Política de Seguridad de la Información

ajuntament D'eivissa

PATRONAT D'ESPORTS
AJUNTAMENT D'EIVISSA

PATRONAT DE MÚSICA
AJUNTAMENT D'EIVISSA

MUSEU D'ART CONTEMPORANI D'EIVISSA

CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR.

Texto aprobado por Decreto de Alcaldía, el día de su firma digital.

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 del Ayuntamiento de Eivissa supone la derogación de cualquier otra que existiera a nivel de los diferentes departamentos municipales.

2. OBJETIVO.

La Política de Seguridad de la Información del Ayuntamiento de Eivissa y sus Organismos autónomos, 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 apoyan el Ayuntamiento de Eivissa y sus Organismos autónomos 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 Eivissa.

El Ayuntamiento de Eivissa, 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 población del municipio de Eivissa.

El Ayuntamiento de Eivissa ejerce sus competencias, en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Islas Baleares.

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

El Ayuntamiento de Eivissa 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 el ámbito de la administración

electrónica, reconociendo así como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales 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 del Ayuntamiento de Eivissa.

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:

1. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por el Ayuntamiento de Eivissa.

2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

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

4. Proteger los recursos de información del Ayuntamiento de Eivissa 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, legalidad y confiabilidad de la información.

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

3. ALCANCE.

Esta Política de Seguridad de la Información será de obligado cumplimiento para todos los órganos superiores y directivos del Ayuntamiento de Eivissa y sus Organismos autónomos, así como para terceras partes a las que el Ayuntamiento de Eivissa y sus Organismos autónomos presten servicios, cedan información, o de las que utilicen servicios o manejen información.

Esta Política estará disponible para consulta de todos ellos a través de las Sedes Electrónicas, la Página web corporativa o la Intranet del Ayuntamiento de Eivissa.

Esta Política se aplica a todos los Departamentos Municipales del Ayuntamiento de Eivissa, entendiendo por Departamentos Municipales a sus Servicios, Negociados, Direcciones Generales, Organismos Autónomos, Sociedades Municipales con mayoría de capital social municipal y demás entes que decida la Alcaldía del Ayuntamiento de Eivissa; a sus recursos y a los procesos afectados por el Real Decreto 3/2010, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

4. 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, o los servicios que se prestan.

Prevención.

El Ayuntamiento de Eivissa 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 Esquema Nacional de Seguridad (en adelante, 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 de Seguridad de la Información, los órganos directivos 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.

Detección.

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, estos órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

Respuesta.

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

Recuperación.

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

5. MARCO NORMATIVO.

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

- 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.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- 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.
- Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
- 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
- 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.
- 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.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 414/2015, de 29 de mayo, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

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

6. ESTRUCTURA DOCUMENTAL.

Con el fin de asegurar una correcta 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 el ámbito de la administración electrónica, el Ayuntamiento de Eivissa ha diseñado un Sistema de Gestión de la Seguridad de la Información SGSI.

La documentación que compone el SGSI del Ayuntamiento de Eivissa se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel: Política de Seguridad de la Información.
b) Segundo nivel: Normativa de Seguridad de la Información.
c) Tercer nivel: Procedimientos de Seguridad de la Información.
d) Cuarto nivel: Instrucciones Técnicas de Seguridad de la Información

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos del Ayuntamiento de Eivissa y sus Organismos autónomos, sin necesidad de revisar su estrategia de seguridad.

El personal del Ayuntamiento de Eivissa y de sus Organismos autónomos tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, la Normativa, los Procedimientos y las Instrucciones Técnicas de Seguridad de la información estarán disponibles en una sección específica en la Intranet/Extranet corporativa de forma que sea accesible desde dentro y fuera del dominio.

6.1. Primer nivel: Política de Seguridad de la Información.

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto y aprobada por Decreto de Alcaldía.

6.2. Segundo nivel: Normativa de Seguridad de la Información.

El segundo nivel desarrolla la Política de Seguridad de la Información mediante normativas específicas que abarcan un área o aspecto determinado de la seguridad de la información.

La normativa de Seguridad de la Información será aprobada por el Alcalde a propuesta del Comité de Seguridad de la Información del Ayuntamiento de Eivissa, y especificará, al menos:

a) Lo que se considerará uso correcto de equipos, servicios e instalaciones.
b) Lo que se considerará uso indebido.
c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

6.3. Tercer nivel: Procedimientos de Seguridad de la Información.

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobados por la Alcaldía a propuesta del Comité de Seguridad de la Información del Ayuntamiento de Eivissa.

Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

6.4 Cuarto nivel: Instrucciones Técnicas de Seguridad de la Información.

El cuarto nivel desarrolla los Procedimientos de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información.

Las Instrucciones Técnicas de Seguridad de la Información serán aprobadas por el Comité de Seguridad de la Información del Ayuntamiento de Eivissa.

