Diputación de Cádiz

POLITICA DE SEGURIDAD DE LA DIPUTACION PROVINCIAL DE CÁDIZ

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por decreto de la Presidencia de la Diputación Provincial de Cádiz.

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

2. INTRODUCCIÓN

La Diputación Provincial de Cádiz, sus Organismos Autónomos y las entidades de derecho público y privado vinculadas o dependientes de la misma dependen de los sistemas TIC (Tecnologías de la Información y la Comunicación) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando 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 los servicios prestados.

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 y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las Áreas deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes Áreas deben cerciorarse de 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.

Las Áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con la normativa en materia de Seguridad[1].

1 Artículo 7 del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica aprobado por RD 3/2010, de 8 de enero.

2.1. PREVENCIÓN

Las Áreas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las Áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, 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, las Áreas deben:

1. Autorizar los sistemas antes de entrar en operación.

2. Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

3. Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios 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 la normativa en materia de seguridad[2].

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo previsto en materia de seguridad[3]. Se establecerán mecanismos de detección, análisis y reporte[4] que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Las Áreas deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

- Designar punto de contacto para las comunicaciones con respecto a

2 Artículo 9 del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica aprobado por RD 3/2010, de 8 de enero.
3 Artículo 8 del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica aprobado por RD 3/2010, de 8 de enero.
4 A pesar de que "reportar" es un término obsoleto se utiliza en este documento de conformidad con lo previsto en la normativa en materia de Administración Electrónica, Seguridad y las guías que la desarrolla, como sinónimo de informe o noticia.

incidentes detectados en otras Áreas o en otros organismos.

- Establecer protocolos para el intercambio de información relacionada con el incidente.

2.4. RECUPERACIÓN

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

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades de derecho público y privado vinculadas o dependientes de la misma así como a todos los miembros de la organización, sin excepciones.

4. MISIÓN

Son objetivos de la presente Política de Seguridad los siguientes:

1. Garantizar la seguridad TIC y proteger los activos o recursos de información.

2. Crear la estructura de la organización de la seguridad TIC de la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes de la misma.

3. Marcar las directrices, los objetivos y los principios básicos de seguridad TIC de la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes de la misma.

4. Orientar la organización para la prestación de servicios basados en la gestión de riesgos.

5. Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad TIC.

5. MARCO NORMATIVO

En la redacción del presente documento, se ha tenido en cuenta el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS), aprobado por Real Decreto 3/2010, de 8 de enero, previsto en el art. 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (actualmente incluido en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público), que tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la

información. Y el Real Decreto 951/2015, de 23 de octubre, se modifica 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.

También se ha tenido en cuenta la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS».

Por último, se ha tenido en cuenta, la normativa actualmente aplicable en materia de datos de carácter personal: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento 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 (Reglamento general de protección de datos).

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1 ORGANIGRAMA

La organización de seguridad se divide en 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 incardina el Comité de Seguridad de la Información que es a su vez Responsable de la Información y Responsable del Servicio.

- Nivel 2 – Dirección Ejecutiva: gerencias, que entienden qué hace cada área y cómo las Áreas se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

  En este nivel se incardina el Responsable de la Seguridad.

- Nivel 3 – Operacional, que se centra en una actividad concreta y controla cómo se hacen las cosas.

  En este nivel se incardina el Responsable del Sistema asistido por los Responsables de Sistema Delegados y por los Administradores de la Seguridad del Sistema que se nombren.

6.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

1. El Comité de Seguridad de la Información está formado por el Responsable de Seguridad de la Información y por representantes de las Áreas que se determine por decreto de la Presidencia de la Diputación Provincial de Cádiz,

pudiendo en cualquier caso, a propuesta del Responsable de Seguridad, asistir a las reuniones cualquier miembro de la organización que se estime necesario para el correcto funcionamiento del Comité. La composición del Comité será revisada cada 2 años o cuando se estime pertinente por la Presidencia.

2. La Presidencia del Comité corresponde a la Presidencia de la Diputación Provincial de Cádiz o al Diputado/a Delegado/a que designe.

