SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SGSI.PSI-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Diputación de Córdoba

• Diputación Provincial de Córdoba • Instituto Provincial de Bienestar Social • Instituto Provincial de Cooperación con la Hacienda Local • Instituto Provincial de Desarrollo Económico • Consorcio Provincial de Extinción de Incendios • Patronato Provincial de Turismo de Córdoba • Agencia Provincial de la Energía • Fundación Provincial de Artes Plásticas Rafael Botí • Empresa Provincial de Aguas de Córdoba • Empresa Provincial de Residuos y Medio Ambiente • Empresa Provincial de Informática	**DIPUTACIÓN PROVINCIAL DE CÓRDOBA Y SU SECTOR PÚBLICO INSTITUCIONAL**

ÍNDICE

1. OBJETO

Los ciudadanos confían en que los servicios disponibles por medios electrónicos se presten en unas condiciones de seguridad equivalentes a las que se encuentran cuando se acercan personalmente a las oficinas de la Administración. Además, buena parte de la información contenida en los sistemas de información de las AA.PP. y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

Por lo anteriormente expuesto la Excelentísima Diputación Provincial de Córdoba, el Instituto Provincial de Bienestar Social, el Instituto Provincial de Cooperación con la Hacienda Local, el Instituto Provincial de Desarrollo Económico, el Consorcio Provincial de Extinción de Incendios, el Patronato Provincial de Turismo de Córdoba, la Agencia Provincial de la Energía, la Fundación Provincial de Artes Plásticas Rafael Botí, la Empresa Provincial de Aguas de Córdoba, la Empresa Provincial de Residuos y Medio Ambiente y la Empresa Provincial de Informática (en adelante la Diputación de Córdoba y su Sector Público Institucional)

Aprueba la siguiente Política de Seguridad y debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante, ENS), regulado en el Real Decreto 3/2010, de 8 de Enero, 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. Para que conste el compromiso de Diputación de Córdoba y su Sector Público Institucional hacen pública su visión, misión y valores en materia de seguridad de la información.

Para que todo el personal y usuarios sean conscientes de las obligaciones, normativas y procedimientos en materia de seguridad de la información, esta política y la normativa de seguridad estará a disposición de todos los usuarios autorizados en el portal del empleado o en la intranet corporativa.

Visión:

Las diferentes áreas y servicios deben cerciorarse de que la seguridad de la información es una parte vital de los servicios públicos prestados por Diputación de Córdoba y su Sector Público Institucional.

Misión:

Diputación de Córdoba y su Sector Público Institucional ha de custodiar y tratar dicha información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción) poniendo la seguridad de la información como base.

Valores:

Las áreas y servicios de Diputación de Córdoba y su Sector Público Institucional deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando así la continuidad en la prestación de los servicios con una calidad y seguridad adecuada.

2. ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios, empleados internos y externos Diputación de Córdoba y su Sector Público Institucional, cualquiera que sea su clasificación jerárquica. Igualmente, aplica a todos los sistemas de la información e infraestructuras de comunicación utilizadas para la realización de las funciones propias de las distintas entidades.

3. MARCO NORMATIVO

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece principios y derechos relativos a la seguridad en relación con el derecho de los ciudadanos a comunicarse con las AA.PP. a través de medios electrónicos; y su artículo 42 crea el Esquema Nacional de Seguridad. Aún estando derogada establece los principios de la seguridad de la información en la administración electrónica.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. Las normas técnicas complementarias de interoperabilidad desarrollan ciertos aspectos técnicos.

Las Leyes 39/2015 y 40/2015 regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

Así mismo, la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos y garantía de los derechos digitales, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, además de

garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Reglamento (EU) 679/2016, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos establece en la obligación de disponer medidas técnicas y organizativas para garantizar la confidencialidad, disponibilidad e integridad de la información. Así mismo dispone que dichas medidas han de ser proactivas y el responsable del tratamiento ha de ser capaz de demostrar que se siguen esas medidas y demostrar su aplicación.

4. ORGANIZACIÓN DE SEGURIDAD.

Para gestionar y coordinar proactivamente la seguridad de la información se constituye como órgano de gestión el Comité de Seguridad de la Información.

