POLITICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE CÁCERES.

2. APROBACIÓN Y ENTRADA EN VIGOR

El texto será aprobado por acuerdo del Excmo. Ayuntamiento-Pleno y su entrada en vigor se producirá en el momento que se proceda a su publicación a través de la sede electrónica del Ayuntamiento de Cáceres y el Boletín Oficial de la Provincia.

3. INTRODUCCIÓN

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

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

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

Por tanto, para el Ayuntamiento de Cáceres, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 9 del ENS.

4. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Cáceres, que están relacionados con el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos, o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

Todos los empleados públicos y cargos del Ayuntamiento de Cáceres, así como el personal de terceros relacionados con éste, que se encuentren afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Cáceres en el alcance de esta Política, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, se recoge en el ANEXO I - MARCO NORMATIVO y deberá mantenerse actualizado, siendo responsabilidad del Comité de Seguridad de la Información del Ayuntamiento de Cáceres. En dicho Anexo se incluirán también las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN).

Así mismo, el Comité de Seguridad de la Información del Ayuntamiento de Cáceres también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Cáceres, derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

6. CUMPLIMIENTO DE PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE SEGURIDAD

El Ayuntamiento de Cáceres, para lograr el cumplimiento de los artículos del Real Decreto por el que se regula el Esquema Nacional de Seguridad, que recogen los principios básicosy de los requisitos mínimos, ha implementado diversas medidas de seguridad, proporcionadas 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 se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. 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.

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

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

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

El Ayuntamiento de Cáceres 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 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 deseguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.
Así mismo, 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 empleados del Ayuntamiento de Cáceres deberán recibir información, formación y concienciación en materia de seguridad. Se establecerá un programa de concienciación continua.
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.

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 cambien 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)
El Ayuntamiento de Cáceres implementará un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán 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, el Ayuntamiento de Cáceres implementará 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, los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Cuando se produzca 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.
El Ayuntamiento de Cáceres 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, el Ayuntamiento de Cáceres 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)
El Ayuntamiento de Cáceres 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(1). 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)
El Ayuntamiento de Cáceres organizará su seguridad comprometiendo a todas las personas integrantes de la organización, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 17)
El Ayuntamiento de Cáceres implementará mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 18)
El Ayuntamiento de Cáceres implementará 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)

1 Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 32 del anexo II, de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

El Ayuntamiento de Cáceres tendrá en cuenta, para la adquisición de productos que 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 riesgosasumidos 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)

El Ayuntamiento de Cáceres implementará mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta 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 desarrollarán procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias del Ayuntamiento de Cáceres. De igual modo, se implementarán mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren los documentos, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

Registro de actividad y detección de código dañino (artículo 24)

El Ayuntamiento de Cáceres habilitará 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 ENS, 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.

En concreto, el Ayuntamiento dispondrá de una solución integral de antivirus, tanto en puestos de trabajo como en servidores, que incorpore funcionalidades tanto de EPP (primera línea de defensa en los puestos del Ayuntamiento, basada en la prevención), como de EDR (complementa la protección de la solución EPP, detectando código dañino, incorporando mecanismos de respuesta así como medidas para revertir los daños) y de integración con los cortafuegos perimetrales, para bloqueo de funcionalidades en caso de detección de amenazas.

Mejora continua del proceso de seguridad (artículo 27)

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Ayuntamiento de Cáceres habilitará registros de la actividad de los usuarios, reteniendo la información necesaria para monitorización.

7. ORGANIZACIÓN DE LA SEGURIDAD

La Organización de la Seguridad de la Información en el Ayuntamiento de Cáceres se establece en la forma que se indica a continuación.

7.1 Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD): El así designado por el Ayuntamiento de Cáceres.
- Responsable de la Información: El Alcalde o Concejal Delegado.
- Responsable de los Servicios: La Secretaría General , apoyada por los Jefes o máximos responsables de cada una de las Unidades Administrativas y Servicios Municipales del Ayuntamiento de Cáceres en las materias que les conciernan.
- Responsable de Seguridad: El Jefe del Servicio de Desarrollo Tecnológico del Ayuntamiento de Cáceres.
- Responsable del Sistema: El Jefe de la Sección de Seguridad, Sistemas Informáticos y Telecomunicaciones del Ayuntamiento de Cáceres.
- Responsable Delegado del Sistema: El Técnico de Seguridad Informática y Telecomunicaciones del Ayuntamiento de Cáceres.