3. La Secretaría del Comité la asume el Responsable de la Seguridad y como tal le corresponde:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

4. El Comité de Seguridad de la Información se reunirá con carácter ordinario 2 veces al año y con carácter extraordinario por acuerdo de la Presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.

El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitidas, de conformidad con lo establecido en la legislación de régimen jurídico del sector público[5].

5. El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Como responsable de la Información tiene la potestad de establecer los requisitos de la información en materia de seguridad. O en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.
- Como responsable del Servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad. O en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
- Atender las inquietudes de la Corporación y de las diferentes Áreas.
- Informar regularmente del estado de la seguridad de la información a la Presidencia.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de

5 Artículo 17 de la ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

la Información.

- Elaborar la estrategia de evolución de la Diputación Provincial de Cádiz, Organismos Autónomos y entidades vinculadas o dependientes en lo que respecta a la 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 decreto de Presidencia de la Corporación.
- Proponer a Presidencia normativa de seguridad de la información para su aprobación si procede.
- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- Elaborar y proponer para su aprobación por la Presidencia los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Dar cuenta de los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Dar cuenta de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. 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 que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Proponer a la Presidencia para su aprobación planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes Áreas.
- 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 TIC.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Proponer el establecimiento de medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información y protección de datos de carácter personal.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Áreas de la Organización,

elevando a Presidencia aquellos casos en los que no tenga suficiente autoridad para decidir.

- En caso de ocurrencia de incidentes de seguridad de la información propondrá para su aprobación a Presidencia el Plan de Mejora de la Seguridad.

6. El Comité de Seguridad de la Información recabará regularmente del personal técnico propio, ya sea de la Diputación como de entidades dependientes o vinculadas, o externo, mediante la formalización de los correspondientes contratos, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

6.3. RESPONSABLE DE LA SEGURIDAD

1. El responsable de Seguridad será nombrado mediante decreto de la Presidencia de la Diputación Provincial de Cádiz a propuesta del Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

2. El Responsable de Seguridad tiene encomendadas las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. Elaborando para ello planes de concienciación y formación para su posterior aprobación por la Presidencia, previa supervisión del Comité de Seguridad de la Información.
- Determinar la categoría de los sistemas.
- Elaborar el análisis de riesgos.
- La declaración de aplicabilidad.
- Adoptar medidas de seguridad adicionales.

- Configurar la seguridad.
- Elaborar la documentación de seguridad del sistema y la normativa de seguridad.
- Proponer al Comité de Seguridad para su revisión y traslado a Presidencia los procedimiento operativos de seguridad elaborados por el Responsable del Sistema.
- Reportar al Comité de Seguridad de la Información el estado de la seguridad del sistema.
- Elaborar, junto al Responsable de Sistemas, los planes de mejora de la seguridad para su posterior aprobación por la Presidencia, previa supervisión por el Comité de Seguridad de la Información.
- Especificación del ciclo de vida de los sistemas: arquitectura, desarrollo, operación o cambios, para su posterior aprobación por la Presidencia, previa supervisión por el Comité de Seguridad de la Información.

3. En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad se podrán designar cuantos Responsables de Seguridad Delegados se considere necesarios.

La propuesta de designación corresponde al Responsable de la Seguridad y su nombramiento se efectuará por decreto de Presidencia. Por medio de la designación de delegados, se delegan las funciones que consten en el decreto de delegación. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

6.4. RESPONSABLE DEL SISTEMA

1. El responsable del Sistema será nombrado mediante decreto de la Presidencia de la Diputación Provincial de Cádiz a propuesta del Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

2. El Responsable de Sistema tiene encomendadas las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada por el Responsable de Seguridad y comunicada al Comité de Seguridad de la Información (como Responsable de la Información y de Servicios).

- Elaborar los procedimiento operativos de seguridad.

- Elaborar, junto al Responsable de Seguridad, los planes de mejora de la seguridad para su posterior aprobación por la Presidencia, previa supervisión por el Comité de Seguridad de la Información.

- Elaborar los planes de continuidad para su traslado al Responsable de seguridad y posterior aprobación, previo visto bueno del Comité de Seguridad de la Información, de la Presidencia.