El Comité estará constituido por los siguientes cargos:

Responsable de la información: que tendrá potestad de aprobar los requisitos de una información en materia de seguridad y tendrá capacidad ejecutiva para aprobar, planificar y trasladar estas necesidades al Pleno de Diputación de Córdoba y extensivo a sus sector público institucional. Podrá convocar las reuniones del Comité. Será responsable directo de la ejecución de las medidas adoptadas por el comité y su seguimiento.

Responsable de Seguridad: asesorará y tendrá potestad para determinar técnicamente los requisitos de seguridad de la información y de los servicios en materia de seguridad. Así mismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros del comité.

Administrador de los sistemas de la información: será miembro de este comité. Tendrán la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar coordinadamente al **Responsable de la Información** del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad y de la seguridad de los sistemas de la información.

Responsables de Entidades del Sector Público Institucional: serán las personas responsables de los servicios o de la explotación de las distintas instituciones que establecen los requisitos, fines y medios para la realización de las tareas en las distintas instituciones. Además, tendrán la responsabilidad legal de vigilar el cumplimiento de las normas de seguridad dentro de su institución e informar al **Responsable de la Información** del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

En caso de vacante o ausencia de los Responsables de entidades del Sector Público Institucional deberá asistir a las sesiones del Comité la persona que ejerza las funciones de dirección o gerencia de la entidad correspondiente.

Representante de la Diputación Provincial: Será la persona que representará a los distintos servicios de la entidad, y coordinará y gestionará la información de la institución.

Secretaría: tendrá la obligación de supervisar que los procedimientos aprobados por el comité se ajusten a derecho y asesorar al comité en esta materia. Además, levantará acta de las reuniones.

Delegado de Protección de Datos: Ejercerá las siguientes funciones y competencias:

1) Informar y asesorar a los miembros del Comité en la materia de protección de datos.
2) Supervisar el cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas aprobadas por el mismo Comité en la actividad del mismo.
3) Participar con voz pero sin voto en las reuniones del Comité de seguridad de la información, señalando que si un asunto se sometiera a votación se hará constar siempre en acta su parecer.

Los miembros de este comité serán nombrados por decreto de Presidencia una vez aprobado en pleno este documento, contemplando medidas transitorias con objeto de garantizar el cumplimiento de la seguridad. Además, las futuras resoluciones de nombramientos de responsables de áreas, responsables de entidades vinculadas o cambios en la distribución de funciones de área y entidades deberán contemplar expresamente el nombramiento como miembro en este comité de seguridad de la información.

4.1 FUNCIONES DEL COMITÉ DE SEGURIDAD

Sus funciones son las siguientes:

- Responsabilidades derivadas del tratamiento de datos de carácter personal.
- Atender las inquietudes de la Corporación y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información a la Junta de Gobierno.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de Diputación de Córdoba y su Sector Público Institucional en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Comité de Seguridad.
- 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 la empresa 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 las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la empresa. 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 empresa, 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.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.

- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

4.2 GRUPO DE TRABAJO DE CARÁCTER PERMANENTE.

El Comité 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, monitorización de la actividad de las organizaciones, en especial de la Diputación de Córdoba y EPRINSA, determinación de la idoneidad de convocar sesiones extraordinarias, así como establecer el orden del día de las sesiones. Estará integrado por los siguientes miembros:

- Responsable de la información
- Responsable de Seguridad
- Administrador de los sistemas de la información
- Representante de la Diputación Provincial
- Secretario
- Delegado de protección de datos

5. CONCIENCIACIÓN

Diputación de Córdoba y su Sector Público Institucional establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo a esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad.

El Comité establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

6. GESTIÓN DEL RIESGO

Diputación de Córdoba y su Sector Público Institucional realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgo, siguiendo las directrices expuestas por el ENS en su artículo 6, de modo que se puedan anticipar los riesgos existentes. Este análisis de riesgo y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el comité desarrollará un procedimiento de Análisis de Riesgos y Evaluación de Impacto Potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad del análisis y cuándo se realizará de modo excepcional.

7. REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso de Diputación de Córdoba y su Sector Público Institucional con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad para adaptarse a cambios en el entorno legislativo, técnico u organizativo.