7.2 Comité de Seguridad de la Información

El Ayuntamiento de Cáceres constituye un Comité de Seguridad de la Información, como órgano colegiado y está formado por los siguientes miembros:

- Presidente: Alcalde/Concejal Delegado.
- Secretario: Designar entre los miembros del comité/decidir otra persona.
- Vocales:
  1. Responsable de los Servicios: El Secretario General o persona en quien pudiera delegar..
  2. Responsable de Seguridad. Jefe del Servicio de Desarrollo Tecnológico del Ayuntamiento de Cáceres.
  3. Responsable del Sistema. Jefe de Sección de Seguridad, Sistemas Informáticos y Telecomunicaciones del Ayuntamiento de Cáceres.
  4. El Delegado de Protección de Datos del Ayuntamiento de Cáceres, que será convocado cuando hayan de abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como cuando se juzgue oportuno. Participará en las sesiones con voz pero sin voto. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Ayuntamiento de Cáceres con periodicidad mínima semestral, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

7.3 Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad.

- Funciones del Responsable de la Información y de los Servicios:
  - ¬ Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, previa propuesta al Responsable de Seguridad, y/o Comité de Seguridad de la Información.
  - ¬ Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
  - ¬ Informar sobre los derechos de acceso al Servicio y a la Información.
  - ¬ Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.
- Funciones del Responsable de Seguridad:
  - ¬ Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
  - ¬ Promover la formación y concienciación en materia de seguridad de la información.
  - ¬ Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
  - ¬ Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
  - ¬ Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
  - ¬ Gestionar las revisiones externas o internas del sistema.
  - ¬ Gestionar los procesos de certificación.
  - ¬ Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Las funciones del Responsable del Sistema:
  - ¬ Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
  - ¬ Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
  - ¬ Elaborar los procedimientos operativos necesarios.

- ¬ Definir la topología y la 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.

- ¬ Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.

- ¬ Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

- ¬ Llevar a cabo las funciones del administrador de la seguridad del sistema:

    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

- Las funciones del Responsable Delegado del Sistema:
    - Hacerse cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funcionesconcretas de las responsabilidades que se le atribuyen.

7.4 Funciones del Delegado de Protección de Datos

Corresponde al Delegado de Protección de Datos del Ayuntamiento de Cáceres las funciones atribuidas a tal figura en el Reglamento UE 2016/679, de 27 de abril (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Tales funciones se ejercerán en los términos y condiciones y con el alcance señalados en la citada normativa.

7.5 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello, se encargará de:
  - ¬ Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - ¬ Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - ¬ Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
  - ¬ Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
  - ¬ Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - ¬ Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
  - ¬ Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
  - ¬ Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
  - ¬ Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y, en particular, en materia de protección de datos de carácter personal.
  - ¬ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.6 Procedimientos de designación

"El pleno de la Corporación es el órgano que aprueba la creación del comité de seguridad de la Información y habilita al Alcalde-Presidente para que proceda al nombramiento de sus integrantes y la designación de los Responsables identificados en la política de Seguridad".

Los miembros del Comité, así como los Roles de Seguridad, serán revisados cada cuatro años, o con ocasión de vacante.

7.7 Resolución de conflictos

El Comité de Seguridad de la Información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

8. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Cáceres solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del 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) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adoptando las medidas oportunas tales como la designación de un Delegado de Protección de Datos (Resolución de Alcaldía nº 2021/26975P de 20 de septiembre de 2021); la aprobación y publicación del Registro de Actividades de Tratamiento del Ayuntamiento (Decreto de Alcaldía Presidencia 2020000049, de 23-12-2020); el establecimiento y aplicación de los criterios del deber de información, diferenciando la información básica y la información detallada, con especificación de los diferentes ámbitos de actuación del Ayuntamiento; la definición del procedimiento para el ejercicio de los derechos de los ciudadanos en materia de protección de datos, con establecimiento de modelos tipo para facilitar dicho ejercicio; la definición y actualización de una política de privacidad adaptada a la normativa vigente en materia de protección de datos; el establecimiento de cláusulas tipo en materia de protección de datos en el ámbito de la contratación administrativa; el asesoramiento de las diferentes unidades, servicios y órganos municipales en materia de protección de datos, así como el impulso de la conciencia que sobre dicha materia debe tener la Administración.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información aprobará el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un

procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponderá al Comité de Seguridad de la Información la revisión anual de la presente Política aprobando, en caso de que sea necesario, mejoras de la misma.

