DIPUTACIÓN DE BADAJOZ

BOLETÍN OFICIAL DE LA PROVINCIA
Boletín ordinario n.º 192
Anuncio **3937/2026**
miércoles, 7 de octubre de 2026

ADMINISTRACIÓN LOCAL
DIPUTACIONES
Diputación de Badajoz
Área Funcional de Presidencia y Relaciones Institucionales
Badajoz

Anuncio 3937/2026

"Resolución de la Presidenta de fecha 1 de octubre de 2026, sobre la aprobación de la política de seguridad de la Diputación de Badajoz"

Para general conocimiento, se hace pública la resolución dictada por la Presidenta de la Institución provincial, con fecha 1/10/2026, aprobando el documento de política de seguridad de la Diputación de Badajoz y su anexo, de conformidad con lo dispuesto en el artículo 12 del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que sustituye al hasta ahora vigente, aprobado mediante resolución de 3/3/2020, con el siguiente contenido literal:

"RESOLUCIÓN DE LA PRESIDENTA DE FECHA 1 DE OCTUBRE DE 2026, APROBANDO LA POLÍTICA DE SEGURIDAD DE LA DIPUTACIÓN DE BADAJOZ

En el ámbito de las administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos, comporta una obligación correlativa de las mismas, que tiene como premisas la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, exigiéndose una aplicación segura de las Tecnologías de la Información y la Comunicación –TIC-.

La seguridad se entiende como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. A tal efecto, la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en su artículo 42.2 dispone la creación, a través de Reglamento, del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad, en la utilización de los medios electrónicos que permitan la adecuada protección de la información.

En cumplimiento de la misma, se aprobó 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. Esta norma 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, siendo de aplicación a las administraciones públicas, para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios en los medios electrónicos que gestione en el ejercicio de sus competencias.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse, manteniéndose actualizado de forma permanente, conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos estándares internacionales sobre seguridad y auditoria, y la consolidación de las infraestructuras que le sirven de apoyo. Por ello es necesario actualizar el ENS, plasmándose en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Con la norma referida, se pretende proporcionar las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de una serie de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de manera que permita a los ciudadanos ejercer sus derechos, y a las administraciones cumplir sus deberes, a través de estos medios electrónicos.

A tal efecto, en el ámbito Europeo, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, regula las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. Además, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,

y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). También el Reglamento Delegado (UE) número 907/2014 de la Comisión de 11 de marzo de 2014, que completa el Reglamento (UE) número 1306/2013 del Parlamento Europeo y del Consejo, en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro. Anexo I - apartado 3 B) ii): "A partir del 16 de octubre de 2016, la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO/IEC 27001: Information Security management systems Requeriments (ISO) (Sistema de gestión de la seguridad de la Información-Requisitos) (ISO)".

En el ámbito Nacional, cabe destacar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, 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 y Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS.

En el ámbito Autonómico, la Ley 1/2002, de 28 de febrero, de Gobierno y Administración de la Comunidad Autónoma de Extremadura, la Ley 4/2013, de 21 de mayo, Gobierno Abierto de Extremadura, y por último el decreto 225/2014, de 14 de octubre, de régimen jurídico de Administración Electrónica de la Comunidad Autónoma de Extremadura.

De conformidad con el Real Decreto 311/2022 de 3 de mayo, su artículo 12 establece que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente", "se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

ñ) Mejora continua del proceso de seguridad."

En base a todo lo anterior, la Presidencia de la Diputación de Badajoz, en el ejercicio de las competencias que le otorga al efecto el artículo 34.1,o), de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, en relación con el artículo 12.2 del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad,

RESUELVE:

Primero.- Aprobar el documento "Política de seguridad de la Diputación de Badajoz", anexo a la presente resolución, que sustituye al hasta ahora vigente, aprobado por la Presidencia de la Corporación, mediante resolución de 3 de marzo de 2020.