7. ORGANIZACIÓN DE LA SEGURIDAD.

La organización de la seguridad en el Ayuntamiento de Eivissa queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

Dentro de organigrama de la Organización podemos distinguir 3 niveles:

- **Nivel 1 – Órganos de Gobierno**: alta dirección, que entiende la misión de la Organización, determina los objetivos que se propone alcanzar y responde de que se alcancen. En este nivel se encontrará el **Responsable de la Información y de los tratamientos de datos personales y el Responsable de los Servicios.**

- **Nivel 2 – Dirección Ejecutiva**: gerencias, que entienden qué hace cada departamento y cómo los departamentos se coordinan entre sí para alcanzar

los objetivos marcados por la Dirección. En este nivel se encontrará el **Responsable de la Seguridad y Delegado de Protección de Datos.**

- **Nivel 3: Operacional**, que se centra en una actividad concreta y controla cómo se hacen las cosas. En este nivel estará el **Responsable del Sistema.**

7.1. Alcaldía

La Alcaldía del Ayuntamiento de Eivissa, asegura el compromiso de la corporación en la aplicación del ENS.

Este compromiso se manifiesta mediante la aprobación de la presente Política de Seguridad de la Información, así como de todas aquellas modificaciones o actualizaciones de la misma que el Comité de Seguridad de la Información pueda proponer, en el ámbito de sus competencias.

7.2. Comité de Seguridad de la Información: composición, funciones y responsabilidades.

La composición, funciones y responsabilidades del Comité se establecerán por Decreto de Alcaldía.

Serán funciones del Comité de Seguridad de la Información:

- Coordinar todas las funciones de seguridad de la Organización.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación sin fisuras en el caso de que deban ser activados.
- Elaborar la Política de Seguridad Corporativa, que será aprobada por la Alta Dirección.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los responsables de seguridad se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Atender a las inquietudes de la Alta Dirección y transmitírselas a los Responsables de Seguridad pertinentes. De estos últimos, recabar respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.
- Recabar de los Responsables de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes, se consolidan y resumen para la Alta Dirección.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad.

- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.

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

El Comité de Seguridad de la Información estará compuesto por:

- Responsable de la Información y de los tratamientos de datos personales (Nivel 1 - Órganos de gobierno).
- Responsable de los Servicios (Nivel 1 - Órganos de gobierno).
- Responsable de Seguridad (Dirección Ejecutiva - Nivel 2).
- Delegado de Protección de Datos (Dirección Ejecutiva - Nivel 2).
- Responsable del Sistema (Nivel 3 – Operacional).
- Administrador de la Seguridad del Sistema (Nivel 3 – Operacional, de perfil técnico).
- Vocales (Según necesidad).

7.3 Responsable de la Información y de los tratamientos de datos personales.

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa. Sus funciones y responsabilidades son:

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

7.4 Responsable de los Servicios.

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa. Sus funciones y responsabilidades 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.

7.5. Responsable de Seguridad de la Información.

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa. Será el encargado de establecer las medidas necesarias para cumplir los requisitos de seguridad establecidos por el responsable de la información y de los servicios manejados por el sistema.

Teniendo en cuenta la complejidad organizativa y funcional de los medios electrónicos utilizados por el Ayuntamiento de Eivissa, en ejercicio de la potestad de

autoorganización de la Administración municipal, el Responsable de Seguridad podrá asignar diversos cometidos a unidades orgánicas o empleados públicos, o especializar funciones por razones técnicas u organizativas. Esta asignación no supondrá en ningún caso una delegación de las competencias que le corresponden.

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

a. Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b. Analizar y elevar al Comité de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.
c. Identificar los niveles de seguridad de la información tratada y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
d. Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.
e. Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
f. Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.
g. Realizar o promover auditorias periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
h. Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.
i. Realizar, junto al Responsable de los Servicios y contando con la participación del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
j. Valorar los riesgos residuales respecto de la información calculada en el análisis de riesgos.
k. Realizar el seguimiento y control de los riesgos.

7.6 Delegado de Protección de Datos

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa y se comunicaran sus datos de contacto a la Agencia Española de Protección de Datos. Sus principales responsabilidades, funciones y tareas son las siguientes:

a. Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
b. Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados

miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.

c. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
d. Identificación de las bases jurídicas de los tratamientos.
e. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
f. Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico distintas de las establecidas por la normativa general de protección de datos.
g. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
h. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
i. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
j. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
k. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
l. Diseño e implantación de políticas de protección de datos.
m. Auditoría de protección de datos.
n. Establecimiento y gestión de los registros de actividades de tratamiento.
o. Análisis de riesgo de los tratamientos realizados.
p. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
q. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
r. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
s. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
t. Realización de evaluaciones de impacto sobre la protección de datos.
u. Relaciones con las autoridades de supervisión.
v. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

7.7. Responsable del Sistema.

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa. Sus responsabilidades son las siguientes:

a. Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la

seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.

b. Realizar, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
c. Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
d. Realizar el seguimiento y control de los riesgos.
e. Suspender, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

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

7.8. Administrador de la Seguridad del Sistema.

Será designado por Decreto de Alcaldía del Ayuntamiento de Eivissa. Este rol es compatible con el de Responsable del Sistema. Sus responsabilidades son las siguientes:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
b. 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.
c. 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.
d. La aplicación de los Procedimientos Operativos de Seguridad.
e. Aplicar cambios en la configuración vigente del Sistema de Información.
f. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
g. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
h. 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.
i. 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.
j. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
k. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.9. Resolución de conflictos.

