
# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

# Índice

# 1 Aprobación y Entrada en Vigor

Texto aprobado el día 31 de enero de 2019 por Resolución dictada por el Presidente.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

# 2 Introducción

La Diputación de Jaén 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 la Diputación de Jaén y todo su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La Diputación de Jaén debe 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.

La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

## 2.1 Prevención

La Diputación de Jaén debe 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 implementará 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Diputación de Jaén debe:

- 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, los servicios deben 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 produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

## 2.3 Respuesta

La Diputación de Jaén:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece 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 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Diputación de Jaén ha desarrollado planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y

actividades de recuperación.

# 3 Alcance

Esta política de seguridad será de obligado cumplimiento para todos los miembros de la Diputación de Jaén, siendo aplicable a todos los activos empleados por el mismo en la prestación de los servicios a los ciudadanos, a otras administraciones así como para su propia gestión y funcionamiento.

# 4 Misión

La Diputación garantiza los principios de solidaridad y equilibrio intermunicipal y asegura la prestación integral y adecuada de los servicios de competencia municipal, es decir, garantiza que en todos y cada uno de nuestros municipios, con independencia de su tamaño, los ciudadanos y ciudadanas contemos con igualdad en el acceso a servicios, equipamientos e infraestructuras de calidad. Este es el cometido que le reserva la normativa básica local del Estado y que recoge el Estatuto de Autonomía de Andalucía.

Para lograr este fin, la Diputación Provincial de Jaén presta asistencia y cooperación jurídica, económica y técnica a los municipios especialmente a los de menor capacidad económica y de gestión, coopera y coordina los servicios municipales y presta servicios públicos de carácter supramunicipal procurando que la unión entre los municipios, especialmente a través de la fórmula de los consorcios, logre una gestión de calidad, eficiente y generadora de economías de escala.

La Diputación Provincial de Jaén trabaja desde un modelo plural y participativo de colaboración con los Ayuntamientos que trata de dotar a las ciudadanas y ciudadanos de igualdad de capacidades y oportunidades para su desarrollo, a través de unas políticas locales activas de mejora socioeconómica, bienestar social y conocimiento que toman como parámetros de referencia el equilibrio territorial y el crecimiento desde el desarrollo sostenible.

Actuaciones y servicios desarrollados por la administración local, en colaboración con los Ayuntamientos, desde la eficiencia y la calidad, tratando de alcanzar los objetivos planteados desde una gestión adecuada de los recursos económicos, ampliando la cobertura de nuestras actuaciones, primando la calidad en la prestación de servicios y en los procedimientos, haciéndolos transparentes y eficaces, en un proceso de mejora continua en el que se encuentran implicados los recursos humanos de la organización.

# 5 Marco normativo

El marco normativo en materia de seguridad de la información en el que la Diputación de Jaén desarrolla su actividad, esencialmente, es el siguiente:

- 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 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

# 6 Organización de la Seguridad

La implantación de la Política de Seguridad en la Diputación de Jaén requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsable del Servicio

c) Responsable de la Información

d) Responsable de Seguridad de la Información

e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

## 6.1 Comité de seguridad de la información

La Seguridad de la Información es una responsabilidad organizativa que es compartida con el Presidente. En consecuencia, este promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vía definida y el palpable apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas y por un Presidente que será responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones..

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Presidente
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dicho activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.

- Elaboración y actualización de planes de continuidad.
- Cumplimiento y difusión de las Políticas de Seguridad.

El Secretario del Comité de Seguridad TIC será el Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable del impulso de la ejecución directa o delegada de las decisiones del Comité.

## 6.2 Responsable de la Información

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

## 6.3 Responsable del Servicio

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio.

## 6.4 Delegado de Protección de Datos

De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento

## 6.5 Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Asistencia al Presidente del Comité de Seguridad en la elaboración del orden del día de las sesiones a celebrar.

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de la Diputación de Jaén.

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:

    - La estrategia de seguridad de la información definida por el Comité de Seguridad.

    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de la Diputación de Jaén y normativa de desarrollo.

- Supervisar los incidentes de seguridad producidos en la Diputación de Jaén.

- Difundir en la Diputación de Jaén las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.

- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.

- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de la Diputación de Jaén.

## 6.6 Responsable del Sistema

Es responsable de asegurar la ejecución de medidas para asegurar los activos y servicios de los sistemas de información, que soportan la actividad de la Diputación de Jaén, de acuerdo a los objetivos de la organización.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de la Diputación de Jaén, conforme a la estrategia de seguridad definida.

- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en la Diputación de Jaén.

- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

# 7 Procedimientos de designación

Se designan las siguientes responsabilidades:

- La Secretaría General que actuará como Responsable de Seguridad.
- El Director ó Directores del Área responsable en materia de Administración Electrónica y Recursos Humanos que actuará como Responsable del Sistema.
- El Gerente del Instituto de Estudios Giennenses que actuará como Responsable de la Información.
- Los Directores de cada Área y gerentes de Organismos Autónomos que actuarán como Responsables del Servicio.

Los nombramientos se revisarán cuando alguno de los puestos quede vacante, correspondiendo los nombramientos y ceses al Presidente de la Diputación mediante resolución.

# 8 Revisión de la Política de Seguridad de la Información

Será misión del Comité de Seguridad TIC la revisión bienal de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de la misma. La Política será aprobada por el Presidente de la Diputación y difundida para que la conozcan todas las partes afectadas.

# 9 Datos de Carácter Personal

La Diputación de Jaén trata datos de carácter personal.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

# 10 Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos cada dos años.
- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

# 11 Desarrollo de la política de seguridad de la información

Esta política de seguridad de la Información complementa las políticas de seguridad de la Diputación de Jaén en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

# 12 Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de la Diputación de Jaén son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los empleados de la Diputación de Jaén tienen la obligación de conocer y cumplir esta política de seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los empleados de la Diputación de Jaén recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Diputación de Jaén, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

# 13 Terceras partes

Cuando la Diputación de Jaén preste servicios a otros organismos o manejen información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación de Jaén utilice servicios de terceros o cedan información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política 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.