PO.ENS-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

AYUNTAMIENTO DE CORDOBA

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	PO.ENS-01	DOCUMENTO:	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	Junio 2024

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
RESPONSABLE DE SEGURIDAD	COMITÉ DE SEGURIDAD TIC	JUNTA DE GOBIERNO LOCAL
FECHA:	FECHA:	FECHA:
Enero 2024	Abril 2024	Junio 2024

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	MODIFICACIONES:	ENTRADA EN VIGOR:

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☒	PUBLICABLE	☐	USO INTERNO	☐	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☒	IP A	☐	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

Ayuntamiento de Córdoba

Capitulares, 1
14071, Córdoba, Córdoba
ESPAÑA
https://cordoba.es

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta "Política de Seguridad de la Información", en adelante Política, ha sido aprobada por acuerdo de la Junta de Gobierno Local del Ayuntamiento de Córdoba y es efectiva desde la fecha del acuerdo y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El Ayuntamiento de Córdoba depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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 y delegaciones deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), 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 y delegaciones 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. Además, deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizándose la conservación de los datos e información, de acuerdo al artículo 8 del ENS.

2.1. PREVENCIÓN

Las áreas y delegaciones 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 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, se deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Las diferentes áreas y delegaciones deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras delegaciones 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).

2.4. CONSERVACIÓN

Para garantizar la disponibilidad de los servicios críticos y la conservación de los datos e informaciones en soporte electrónico, las áreas y delegaciones deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. MISIÓN

3.1. MISIÓN Y OBJETIVOS DEL AYUNTAMIENTO DE CÓRDOBA

El Ayuntamiento de Córdoba, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población del municipio de Córdoba, ejerciendo sus competencias en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Andalucía. Para ello, hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

3.2. MISIÓN Y OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Ayuntamiento de Córdoba ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, reconociendo así, como activos estratégicos, la información y los sistemas que la soportan.

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

Esta Política de Seguridad, formalizada como instrumento encaminado a la gestión y protección de los servicios que presta el Ayuntamiento de Córdoba, se sustenta en los principios básicos en materia de seguridad de la información:

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.
O. Mejora continua del proceso de seguridad.

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

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

- Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por el Ayuntamiento de Córdoba.
- Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
- Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
- Proteger los recursos de información del Ayuntamiento de Córdoba y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

4. ALCANCE

Esta Política se aplicará a todas las áreas y delegaciones del Ayuntamiento de Córdoba, a sus recursos y a los procesos afectados por el Real Decreto 311/2022 y la normativa en materia de protección de datos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Los Organismos Autónomos y Empresas Municipales dependientes del Ayuntamiento de Córdoba podrán adherirse a esta Política a través del procedimiento correspondiente.

Con esta Política de Seguridad de la Información, la organización muestra su compromiso por establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de acuerdo a los principios recogidos en el artículo 5 del Real Decreto 311/2022. Esto es:

- Entender la seguridad como un proceso integral.
- Gestionar la seguridad basándonos en los riesgos.

- Monitorizar y vigilar contínuamente los eventos de seguridad para garantizar la prevención, detección, respuesta y conservación.
- Establecer líneas de defensa.
- Vigilancia continua.
- Evaluar el estado de la seguridad periódicamente.
- Realizar una diferenciación clara de las responsabilidades.

5. MARCO NORMATIVO

El marco normativo que afectan al desarrollo de las actividades y competencias del Ayuntamiento de Córdoba y, en particular, a la prestación de sus servicios electrónicos está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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 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 se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).

También forman parte del marco normativo las restantes normas 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 carácter personal. Las normas que constituyen el marco normativo completo se encuentran recogidas en un registro al efecto, el cual se revisa y se mantiene actualizado.

Además, se deben tener en cuenta 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 Responsable de Seguridad asegurará que se han identificados las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en el Ayuntamiento de Córdoba se establece en

la forma que se indica a continuación.

6.1. ROLES DE SEGURIDAD

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente y siguiendo las premisas del ENS, el Ayuntamiento ha establecido los siguientes roles de seguridad:

- Responsable de la Información.
- Responsables del Servicio.
- Responsable de Seguridad.
- Responsable del Sistema.
- Administrador de Seguridad.