Segundo.- Determinar la composición del Comité de Seguridad previsto en el documento de política de seguridad, integrado de la siguiente manera:

- Responsable de la Información y del Servicio, que es la Presidencia de la Diputación de Badajoz, o Diputado/a en quien delegue.
- Secretario/a General o funcionario/a en quien delegue.
- Responsable de la seguridad.
- Director/a del Área funcional de Innovación y Administración Digital.
- Director/a del Área funcional de Presidencia y Relaciones Institucionales.
- Gerente del Consorcio para la Gestión de Servicios Medioambientales en la Provincia de Badajoz (PROMEDIO).
- Gerente del Organismo Autónomo de Recaudación y Gestión Tributaria (OAR).
- Gerente del Consorcio Provincial de Prevención y Extinción de Incendios (CPEI).

- Gerente del Organismo Autónomo para la Protección de la Legalidad Urbanística (OAPLU_RESTAURA).
- Coordinador/a del Organismo Autónomo "Patronato Provincial de la Escuela de Tauromaquia".
- Delegado de Protección de Datos.

"La Presidencia del Comité corresponde a la Presidencia de la Diputación Provincial de Badajoz.

"La Secretaría del Comité la asume el responsable de seguridad.

"El citado Comité celebrará sesión constitutiva, dentro del plazo de un mes a la entrada en vigor del documento de política de seguridad.

Tercero.- Nombrar al:

- Director del Área funcional de Innovación y Administración Digital, como responsable de la seguridad.
- Jefe de Servicio de Tecnología y Sistemas Corporativos, perteneciente al Área funcional de Innovación y Administración Digital, como Responsable del Sistema de Diputación de Badajoz; sin menoscabo del nombramiento del resto de responsables del sistema de los diferentes organismos autónomos y entidades de derecho público y privado vinculadas o dependientes de la Diputación de Badajoz.

Cuarto.- El documento de política de seguridad será publicado en el Boletín Oficial de la Provincia, así como en la Web oficial de la Diputación de Badajoz, sin perjuicio de surtir efectos jurídicos, desde la fecha de firma de la resolución. El documento será objeto de difusión interna, por resultar de obligado cumplimiento a todos los miembros de la Diputación Provincial de Badajoz, sus organismos autónomos y las entidades de derecho público y privado vinculadas o dependientes de la misma.

Quinto.- El Área funcional de Innovación y Administración Digital realizará las acciones necesarias, a los efectos acordados.

Sexto.- Dar traslado de los acuerdos adoptados, al Pleno de la Corporación, en la próxima sesión ordinaria que celebre, de conformidad con lo establecido en el artículo 62 del RD 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

Lo dispone así la Presidenta de la Institución con fecha de firma electrónica, y por la Oficial Mayor, Secretaria General en funciones, se toma razón para su transcripción al libro electrónico de resoluciones, a los solos efectos de garantizar la integridad, autenticidad, calidad, confidencialidad, protección y conservación de los ficheros electrónicos correspondientes, conforme a lo dispuesto en el artículo 3.2, e) del Real Decreto 128/2018, de 16 de marzo, por el que se regula el Régimen Jurídico de los Funcionarios de Administración Local con Habilitación de Carácter Nacional.

La Oficial Mayor, Secretaria General en funciones, María Fernanda Rubio Cortés.

ANEXO

DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA DIPUTACIÓN DE BADAJOZ

1. Aprobación y entrada en vigor.

Este documento es efectivo desde la fecha de resolución aprobatoria de la Presidencia de Diputación de Badajoz, sin perjuicio de su publicación en el Boletín Oficial de la Provincia, así como en la Web oficial de la Diputación de Badajoz, permaneciendo en vigor, hasta que sea reemplazado por un nuevo documento de política de seguridad.

2. Introducción.

La Diputación Provincial de Badajoz, 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 a la normativa en materia de seguridad.

3. Alcance.

Esta política se aplica a todos los sistemas TIC de la Diputación Provincial de Badajoz, 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 de Diputación de Badajoz.