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

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

8. SEGURIDAD DE LA INFORMACIÓN

8.1 Clasificación de la Información

Es necesario clasificar la información utilizada en los distintos Departamentos Municipales para dejar bien definido quién debe hacer qué con qué información. Se debe establecer niveles de información en función de sus exigencias de seguridad. Estos nivelen son: CONFIDENCIAL, DIFUSIÓN LIMITADA, SIN CLASIFICAR y PÚBLICO.

Toda la documentación, digital o impresa, debe indicar la clasificación de la información que contiene, salvo la información catalogada como PÚBLICA.

Para dicha clasificación se definirán procedimientos de control tales como:

- Procedimiento para clasificar información: quién determina a qué clase pertenece y en base a qué criterios.
- Procedimiento para cambiar la clasificación: quién puede alterar la etiqueta de una información, en base a qué criterios y dejando qué registro.
- Procedimientos para tratar la información en base a su nivel.

La clasificación de la información debe tener en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella.

9. DATOS DE CARÁCTER PERSONAL.

El Ayuntamiento de Eivissa trata datos de carácter personal. El registro de tratamientos de datos personales está publicado en la página web, Portal de transparencia o Sede electrónica del Ayuntamiento de Eivissa.

Cada departamento municipal se encargará de gestionar y mantener actualizado el registro de actividades del tratamiento en los que aparece como responsable de los mismos.

Todos los sistemas de información del Ayuntamiento de Eivissa se ajustarán a los niveles de seguridad requeridos por la normativa.

10. GESTIÓN DE RIESGOS.

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

a. Regularmente, al menos una vez al año.
b. Cuando cambie la información manejada.
c. Cuando cambien los servicios prestados.
d. 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.
e. 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 la armonización de los Análisis de Riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información, asimismo, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

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

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

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

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el

Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El Comité STIC trasladará a la Concejalía de Sistemas de Información y Mejora Continua las necesidades de inversión en materia de seguridad detectadas mediante dichos análisis.

11. OBLIGACIONES DEL PERSONAL

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

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

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

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

12. TERCERAS PARTES.

Cuando el Ayuntamiento de Eivissa utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité de Seguridad de la Información establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Eivissa preste servicios a otros organismos o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se exigirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

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

Cuando el Ayuntamiento de Eivissa 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 deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13. REVISIÓN.

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

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad como a la adaptación a los cambios en el marco legal, infraestructura tecnológica, organización general, etc. Entre los elementos a considerar se incluyen:

- Análisis y evaluación de riesgos.
- Resultados de auditorías o revisiones de terceros independientes o internas.
- Estado de las medidas preventivas o correctivas que pudieran estar planificadas.

- Análisis de cumplimiento por parte de las empresas que prestan los servicios en el Ayuntamiento.
- Tendencias asociadas a amenazas y vulnerabilidades.
- Información asociada a incidentes de seguridad identificados en el Ayuntamiento.
- Recomendaciones o directrices de órganos competentes.
- Cambios en el estándar adoptado como marco de referencia.

Se mantendrá un registro de las revisiones realizadas y se conservará, como evidencia, las actas aprobadas de las reuniones mantenidas con los cambios acordados en la Política de Seguridad de la Información.
Las sucesivas revisiones no exigen una aprobación de la política en su totalidad, sino que serán realizadas y entrarán en vigor cuando así lo acuerde el Comité de Seguridad.

14. DIFUSIÓN Y CUSTODIA DE LA POLÍTICA

El Ayuntamiento de Eivissa, a través del Comité de Seguridad de la Información, potenciará el conocimiento y difusión de la presente Política en los niveles adecuados, dado que interpreta este factor como crítico para asegurar su implantación eficaz y un cumplimiento efectivo.

Corresponde al Comité de Seguridad de la Información impulsar de forma efectiva la implantación de la Política de Seguridad de la Información.

La distribución a las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad se realizará tan sólo en los casos que sean oportunos para salvaguardar la Política de Seguridad de la Información del Ayuntamiento de Eivissa. Será responsabilidad del centro gestor o servicio promotor de expedientes de contratación realizar esta difusión y vigilancia de su cumplimiento.

Una vez aprobada y publicada, el original firmado o el fichero correspondiente validado por firma electrónica, quedará bajo la custodia del Responsable de Seguridad.

15. INCUMPLIMIENTO

El incumplimiento manifiesto por parte del personal laboral y funcionario del Ayuntamiento de Eivissa de la Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.