6.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Ayuntamiento de Córdoba ha constituido un Comité de Seguridad de la Información, denominado Comité de Seguridad TIC (CSTIC), como órgano colegiado, y está formado por los siguientes miembros:

- Presidencia: Coordinador/a General del Ayuntamiento.
- Secretario/a: Responsable de Seguridad.
- Vocales:
    - Titular del Órgano de Apoyo a la Junta de Gobierno Local.
    - Responsables de Tecnologías de la Información y la Comunicación.
    - Responsables de Gestión.
    - Responsables de Hacienda.
    - Responsables de Recursos Humanos.
    - Responsables de Contratación.
    - Responsable del Sistema.
    - Delegado/a de Protección de Datos.
    - Responsable de Transparencia.

En las reuniones del CSTIC podrán participar cuantos asesores, internos o externos, se estime conveniente por parte de la Presidencia del mismo. Asistirán los Responsables de la Información y los Servicios en los casos en que sean requeridos para ello.

En caso de vacante, ausencia o enfermedad y en general cuando concurra una causa justificada, los miembros del Comité podrán ser sustituidos por suplentes de tales órganos. Serán designados por el mismo procedimiento que los titulares a propuesta de los mismos. El Secretario/a del Comité tendrá voz y voto y ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.

El Comité se reunirá al menos una vez al año de forma presencial o telemática y se regirá por las

normas sobre los órganos colegiados que contiene la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

6.3. FUNCIONES DE LOS ROLES DE SEGURIDAD

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad.

6.3.1. Funciones del Responsable de la Información

- Establecer los requisitos, en materia de seguridad, de la información tratada.
- Determinar los niveles de seguridad de la información. Para ello, podrá recabar asesoramiento del Responsable de Seguridad y del Responsable del Sistema.
- Ser responsable último del uso que se haga de una cierta información y, por tanto, de su protección.
- Informar sobre el estado de la seguridad en el área de los sistemas de información y comunicación.
- Proporcionar la información necesaria al Responsable de Seguridad para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar.
- Verificar que los análisis de riesgos realizados se correspondan en todo momento con la información aportada para la realización de los mismos.

6.3.2. Funciones de los Responsables del Servicio

- Establecer los requisitos, en materia de seguridad, del servicio que le compete.
- Determinar los niveles de seguridad de dicho servicio. Para ello, podrá recabar asesoramiento del Responsable de Seguridad y del Responsable del Sistema.
- Incluir las especificaciones de seguridad en el ciclo de vida del servicio, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad del servicio que le compete, teniendo en consideración la repercusión en la capacidad del Ayuntamiento para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al Responsable de Seguridad del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.
- Proporcionar la información necesaria al Responsable de Seguridad para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar.
- Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

6.3.3. Funciones del Responsable de Seguridad

El Responsable de Seguridad es la persona designada por el máximo órgano de gobierno, según el procedimiento descrito en esta Política, para la supervisión de la seguridad de los sistemas de información. Será el encargado de determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los Responsables de la Información y de los Servicios.

Las dos funciones esenciales del Responsable de Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Entre las funciones que se le atribuyen al Responsable de Seguridad, se encuentran las siguientes:

- Coordinar y controlar las medidas definidas en el Registro de Actividades del Tratamiento y en general encargarse del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportar directamente al Comité de Seguridad de la Información.
- Actuar como Secretario del Comité de Seguridad de la Información.
- Recopilar los requisitos de seguridad de los Responsables de Información y Servicio y realizar la categorización del Sistema.
- Realizar el Análisis de Riesgos.
- Elaborar, o designar al responsable de elaborar, la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitar al Responsable de la Información y a los Responsables del Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinar la elaboración de la Documentación de Seguridad del Sistema.
- Participar en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por parte de los Órganos de Gobierno municipales.
- Participar en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborar, o designar al responsable de elaborar, los procedimientos operativos de Seguridad de la Información.
- Interpretar las dudas que puedan surgir en la aplicación de la normativa y los procedimientos.

- Facilitar periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a la seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborar, junto al Responsable del Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Analizar y proponer salvaguardas que prevengan incidentes similares en caso de que estos se hubieran producido.
- Elaborar, o designar al responsable de elaborar, los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Elaborar, o designar al responsable de elaborar, los Planes de Continuidad de Sistemas que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable del Sistema.
- Aprobar las directrices propuestas por el Responsable del Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Determinar la categoría de seguridad del sistema en función de la valoración del impacto que tendría un incidente de seguridad que afectase a la información o a los servicios.

El Responsable de Seguridad deberá ser distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios así lo requiriera, el Ayuntamiento podrá designar Responsables de Seguridad Delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables de Seguridad Delegados tendrán dependencia directa del Responsable de Seguridad.

En el caso de externalización del servicio de Responsable de Seguridad, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.