- Remitir al Responsable de Seguridad la especificación del ciclo de vida de los sistemas: arquitectura, desarrollo, operación o cambios, para su posterior aprobación por la Presidencia, previa supervisión por el Comité de Seguridad de la Información.

3. En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema se podrán designar cuantos Responsables de Sistema Delegados considere necesarios.

La propuesta de designación corresponde al Responsable del Sistema y su nombramiento se efectuará por decreto de Presidencia. Por medio de la designación de delegados, se delegan las funciones que consten en el decreto de delegación. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reportan.

6.5. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA.

1. El Administrador de la Seguridad del Sistema será nombrado mediante decreto de la Presidencia de la Diputación Provincial de Cádiz a propuesta del Responsable del Sistema. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

2. El Administrador de la Seguridad del Sistema tiene encomendadas las siguientes funciones:

- 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 al Responsable de 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.

6.6. COORDINACION DE LOS MIEMBROS DE LA ORGANIZACION

1. El Administrador de Seguridad del Sistema reporta al Responsable del Sistema y al Responsable del Sistema Delegado:

- Los incidentes relativos a la seguridad del sistema.
- Las acciones de configuración, actualización o corrección

2. El Responsable del Sistema informa:

- Al Comité de Seguridad de la Información (como Responsable de la Información y del Servicio) de las incidencias funcionales relativas a los sistemas de información y de los servicios.
- Al Responsable de la Seguridad de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema, facilitará un resumen consolidado de los incidentes de seguridad e informará de la eficacia de las medidas de protección que se deben implantar.

3. El Responsable de la Seguridad reporta:

- Al Comité de Seguridad de la Información (en su condición de Responsable de la Información y de Servicios):
    1. Un resumen consolidado de actuaciones en materia de seguridad.
    2. Un resumen consolidado de incidentes relativos a la seguridad de la información.
    3. El estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto y de las desviaciones significativas de riesgo respecto de los márgenes aprobados
- A la Presidencia de la Diputación de la Organización, según lo que se acuerde en el Comité de Seguridad de la Información.

6.7. RESOLUCION DE CONFLICTOS

Los conflictos entre las diferentes personas u órganos responsables que componen la estructura organizativa de la política de seguridad de la información serán resueltos por el superior jerárquico común, en su defecto, prevalecerán las decisiones del Comité de Seguridad de la Información, en aquellos casos en que este no tenga bastante autoridad para decidir, el Comité lo elevará a Presidencia.

7. APROBACION Y MODIFICICACION DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. La Política de Seguridad se aprueba por decreto de la Presidencia de la Diputación de Cádiz, a propuesta del Comité de Seguridad de la Información.

2. Será misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y, si procede, la propuesta de revisión o mantenimiento de la misma. Las modificaciones de la Política, que procedan tras la revisión, será aprobada por decreto de la Presidencia de la Diputación de Cádiz a propuesta del Comité de Seguridad de la Información.

3. La Política de Seguridad de la Información aprobada y sus posteriores modificaciones serán difundida para que la conozcan todas las partes afectadas y publicada en la página web de la Diputación Provincial de Cádiz.

8. DATOS DE CARÁCTER PERSONAL

1. La Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes se ajustarán a lo exigido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento 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 (Reglamento general de protección de datos).

2. La Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes, como responsables del Tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con la normativa en la materia de acuerdo con el principio de responsabilidad proactiva.

3. El Delegado de Protección de Datos podrá poner en conocimiento del Comité de Seguridad de la Información las cuestiones relacionadas con la protección de datos que sean necesarias y participará, desde el inicio, en todas las cuestiones relacionadas con la protección de datos contribuyendo así al cumplimiento de la normativa en la materia.

4. En caso de conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información y el Delegado de Protección de Datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

9. GESTIÓN DE RIESGOS

1. Todos los sistemas sujetos a esta Política deberán realizar un análisis de

riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

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

3. El proceso de Gestión de Riesgos se divide en los siguientes pasos:

Paso 1 – Categorizar el sistema de información

- El Comité de Seguridad de la Información (como Responsable de la Información y de Seguridad), a propuesta del Responsable de Seguridad, establece los niveles de seguridad requeridos de la información y de los servicios[6].
- Se deduce automáticamente la categoría del sistema de información[7].