Las Diputaciones gestionan las competencias que las leyes atribuyen a las provincias, ejercitándolas y prestando su servicio a los ayuntamientos como tarea fundamental, garantizándoles la suficiencia y universalidad de la prestación de los servicios municipales básicos (abastecimiento de agua, recogida de residuos, obras públicas, etc..), especialmente a los de población inferior a 20.000 habitantes. También la Ley permite a las provincias, que sus diputaciones ejerzan competencias genéricas de fomento del desarrollo provincial.

En cualquier caso, las competencias provinciales, gestionadas por las diputaciones, lo son para garantizar la solidaridad y el equilibrio entre los municipios, de forma que no existan desigualdades, se presten unos servicios y se doten de unas infraestructuras suficientes para el bienestar de la ciudadanía en todos ellos, en especial a aquellos municipios que cuentan con menos recursos para poder cumplir con los servicios de competencia municipal.

Las competencias provinciales son las que les atribuyan las leyes, en todo caso:

- La coordinación de los servicios municipales entre sí para la garantía de la prestación integral y adecuada.
- La asistencia y cooperación jurídica, económica y técnica a los Municipios.
- La prestación de servicios públicos de carácter supramunicipal.
- La cooperación en el fomento del desarrollo económico y social y en la planificación en el territorio provincial.
- El ejercicio de funciones de coordinación en la elaboración y el seguimiento de la aplicación de las medidas contenidas en los planes económico-financiero.
- La asistencia en la prestación de los servicios de gestión de la recaudación tributaria, y de servicios de apoyo a la gestión financiera de los municipios con población inferior a 20.000 habitantes.
- La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20.000 habitantes.
- El seguimiento de los costes efectivos de los servicios prestados por los municipios de su provincia y su colaboración para una gestión coordinada más eficiente de los servicios que permita reducir estos costes.
- La contratación centralizada en los municipios con población inferior a 20.000 habitantes.
- La aprobación anual de un plan provincial de cooperación a las obras y servicios de competencia municipal, en cuya elaboración deben participar los municipios de la provincia.

Las competencias provinciales que ha de llevar a cabo la Diputación de Badajoz antes mencionadas implican el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones fomentadas por el uso de medios electrónicos.

Son objetivos del presente documento de política de seguridad los siguientes:

- Garantizar la seguridad TIC y proteger los activos o recursos de información.
- Crear la estructura de la organización de la seguridad TIC de la Diputación Provincial de Badajoz, sus organismos autónomos y entidades vinculadas o dependientes de la misma.
- Asegurar que se cumplen los requisitos legales aplicables.
- Asegurar que se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Orientar a la organización para la prestación de servicios basados en la gestión de riesgos.
- Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad TIC.
- Asegurar que cada empleado es responsable de cumplir esta política de seguridad y sus procedimientos según aplique a su puesto.
- Asegurar que se implementa, se mantiene y se realiza un seguimiento del Esquema Nacional de Seguridad.

5. Marco normativo.

El marco normativo que afecta al desarrollo de las actividades y competencias de la Diputación de Badajoz, está constituido por normas jurídicas estatales y autonómicas orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco, se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

También forman parte del referido marco, aquellas normas aplicables a la Administración Electrónica de Diputación de Badajoz, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de esta política de seguridad de Información.

6. Cumplimiento de artículos.

La Diputación de Badajoz, para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20).

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a Diputación de Badajoz estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

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

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos competenciales o contractuales.

b. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c. Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Vigilancia continua y reevaluación periódica (artículo 10) e integridad y actualización del sistema (artículo 21).

La Diputación de Badajoz ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Asimismo, solicitará la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 15) y profesionalidad (artículo 16).

Todos los miembros de Diputación de Badajoz dentro del ámbito del ENS, atenderán a sesiones de concienciación en materia de seguridad a lo largo del año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC 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.

Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14).

Todos los sistemas afectados por esta política de seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de 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 y/o los servicios prestados de manera significativa.

- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 25), prevención, detección, respuesta y conservación (artículo 8).