6.3.4. Funciones del Responsable del Sistema

El Responsable del Sistema se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una

responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. Sus funciones, de manera concreta, son las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- 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 con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de Seguridad antes de ser ejecutada.
- Asegurarse de que se aplican los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborar las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.
- Colaborar en el proceso de gestión y análisis de riesgos.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios requiriera personal adicional para el desempeño de estas funciones, el Ayuntamiento podrá designar Responsables del Sistema Delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables del Sistema Delegados tendrán dependencia directa del Responsable del Sistema.

6.3.5. Funciones del Administrador de Seguridad

Sus funciones más significativas serían las siguientes:

- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

- Aplicar los procedimientos operativos de seguridad.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- 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 Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

El Administrador de Seguridad dependerá del Responsable del Sistema. Esta figura será opcional en función de las necesidades de la entidad. En caso de ausencia, dichas funciones las asumirá el Responsable del Sistema.

6.3.6. Funciones del Delegado de Protección de Datos

Respecto al Comité de Seguridad TIC, velará y asesorará para proteger el cumplimiento de los derechos de los interesados en materia de protección de datos.

6.4. FUNCIONES DEL COMITÉ DE SEGURIDAD TIC

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Responsabilidades derivadas del tratamiento de datos personales.
- Atender las inquietudes de la Corporación y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información al órgano superior de gobierno.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución del Ayuntamiento de Córdoba 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 y están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por el propio Comité de Seguridad antes de su aprobación final por la Junta de Gobierno Local.
- Aprobar la normativa de seguridad de la información.

- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de 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 auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Aprobar 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.
- Establecer 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 aquellos casos en los que no tenga suficiente autoridad para decidir.
- En caso de ocurrencia de incidentes de seguridad de la información, aprobará el Plan de Mejora de la Seguridad.

6.5. GRUPO DE TRABAJO DE CARÁCTER PERMANENTE

El Comité de Seguridad TIC contará en su seno con un Grupo de Trabajo de Carácter Permanente a fin de agilizar los desarrollos del Comité que no requieran la presencia de todos los integrantes del mismo.

De manera no exhaustiva, sus funciones son de información a los diferentes órganos y áreas del Ayuntamiento, monitorización de la actividad de los sistemas, seguimiento de las actividades de control del sistema de seguridad de la información, determinación de la idoneidad de convocar sesiones extraordinarias, así como establecer protocolos de actuación frente a incidencias diarias o periódicas. Estará integrado, al menos, por los siguientes miembros:

- Responsable de Seguridad.

- Responsable del Sistema.
- Administrador de Seguridad.
- Delegado de protección de datos.

6.6. PROCEDIMIENTOS DE DESIGNACIÓN

La creación del Comité de Seguridad TIC, el nombramiento de sus integrantes y la designación de los diferentes Responsables debe ser realizada por la Junta de Gobierno Local del Ayuntamiento de Córdoba y comunicada a las partes afectadas.

El Comité de Seguridad TIC será el encargado de designar a los componentes que formarán parte del Grupo de Trabajo de Carácter Permanente. Dichos componentes serán revisados anualmente, sin perjuicio de que, cuando las circunstancias así lo requieran, puedan formar parte del mismo otras personas distintas a las descritas.

Los miembros del Comité, así como los roles de seguridad serán revisados cada dos años o con ocasión de vacante.

6.7. RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad TIC se encargará de la resolución de los conflictos o diferencias de opiniones que pudieran surgir entre los diferentes roles de seguridad.

7. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Córdoba sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos tengan 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.

Estas medidas, tal y como se indica en la disposición adicional primera de la Ley 3/2018 de 5 de diciembre, sobre Protección de Datos y Garantía de Derechos Digitales, se corresponderán con las descritas en el Esquema Nacional de Seguridad, quedando definidas en las políticas, normativas y procedimientos que correspondan.

8. ANÁLISIS Y GESTIÓN DE RIESGOS

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

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.

- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El análisis de riesgos que realice el Ayuntamiento de Córdoba atenderá, igualmente y de manera concreta, a aquellos que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

9.1. INSTRUMENTOS PARA EL DESARROLLO

La Política de Seguridad de la Información del Ayuntamiento de Córdoba se desarrollará, principalmente, por medio de los siguientes instrumentos:

- Normativa de seguridad: homogenizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio. También suelen denominarse 'políticas de seguridad'.
- Procedimientos operativos de seguridad: afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.