Paso 2 – Seleccionar medidas de seguridad

- El Responsable de la Seguridad realiza el pertinente análisis de riesgos.
- El Responsable de la Seguridad determina la Declaración de Aplicabilidad, teniendo en cuenta los mínimos requeridos por la normativa en materia de seguridad[8], y las medidas adicionales que se estimen oportunas.

Paso 3 – Implantar las medidas de seguridad

- El Administrador de Seguridad del Sistema (ASS) se encarga de

6 Ver Anexo I del ENS y guía CCN-STIC 803
7 Ver Anexo I del ENS
8 Ver Anexo II del ENS

aplicar las medidas acordadas[9].

Paso 4 – Evaluar la seguridad del sistema de información

- Corresponde al sistema de gestión que se emplee, pudiendo recurrir a auditoría externas cuando sea pertinente [10].
- Se evalúa el riesgo residual.

Paso 5 – Autorización para operar

- El Comité de Seguridad de la Información (como Responsable de la Información y de Servicio) acepta el riesgo residual sobre la información y los servicios.
- Puede ser necesario un plan de mejora de la seguridad para atender a los riesgos que no son aceptables, regresando al paso 2.

Paso 6 – Monitorizar

- El Administrador de Seguridad del Sistema (ASS) recopila información sobre el desempeño del sistema de información en materia de seguridad.
- El Responsable de la Seguridad monitoriza que el sistema de información se comporta dentro de los márgenes aceptados de riesgo.
- El Comité de Seguridad de la Información (como Responsable de la Información y de Servicio) es informado de desviaciones significativas del riesgo sobre los activos de los que son propietarios; si la desviación es elevada, el Responsable del Sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo

10. RESPUESTAS A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- ASS: Lleva a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- ASS: Aísla el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- ASS: Toma decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves

9 Ver guía CCN STIC 804
10Ver guía CCN STIC 802

(estas actuaciones deben estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).

- ASS: Asegura la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deben estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).

- ASS: Mantiene y recupera la información almacenada por el Sistema y sus servicios asociados.

- ASS: Investiga el incidente: Determina el modo, los medios, los motivos y el origen del incidente.

- El Responsable de Seguridad: Analiza y propone salvaguardas que prevengan incidentes similares en el futuro.

- El Responsable del Sistema: Planifica la implantación de las salvaguardas en el sistema.

- El Comité de Seguridad: Propone para su aprobación por la Presidencia de la Diputación Provincial de Cádiz el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.

- El Responsable del Sistema: Ejecuta el plan de seguridad aprobado.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Esta Política de Seguridad de la Información, que es de obligado cumplimiento, se desarrollará por medio de normativa de seguridad que afronte aspectos específicos, por procedimientos de seguridad y por el resto de documentación técnica que sea preciso elaborar. Toda normativa será aprobada mediante decreto de Presidencia a propuesta del Comité de Seguridad de la Información.

2. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Encontrándose disponible en la intranet e impresa en la sede de la Empresa Provincial de Información de Cádiz, S.A. (EPICSA).

12. AUDITORIAS DE SEGURIDAD

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, de conformidad con lo previsto en el Esquema Nacional de seguridad, al menos cada dos años, cuyo objeto será verificar el cumplimiento de los requerimientos de la normativa en materia de seguridad.

2. Los informes de auditoria serán presentados al Responsable del Sistema para

que analice y proponga las medidas correctoras, las lineas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad. Todo ello será presentado por el Responsable de Seguridad al Comité de Seguridad de la Información para que adopte las medidas necesarias.

13. OBLIGACIONES DEL PERSONAL

1. Todos los miembros de la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes 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 proponer los medios necesarios para que la información llegue a los afectados.

2. Todos los miembros de la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes atenderán a sesiones de concienciación en materia de seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

3. Las personas con responsabilidad en el uso, operación o administración de sistemas de la información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

14. TERCERAS PARTES

1. Cuando la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes 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 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.

2. Cuando la Diputación Provincial de Cádiz, sus Organismos Autónomos y entidades vinculadas o dependientes utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

3. 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 el Comité de Seguridad de la Información antes de seguir adelante.