas especificadas en el artículo 32 del Reglamento UE 2016/679, que deberán garantizar un nivel de seguridad adecuado al riesgo para tratamientos automatizados, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, en particular:

- Para garantizar el cumplimiento de la Política de Seguridad de la Información, los órganos responsables deben:
  - **Autorizar** los sistemas o los servicios antes de entrar en operación.
  - **Evaluar regularmente la seguridad**, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
  - Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.
- Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración 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 según lo establecido en el artículo 9 del ENS.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, los órganos responsables deberán establecer mecanismos de informe que lleguen al responsable de seguridad.

- Los órganos responsables deben establecer mecanismos para

responder eficazmente a los incidentes de seguridad.

Con el fin de garantizar la disponibilidad de los servicios críticos, los órganos responsables deben contar con planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7.4 Líneas de defensa.

El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

- Ganar tiempo para una reacción adecuada.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

7.5 Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

7.6 La seguridad como función diferenciada.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, siendo el Responsable de la Información quien determinará los requisitos de la información tratada, el Responsable del Servicio quien determinará los requisitos de los servicios prestados, y el Responsable de Seguridad quien determinará las decisiones técnicas para satisfacer los requisitos de seguridad de la información y de los servicios.

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 usuarios de los sistemas de información de Zarauzko Udala 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, Zarauzko Udala 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 un comité con funciones concretas, definidas y documentadas.

8.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

Tomando como base esta política, la organización de la seguridad detalla la gestión interna del Comité de Seguridad Corporativa, identificando a todos sus miembros y detallando las atribuciones de cada responsable así como los mecanismos de coordinación y resolución de conflictos.

8.1.1 Pleno del Ayuntamiento.

En materia de seguridad de la información, la el Pleno de Zarauzko Udala tiene las siguientes funciones:

- Aprobar la Política de Seguridad de la Información de Zarauzko Udala y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad y el Reglamento General de Protección de Datos.
- Aprobar el desarrollo organizativo propuesto por el Comité de Seguridad Corporativa.
- Nombramiento y cese de los integrantes del Comité de Seguridad Corporativa.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité de Seguridad Corporativa.
- Nombrar al Delegado de Protección de Datos de Zarauzko Udala.

8.1.2 Comité de Seguridad Corporativa.

El Comité de Seguridad Corporativa, aprobado mediante Decreto Núm. 1503 de 25 de octubre de 2018, será encargado de coordinar la seguridad de la información en Zarauzko Udala e informará a los órganos de gobierno del mismo.

Estará formado por:

- ✓ Responsable del Servicio.

- ✓ Responsable de la Información.
- ✓ Responsable de Seguridad.
- ✓ Responsable del Sistema.
- ✓ Administrador de Seguridad de Sistemas.
- ✓ Delegado de Protección de datos (DPO-DBO).

El Comité de Seguridad Corporativa tendrá las siguientes funciones:

- ➢ Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información en Zarauzko Udala.
- ➢ Elaborar la estrategia de evolución de Zarauzko Udala en lo que respecta a seguridad de la información.
- ➢ Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- ➢ Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por Pleno del Ayuntamiento.
- ➢ Aprobar la Normativa de Seguridad de la Información.
- ➢ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- ➢ Monitorizar los principales riesgos residuales asumidos por Zarauzko Udala y recomendar posibles actuaciones respecto de ellos.
- ➢ Monitorizar el desempeño de los procesos de gestión de incidentes

de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Promover la realización de las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de Zarauzko Udala y en particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Priorizar 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 TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Informar regularmente del estado de la seguridad de la información al Pleno del ayuntamiento.

8.2 ROLES: FUNCIONES Y RESPONSABILIDADES

Tomando como base esta política, existirá un documento de organización de

la seguridad, en el que se recojan las funciones de los diferentes responsables, así como los mecanismos de nombramiento y cese de los mismos.

Los responsables de la seguridad de Zarauzko Udala son los siguientes:

8.2.1 Comité de Seguridad Corporativa

Las funciones y responsabilidades de cada figura del comité de Seguridad Corporativa, será el siguiente:

8.2.2 Responsable del Servicio:

De acuerdo con lo especificado en el ENS, le corresponde la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de los servicios.

Sus funciones son:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

8.2.3 Responsable de la Información:

De acuerdo con lo especificado en el ENS, le corresponde la potestad de establecer los requisitos de la información en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de la información.

El Responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección, siendo el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Sus funciones 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 en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

8.2.4 Responsable de Seguridad:

Cumplirá funciones relativas a la seguridad de los sistemas de información de Zarauzko Udala, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en Zarauzko Udala. Es el equivalente al "Responsable de Seguridad" enunciado en el Esquema Nacional de Seguridad (RD 3/2010).

Sus funciones son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.

- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

8.2.5 Responsable del Sistema:

Esta figura será la encargada de las operaciones del sistema y sus funciones son:

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar

en el Sistema y aprobar las modificaciones importantes de dicha configuración.

- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

8.2.6 Administrador de la Seguridad del Sistema

Administrará las funcionalidades de seguridad determinadas por los responsables anteriores, sus funciones son:

- 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 de

que la actividad desarrollada en el sistema se ajusta a lo autorizado.

- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los 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.

8.2.7 Responsable del tratamiento

De acuerdo con lo especificado en el RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

8.2.8 Delegado de Protección de Datos

Tiene asignadas las funciones contempladas en el art. 39 del Reglamento General de Protección de Datos.