La normativa de seguridad deberá ser aprobada por el Comité de Seguridad TIC y estar a disposición de todos los miembros de la organización municipal que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

9.2. ESTRUCTURA GENERAL

El desarrollo de esta Política incluirá, basándose en el análisis de riesgos, aspectos específicos de la Seguridad de la Información tales como las medidas de seguridad indicadas en el Anexo II del Esquema Nacional de Seguridad (ENS), que quedan clasificadas de la siguiente forma:

- Marco organizativo: orientado a administrar la seguridad de la información dentro de la organización municipal y establecer un marco gerencial para controlar su implementación. Partiendo de la presente Política de Seguridad se desarrollará el resto del marco normativo de seguridad.
- Marco operacional: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

- Medidas de protección: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

9.3. GESTIÓN DE LA DOCUMENTACIÓN

El Comité de Seguridad de la Información ha desarrollado un sistema 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.

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS.

La información documentada será clasificada en: pública o publicable, interna, confidencial y secreta, dando el uso adecuado de acuerdo a dicha clasificación y según el criterio que se establezca en la normativa de clasificación de la información.

9.4. SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los preceptos incumplidos.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Córdoba tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normativas de seguridad, siendo responsabilidad del Responsable de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua dirigido a todos los miembros del Ayuntamiento.

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.

11. TERCERAS PARTES

Cuando el Ayuntamiento de Córdoba preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, definiendo 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 lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de Córdoba utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Además, 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.

En el caso específico de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria deberá designar un POC (Punto o Persona de Contacto) de Seguridad de la información, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información, así como la gestión de los incidentes para el ámbito del servicio que provea. Este POC de seguridad, será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en el Ayuntamiento.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Será preciso la aprobación de este informe por los Responsables de la Información y de los Servicios afectados, así como del responsable del tratamiento de datos.

12. REVISIÓN DE LA POLÍTICA

La Política de Seguridad de la Información deberá ser revisada anualmente y cuando haya cambios sustanciales en la organización municipal. Esta revisión es competencia del Comité de Seguridad TIC y la Política revisada deberá ser aprobada por parte de la Junta de Gobierno Local.

AYUNTAMIENTO DE CÓRDOBA

Hacienda electrónica local y provincial
DIPUTACIÓN DE MÁLAGA

DOCUMENTO ELECTRÓNICO

CÓDIGO DE VERIFICACIÓN DEL DOCUMENTO ELECTRÓNICO

1bddaedb7df81e3d297107e7afd2164a28ded66b

Dirección de verificación del documento: **https://sede.cordoba.es**

Hash del documento: 4fe23aec7eb63b5346ed192b92f8221952f56be12cc808e4a950108b756f7953ef551ab54b0844ac123de a3e2ded6aa72394c8637283514892e56cdf5343966f

METADATOS ENI DEL DOCUMENTO:

Version NTI: http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e

Identificador: ES_LA0016636_2024_00000000000000000000021019271

Órgano: L01140214

Fecha de captura: 05/06/2024 11:56:13

Origen: Administración

Estado elaboración: Otros

Formato: PDF

Tipo Documental: Otros

Tipo Firma: XAdES internally detached signature

Valor CSV: 1bddaedb7df81e3d297107e7afd2164a28ded66b

Regulación CSV: Decreto 3628/2017 de 20-12-2017

Código QR para validación en sede

Código EAN-128 para validación en sede

Ordenanza reguladora del uso de medios electrónicos en el ámbito de la Diputación Provincial de Málaga:
https://sede.malaga.es/normativa/ordenanza_reguladora_uso_medios_electronicos.pdf

Política de firma electrónica y de certificados de la Diputación Provincial de Málaga y del marco preferencial para el sector público provincial (texto consolidado):
https://sede.malaga.es/normativa/politica_de_firma_1.0.pdf

Procedimiento de creación y utilización del sello electrónico de órgano de la Hacienda Electrónica Provincial:
https://sede.malaga.es/normativa/procedimiento_creacion_utilizacion_sello_electronico.pdf

Acuerdo de adhesión de la Excma. Diputación Provincial de Málaga al convenio de colaboración entre la Administración General del Estado (MINHAP) y la Comunidad Autónoma de Andalucía para la prestación mutua de soluciones básicas de Administración Electrónica de fecha 11 de mayo de 2016:
https://sede.malaga.es/normativa/ae_convenio_j_andalucia_MINHAP_soluciones_basicas.pdf

Aplicación del sistema de Código Seguro de Verificación (CSV) en el ámbito de la Diputación Provincial de Málaga:
https://sede.malaga.es/normativa/decreto_CSV.pdf