La Diputación de Badajoz ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, Diputación de Badajoz implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Diputación de Badajoz establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, Diputación de Badajoz dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Existencia de líneas de defensa (artículo 9) y prevención ante otros sistemas de información interconectados (artículo 23).

Diputación de Badajoz ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Diferenciación de responsabilidades (artículo 11) y organización e implantación del proceso de seguridad (artículo 13).

La Diputación de Badajoz ha organizado su seguridad comprometiendo a todos los miembros de la corporación, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "Organización de la seguridad" del presente documento.

Autorización y control de los accesos (artículo 17).

La Diputación de Badajoz ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 18).

La Diputación de Badajoz ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19).

Para la adquisición de productos, Diputación de Badajoz tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de seguridad.

Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26).

La Diputación de Badajoz ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de Diputación de Badajoz. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad y detección de código dañino (artículo 24).

La Diputación de Badajoz ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

7. Organización de la seguridad.

7.1 Estructura de la seguridad.

La organización de la seguridad se divide en tres grandes bloques de responsabilidad:

- Nivel de Gobierno: Recae la responsabilidad legal y la especificación de las necesidades o requisitos, que corresponde a la Dirección de la entidad y a los responsables del tratamiento, de la información y del servicio.
- Nivel Ejecutivo/Supervisión: Que corresponde al responsable de la seguridad y al Delegado de Protección de Datos, en sus respectivos ámbitos.
- Nivel Operacional: La operación del sistema de información, que corresponde al responsable del sistema y al Encargado del Tratamiento, en sus respectivos ámbitos.

7.2 Comité de Seguridad.

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

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

La Secretaría del Comité la asume el responsable de la seguridad y como tal le corresponde:

- Convocar las reuniones del Comité de Seguridad.
- 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.

El Comité de Seguridad se reunirá con carácter constitutivo dentro del mes siguiente a la entrada en vigor del presente documento de política de seguridad, 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 ajustará su funcionamiento a las normas reguladoras del funcionamiento de los órganos colegiados de la Ley 40/2015, de 1 de octubre y, a consecuencia, 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.

El Comité de Seguridad tendrá las siguientes funciones:

- 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 la información.
- Elaborar la estrategia de evolución de la Diputación Provincial de Badajoz, 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, que están alineados con la estrategia decidida en la materia evitando duplicidades.
- Elaborar (y revisar regularmente) la política de seguridad para que sea aprobada por decreto de Presidencia de la Corporación.
- Proponer a Presidencia normativa de la seguridad de la información para su aprobación si procede.
- 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.

- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- 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 auditorias 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.
- 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 TIC.
- 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.

El Comité de Seguridad 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 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.

7.3 Roles: Funciones y responsabilidades.

7.3.1 Responsable de la información y del servicio.

El responsable de la Información es el encargado de determinar los niveles de seguridad de la información de la Diputación de Badajoz. El responsable del servicio es el encargado de determinar los niveles de seguridad de los servicios disponibles en la Diputación de Badajoz. Atendiendo al concepto de responsabilidad unificada, ambas responsabilidades recaen sobre el titular de la Diputación de Badajoz, es decir, su Presidencia.

El Responsable de la Información y del Servicio tiene encomendadas las siguientes funciones:

- 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.
- 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.

7.3.2 Responsable de la seguridad.

El responsable de seguridad será nombrado mediante decreto de la Presidencia de la Diputación Provincial de Badajoz. El nombramiento se revisará cuando sea necesario o cuando el puesto quede vacante.

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.
- Elaborar y proponer para la aprobación por la Presidencia las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Reportar al Comité de Seguridad 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.
- Especificar el 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.
- Constituir el punto de contacto especializado para la coordinación con el CCN-CERT, notificar al mismo y sin dilación indebida de los incidentes que tengan efectos perturbadores en la prestación de los servicios, así como, recibir, interpretar y aplicar las instrucciones y guías emanadas por esta autoridad tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

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 reporta.

