

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SGSI.PSI-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

 Diputación de Córdoba	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO SGSI.PSI-01 REVISIÓN Nº5
			PÁGINA 2 de 17

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	SGSI.PSI-01	DOCUMENTO:	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
---------	-------------	------------	--------------------------------------------

REVISIÓN NÚMERO:	5.0	FECHA DE ENTRADA EN VIGOR:	Noviembre 2023
------------------	-----	----------------------------	----------------

ES ORIGINAL:	<input checked="" type="checkbox"/>	ES COPIA CONTROLADA:	<input type="checkbox"/>	ES COPIA NO CONTROLADA:	<input type="checkbox"/>
--------------	-------------------------------------	----------------------	--------------------------	-------------------------	--------------------------

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
Responsable de Seguridad y DPD	Comité de Seguridad	Pleno de la Diputación

CONTROL DE CAMBIOS:

REVISIÓN N°:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:
1	nov-2022	1.Objeto	Adaptación al art.12 del nuevo ENS-desglose de los requisitos mínimos sobre los que se sustenta.	noviembre 2023
2	nov-2022	2. Alcance	Se detalla el compromiso de la organización 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. Inclusión de la aplicación de todas las Dimensiones de seguridad .Se elimina la referencia específica a la Visión, Misión y Valores unificando su redacción.se incluyen también las Dimensiones de Seguridad que dispone el RD 311/22 de 3 de mayo que regula el ENS.	noviembre 2023
3	nov-2022	3. Marco Organizativo	Inclusión nueva normativa	noviembre 2023
4	nov-2022	4.Organización de seguridad	Eliminación de la figura del Secretario General de la Corporación y su suplente, dejando de ser éstos miembros del Comité, según Decreto de la Presidencia de 8/3/2021. Inserción de la figura del Secretario/a del Comité cuyo rol asume el Responsable de Seguridad. Responsable del Sistema (antiguo Administrador de los Sistemas de la Información). Inclusión de la figura de Responsable del área de Presidencia	noviembre 2023

			<p>Revisión de los miembros del Comité y resolución de conflictos conforme a la Guía 883 del CCN.</p> <p>Incluir entre las funciones del Comité de Seguridad el ser informado sobre los procedimientos de Seguridad de la información de los integrantes del sector público institucional los cuales tienen obligación de tener.</p>	
5	nov-2022	5. Desarrollo de la Política de Seguridad de la Información	Con este apartado se solventó la No conformidad menor 4 del año 2019 y se le adapta la redacción conforme a las modificaciones de la Guía 883 del CCN. Inclusión de la obligación de cumplimiento por parte de todo el personal y servicios/unidades de colaborar en la implementación de la Política de Seguridad de la Información en la organización.	noviembre 2023
6	nov-2022	6. Concienciación	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 seguridad como en materia de privacidad	noviembre 2023
7	nov-2022	7. Competencia para la aprobación de las políticas, normas y procedimientos de Seguridad.	Determinar la competencia para la aprobación de las políticas, normas y procedimientos de Seguridad	noviembre 2023
8	nov-2022	7. Protección de Datos personales	Referencia a la misma en la política que no se encontraba anteriormente	noviembre 2023
9	nov-2022	8. Gestión del Riesgo	Incluye que el análisis de riesgos que se realice atenderá a también a los que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.	noviembre 2023
10	nov-2022	9. Terceras partes	Se incluye según indica la Guía 883 del CCN, participación de la Política de Seguridad y Normativa de Seguridad a otras terceras entidades	noviembre 2023
11	nov-2022	10 Revisión de esta Política de Seguridad	Se añade la competencia del Comité de la revisión anual de esta Política y su aprobación por el mismo.	noviembre 2023

DOCUMENTACIÓN OBSOLETA:	<input type="checkbox"/>	FECHA:	
-------------------------	--------------------------	--------	--

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	<input type="checkbox"/>	PUBLICABLE	<input type="checkbox"/>	USO INTERNO	<input checked="" type="checkbox"/>	CONFIDENCIAL:	<input type="checkbox"/>	SECRETA:	<input type="checkbox"/>
----------	--------------------------	------------	--------------------------	-------------	-------------------------------------	---------------	--------------------------	----------	--------------------------

PRIVACIDAD

NO IP	<input type="checkbox"/>	IP A	<input checked="" type="checkbox"/>	IP B	<input type="checkbox"/>	IP C	<input type="checkbox"/>
-------	--------------------------	------	-------------------------------------	------	--------------------------	------	--------------------------

Confidencialidad Acerca de este documento

AVISO: Este documento está protegido por la legislación referente a propiedad intelectual e industrial y por tratados internacionales. La utilización permitida de esta documentación queda limitada exclusivamente en relación con la Diputación de Córdoba, y todo uso no autorizado será perseguido de acuerdo con la legislación aplicable. Se prohíbe su copia, modificación, reproducción o distribución sin permiso del titular.