- Informar y asesorar al responsable o al encargado del tratamiento.
- Supervisar el cumplimiento del RGPD por el responsable o encargado, incluyendo:
  - La asignación de responsabilidades
  - La concienciación y formación del personal
  - Las auditorías correspondientes
- Asesorar acerca de las Evaluaciones de Impacto (EIPD) y supervisar su aplicación.
- Cooperar y actuar como punto de contacto con la autoridad de control.

9 ANÁLISIS Y GESTIÓN DE RIESGOS

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:

- Regularmente, al menos una vez al año.
- Cuando cambie la información y/o los servicios prestados,
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.

Para el análisis y gestión de riesgos se ha usado una metodología basada en Magerit cuyos principales parámetros implicados sean el valor del activo, la probabilidad de ocurrencia de la amenaza y el Impacto sobre el activo.

El nivel de riesgo máximo aceptable, se ha establecido en base a la metodología elegida y se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen. Como complemento a lo dicho en este apartado de la política, existe un documento en formato "Excel" donde se pueden consultar los parámetros y el umbral de riesgo, la matriz de riesgos (probabilidad de amenaza e impacto) y la gestión del riesgo realizada sobre los activos no esenciales de Zarauzko Udala.

(Consultar "Matriz_Riesgo- Ayto. Zarautz.xlxs")

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se establecen las líneas base que debe constituir Zarauzko Udala para una gestión eficiente de esta Política de Seguridad y de la Normativa de seguridad que la complemente.

10.1 Instrumentos de desarrollo

La Política de Seguridad de la Información de Zarauzko Udala se desarrollará por medio de **una normativa de seguridad** que complemente la primera, y que, regulará normas específicas de seguridad de la información de un área o aspecto determinado, aprobadas por el Comité de Seguridad Corporativo, entre ellas:

- El uso correcto de equipos, servicios e instalaciones.
- Lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.
- Normativa técnica de componentes de Seguridad.

El Responsable de Seguridad podrá aprobar procesos, procedimientos TIC o instrucciones técnicas TIC de un determinado ámbito de actuación

La normativa de seguridad estará disponible en la intranet municipal a disposición de todos los miembros de la organización municipal que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

(El catálogo de normas y procedimientos que desarrollan esta política se describen en el documento: "Documentación de Seguridad- Ayto. Zarautz.docx", asimismo la reglamentación

interna se encuentra disponible en el documento "Normativa Interna de Seguridad- Ayto. Zarautz.docx")

10.2 Aprobación de las normas de seguridad

En toda la organización municipal, la aprobación de las normas técnicas de seguridad se hará de acuerdo a lo dispuesto en la presente política.

10.3 Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la normativa sobre régimen disciplinario de los empleados públicos.

11 CLASIFICACIÓN DE LA INFORMACIÓN

Se ha desarrollado una clasificación de la Información de Zarauzko Udala de forma que se identifiquen los distintos tipos de información utilizadas por la entidad, en base a su sensibilidad, y, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.

El procedimiento de clasificación de la documentación ha partido de la valoración realizada a la información esencial de Zarauzko Udala, establecida mediante el campo "sensibilidad". Este procedimiento queda desarrollado en el apartado 2.3 del documento "*Categorización - Ayto. Zarautz.docx*".

La información se clasificado en 3 ámbitos:

- Información pública: información que puede ser divulgada en cualquier medio sin que esto suponga ningún riesgo para la seguridad de la información de Zarauzko Udala.
- Información privada (de uso interno): información que puede ser conocida únicamente por personal de Zarauzko Udala.
- Información confidencial: información que solo puede ser conocida por la Alcaldía y/o personas delegadas o por el personal de algún Servicio Municipal concreto de Zarauzko Udala.

(Esta política de clasificación de la información se desarrolla en el documento: "Categorización - Ayto. Zarautz.docx")

12 DATOS DE CARÁCTER PERSONAL

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento de los servicios municipales de Zarauzko Udala se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Las medidas de protección de los datos de carácter personal se establecerán a partir de los resultados del Análisis de Riesgos y de la Evaluación de Impacto prevista en el Reglamento General de Protección de Datos.

Todos los sistemas de información de Zarauzko Udala se ajustarán a los niveles de seguridad requeridos por esta normativa.

13 CONCIENCIACIÓN Y FORMACIÓN.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos.

El personal de Zarauzko Udala recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

Se establecerá un programa de concienciación continua dirigido a todos los miembros de Zarauzko Udala, en particular a los de nueva incorporación.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

(Esta política de concienciación y formación se desarrolla en el documento: "Normativa Interna de Seguridad- Ayto. Zarautz.docx")

14 OBLIGACIONES DEL PERSONAL

Todos los miembros de la organización municipal y las empresas y personas terceras que realicen servicios de cualquier clase contratados por Zarauzko Udala o que de alguna manera se presten bajo el control y/o la dirección de Zarauzko Udala 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/as.

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.

(Las funciones y obligaciones del personal se desarrollan en el documento: "Normativa Interna de Seguridad- Ayto. Zarautz.docx")

15 TERCERAS PARTES

Cuando Zarauzko Udala **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 coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Zarauzko Udala **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 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 de la Información 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, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

(Las medidas de seguridad con Terceros se desarrollan en el documento: "Normativa Interna de Seguridad- Ayto. Zarautz.docx")

HISTORIAL DE MODIFICACIONES

REVISIÓN	FECHA	MODIFICACIÓN
01	03/09/18	Redacción inicial.
02	28/09/18	Inclusión de responsables
		–