7.3.3 Responsable del sistema.

El responsable del sistema será nombrado mediante decreto de la Presidencia de la Diputación Provincial de Badajoz. El nombramiento se revisará cuando sea necesario o cuando el puesto quede vacante.

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 a la Presidencia la cual tomará la decisión final.
- Elaborar los procedimientos 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 del Comité de Seguridad.
- Elaborar los planes de continuidad para su traslado al responsable de seguridad y posterior aprobación, previo visto bueno del Comité de Seguridad, 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.

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 reporta.

7.4. Reportes y flujo de información.

El responsable del sistema reporta:

- Al 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, un resumen consolidado de los incidentes de seguridad e

informará de la eficacia de las medidas de protección que se deben implantar.

El responsable de la seguridad reporta:

- Al responsable de la Información y del Servicio las decisiones e incidentes en materia de seguridad que afecten a la información y los servicios, en particular del riesgo residual al que el sistema está expuesto y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Al Comité de Seguridad, en calidad de Secretario, un resumen consolidado de actuaciones en materia de seguridad, un resumen consolidado de incidentes relativos a la seguridad de la información e informará del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

7.5. Resolución de conflictos.

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

8. Aprobación y modificación del documento de la política de seguridad.

La política de seguridad se aprueba por decreto de la Presidencia de la Diputación de Badajoz.

Será misión del Comité de Seguridad la revisión anual de este documento de política de seguridad y, si procede, la propuesta de revisión o mantenimiento del mismo. Las modificaciones de este documento que procedan tras la revisión, serán aprobadas por decreto de la Presidencia de la Diputación de Badajoz a propuesta del Comité de Seguridad.

El documento de la política de seguridad aprobado y sus posteriores modificaciones será difundido para que lo conozcan todas las partes afectadas y publicado en la página Web oficial de la Diputación de Badajoz.

9. Datos de carácter personal.

La Diputación de Badajoz, 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).

La Diputación de Badajoz, 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.

El Delegado de Protección de Datos podrá poner en conocimiento del Comité de Seguridad 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.

En caso de conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad 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.

10. Desarrollo de la política de seguridad de la información.

Esta política de seguridad, 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.

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 corporativa de la Diputación de Badajoz.

Dentro del plazo de 6 meses a la entrada en vigor de la presente resolución, el Comité de Seguridad procederá a la aprobación de las normas y documentos necesarios para el desarrollo de la presente política de seguridad de la Información y a su publicación en la Intranet corporativa de la Diputación de Badajoz.

Queda sin efecto la política de seguridad aprobada por resolución de esta Presidencia con fecha 3 de marzo de 2020, y anteriores, en todo lo que se oponga o contradiga a la presente política de seguridad que ahora se aprueba, permaneciendo en vigor transitoriamente hasta tanto se aprueben las nuevas normas y documentos para el desarrollo de la política de seguridad de la Información de la Diputación de Badajoz.

11. Auditorías de seguridad.

Los sistemas de información serán objeto de una auditoria 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.

Los informes de auditoria serán presentados al responsable del sistema para que analice y proponga las medidas correctoras, las líneas 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 para que adopte las medidas necesarias.

12. Obligaciones del personal.

Todos los miembros de la Diputación Provincial de Badajoz, sus organismos autónomos y entidades vinculadas o dependientes tienen la obligación de conocer y cumplir esta política de seguridad y la Normativa de seguridad, siendo responsabilidad del Comité de Seguridad proponer los medios necesarios para que la información llegue a los afectados.

Se harán públicos los decretos aprobados por la Presidencia de la Diputación de Badajoz en las que se establecen los nombramientos del Comité de Seguridad.

Todos los miembros de la Diputación Provincial de Badajoz, 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.

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.

13. Terceras partes.

Cuando la Diputación Provincial de Badajoz, 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación Provincial de Badajoz, sus organismos autónomos y entidades vinculadas o dependientes utilicen 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en este documento.

Cuando algún aspecto de la política de seguridad 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 responsable de la información y del servicio antes de proseguir."