10. TERCERAS PARTES

Cuando el Ayuntamiento de Cáceres preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. El Ayuntamiento de Cáceres, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que el Ayuntamiento de Cáceres, lleve a cabo en materia de Seguridad en relación con otros organismos.
Cuando el Ayuntamiento de Cáceres utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación 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 esta Política de Seguridad.
Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

ANEXO I.- NORMAS APLICABLES (MARCO NORMATIVO)

1. LEGISLACIÓN Y DISPOSICIONES QUE LA DESARROLLAN

El marco normativo aplicable está integrado por las siguientes normas:

- ¬ 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.
- ¬ Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- ¬ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ¬ 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 sederoga la Directiva 95/46/CE (Reglamento general de protección de datos).
- ¬ El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en lastransacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- ¬ Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- ¬ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- ¬ Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley)
- ¬ Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28de junio)
- ¬ Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- ¬ Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- ¬ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ¬ Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- ¬ Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- 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.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 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.
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.

2. INSTRUCCIONES TÉCNICAS OBLIGATORIAS

- 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 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 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.

3. Guías CCN-Cert

- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 470-2. PILAR – CONTINUIDAD MANUAL DE USUARIO V7.1.
- GUÍA DE SEGURIDAD (CCN-STIC-800) ESQUEMA NACIONAL DE SEGURIDAD GLOSARIO DE TÉRMINOS Y ABREVIATURAS.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 801 ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 802 ENS. GUÍA DE AUDITORÍA.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 803 ENS. VALORACIÓN DE LOS SISTEMAS.
- GUÍA DE SEGURIDAD (CCN-STIC-805) ESQUEMA NACIONAL DE SEGURIDAD POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 806 PLAN DE ADECUACIÓN AL ENS.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 811 INTERCONEXIÓN EN EL ENS.
- GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-812) SEGURIDAD EN ENTORNOS Y APLICACIONES WEB.
- GUÍA DE SEGURIDAD (CCN-STIC-815) ESQUEMA NACIONAL DE SEGURIDAD MÉTRICAS E INDICADORES.
- GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-820) GUÍA DE PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE I: NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA ENTIDAD NG00
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE II: NORMAS DE ACCESO A INTERNET NP10.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE III: NORMAS DE USO DEL CORREO ELECTRÓNICO (E-MAIL) NP20.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE IV: NORMAS PARA TRABAJAR FUERA DE LAS INSTALACIONES DE LA ENTIDAD NP30.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE V: NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS NP40.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE VI: ACUERDO DE CONFIDENCIALIDAD PARA TERCEROS NP50.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE VII: MODELO DE CONTENIDO DE BUENAS PRÁTICAS PARA TERCEROS NP60.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 APÉNDICE VIII: NORMATIVA DE USO DE REDES SOCIALES NP70.

- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 821 ESQUEMA NACIONAL DE SEGURIDAD NORMAS DE SEGURIDAD.
- GUÍA DE SEGURIDAD (CCN-STIC-822) ESQUEMA NACIONAL DE SEGURIDAD PROCEDIMIENTOS DE SEGURIDAD. ANEXOS I, II Y III.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 844 INES – INFORME NACIONAL DEL ESTADO DE LA SEGURIDAD MANUAL DE USUARIO.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-836 SEGURIDAD EN REDES PRIVADAS VIRTUALES (VPN).
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 819 MEDIDAS COMPENSATORIAS.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 831 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 845A LUCIA – MANUAL DE USUARIO.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 845C LUCIA – MANUAL INSTALACIÓN ORGANISMO.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 845D LUCIA – MANUAL DE ADMINISTRADOR.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 809 DECLARACIÓN, CERTIFICACIÓN Y APROBACIÓN PROVISIONAL DE CONFORMIDAD CON EL ENS Y DISTINTIVOS DE CUMPLIMIENTO.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 817 ESQUEMA NACIONAL DE SEGURIDAD. GESTIÓN DE CIBERINCIDENTES.
- GUÍA DE SEGURIDAD (CCN-STIC-818) HERRAMIENTAS DE SEGURIDAD EN EL ENS.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 824 INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS TIC.
- GUÍA DE SEGURIDAD (CCN-STIC-830) ÁMBITO DE APLICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD.
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC 835 ESQUEMA NACIONAL DE SEGURIDAD BORRADO DE METADATOS.
- GUÍA CCN-STIC-844 INES ANEXO II RECOPILACIÓN DE DATOS.

4. Otras guías

- GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES
- Guías de Magerit:
  - Libro I: Método
  - Libro II: Catálogo de Elementos
  - Libro III: Guía de Técnicas