Diputación de Córdoba

Plaza Colón , 15
14001 Córdoba, Córdoba
ESPAÑA
<https://www.dipucordoba.es>

- 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
- Grupo Cinco Suelo Industrial

**DIPUTACIÓN PROVINCIAL DE
CÓRDOBA Y SU SECTOR PÚBLICO
INSTITUCIONAL**

ÍNDICE

1. OBJETO	4
2. ALCANCE	5
3. MARCO REGULATORIO EN QUE SE DESARROLLAN LAS ACTIVIDADES	6
4. ORGANIZACIÓN DE SEGURIDAD.	8
4.1 FUNCIONES DEL Comité de Seguridad	10
4.2 GRUPO DE TRABAJO DE CARÁCTER PERMANENTE.	11
5. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	12
6. CONCIENCIACIÓN	12
7. PROTECCIÓN DE DATOS PERSONALES	12
8. GESTIÓN DEL RIESGO	13
9. TERCERAS PARTES	13
10. REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD	14

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.

En su empeño por garantizar que estos servicios cuenten con las máximas garantías en materia de seguridad, la Diputación Provincial de Córdoba desarrolla esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por el ENS en lo referente a:

- 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.

Por todo 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, la Empresa Provincial de Informática y Grupo Cinco Suelo Industrial (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 311/2022, de 3 de mayo, 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.

 Diputación de Córdoba	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.PSI-01 REVISIÓN Nº5	
		PÁGINA	8 de 17

Para que conste el compromiso de la 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 todo el personal en el portal del empleado y/o en la intranet corporativa y para los/as usuarios/as en la web de la entidad.

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.

La 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 atendiendo a los principios básicos que rige el Esquema Nacional de Seguridad.

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.

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 continuamente los eventos de seguridad para garantizar la prevención, detección, respuesta y conservación.
- Establecer líneas de defensas
- Reevaluar el estado de la seguridad periódicamente
- Realizar una diferenciación clara de las responsabilidades.

Además, a fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la

 Diputación de Córdoba	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.PSI-01 REVISIÓN Nº5	
		PÁGINA	9 de 17

categoría del sistema, se tendrán en cuenta las dimensiones de la seguridad , tal y como lo indica el Real Decreto 311/2022 de 3 de mayo, que regula el Esquema Nacional de Seguridad:

- **Disponibilidad [D]:** La disponibilidad de la información se refiere a que se encuentre accesible cuando se necesite.
- **Autenticidad [A]:** Se refiere a que la información provenga de una fuente fidedigna.
- **Integridad [I]:** Asegurando que la información sea correcta y esté libre de modificaciones y errores.
- **Confidencialidad [C]:** La información es accesible únicamente por personal autorizado. «need-to-know»|solo es del conocimiento de usuarios con acceso. De esta manera, garantiza la no divulgación sin consentimiento y aprobación previa.
- **Trazabilidad [T]:** La información se puede rastrear desde su origen, camino y destino. Importantísima en la gestión de la calidad y la seguridad en los procesos.

3. MARCO REGULATORIO EN QUE SE DESARROLLAN LAS ACTIVIDADES

La base normativa que afecta al desarrollo de las actividades y competencias de la Excm. Diputación Provincial de Córdoba, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está regulada, principalmente, por la siguiente legislación:

- 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 inicialmente por el Real Decreto 3/2010, de 8 de enero y posteriormente por su actualización por Real Decreto 311/2022 de 3 de mayo 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.
- La Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen (LRBRL) de aplicación a la administración local.
- La Ley 5/2010, de 11 de junio, de autonomía local de Andalucía (LAULA).
- 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.
- La Ley de Seguridad de las Redes y Sistemas de la Información aprobada mediante Real Decreto-Ley 12/2018, de 7 de septiembre, que transpone al ordenamiento jurídico español la directiva europea sobre la materia, la conocida como Directiva NIS que establece un marco común de seguridad en la Red en toda la UE y refuerza las medidas de protección en el entorno virtual. Afecta, por un lado, a los operadores de servicios esenciales; es decir, aquellos necesarios «para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas, que dependan para su provisión de redes y sistemas de información», según la definición que recoge la propia norma; y por extensión, las infraestructuras críticas también verán incrementada su seguridad de la información. Establece la obligación de que las empresas notifiquen los incidentes de ciberseguridad. Los operadores de servicios esenciales tendrán que designar a una persona como responsable de la seguridad de la información para que ejerza las funciones de punto de contacto y coordinación con las autoridades competentes y CSIRT (equipos de respuesta a incidentes de seguridad) de referencia.
- El Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Tiene como finalidad desarrollar la Directiva NIS, aprobada en 2018, en cuanto al marco

institucional en la materia, la cooperación y coordinación, la gestión y notificación de incidentes, las medidas a implementar, la supervisión de los requisitos de ciberseguridad o la función del CISO.

También forman parte del marco normativo las restantes normas estatales y autonómicas orientadas a la Administración Electrónica de la Diputación Provincial de Córdoba, a la seguridad de la información y los servicios que ésta maneja, así como a la protección de datos de carácter personal.

El mantenimiento de todo este marco normativo será responsabilidad del Responsable de Seguridad y se mantendrá de forma Anexa en los medios y/o soportes que determine el Comité de Seguridad.

También se incluirán 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 la Seguridad asegurará que se han identificado las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

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 su 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. Asumirá las funciones de secretario del Comité de Seguridad de conformidad con la Guía CCN 801 sobre atribución de responsabilidades y funciones.
- **Responsable del área de Presidencia:** será la persona responsable del Servicio de Presidencia de la Diputación o unidad asimilada. Representa administrativamente a la Presidencia, con quien llevará a cabo las labores de coordinación y gestión necesarias.
- **Responsable del Sistema (antiguo 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 procedente de los mismos.
- **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.

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

Resolución de conflictos

El Comité de Seguridad de la Información, se encargará de resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización. En caso de que el Comité no tuviera capacidad o autoridad para la resolución de determinados conflictos, lo elevará a Presidencia para su resolución.

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 la 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.
- Ser informado sobre los procedimientos de Seguridad de la información de los integrantes del sector público institucional los cuales tienen obligación de tener.
- 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 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 .
- 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
- Responsable del Sistema (antiguo Administrador de los Sistemas de la Información)
- Representante de la Diputación Provincial
- Responsable de Presidencia.
- Delegado de Protección de Datos

5.DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado 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.

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en la entidad (empleados, proveedores y subcontratistas), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS. Esta documentación estará permanentemente accesible a través de los medios que la Diputación Provincial de Córdoba estime convenientes.

6. CONCIENCIACIÓN

La 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 seguridad como 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.

7. COMPETENCIA PARA LA APROBACIÓN DE LAS POLÍTICAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD.

La competencia para la aprobación de las políticas, normas y procedimientos de Seguridad se estructuraría de la siguiente forma :

- Política de Seguridad de la Información y Política de Protección de Datos: serían aprobadas por el Pleno de la Diputación de Córdoba.
- Normativa de Seguridad de la Información: Tanto la Diputación como todo el Sector Público Institucional propondrá su propia Normativa de Seguridad (ratificada por su presidente/órgano rector) y esta será luego aprobada/ratificada por el Comité de Seguridad en la siguiente reunión del mismo.
- Procedimientos de Seguridad de la Información: Tanto la Diputación como todo el Sector Público Institucional aprobará sus propios procedimientos de Seguridad de la información (aprobados por el responsable de la entidad) e informará de su aprobación al Comité de Seguridad en la siguiente reunión del mismo.

Toda esta documentación deberá ser publicada en cada uno de los portales de información de cada entidad para general conocimiento de todo el personal.

8. PROTECCIÓN DE DATOS PERSONALES

La Diputación Provincial de Córdoba únicamente recogerá datos personales 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 técnicas y organizativas pertinentes para el cumplimiento de la legislación en materia de protección de datos.

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, que estarán definidas en las políticas, normativas y procedimientos que correspondan.

9. GESTIÓN DEL RIESGO

La 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.

El análisis de riesgos que realice la Diputación Provincial 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.

10. TERCERAS PARTES

Cuando la Diputación de Córdoba y su Sector Público Institucional preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación de Córdoba y su Sector Público Institucional 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 atañe 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 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.

11.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.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del órgano competente.