Ayuntamiento de Lucena

# DECRETO

El 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 tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y en él se contienen los principios básicos y requisitos mínimos a fin de garantizar una protección adecuada de la información. Se hace así realidad el mandato del art. 42 de la derogada Ley Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, hoy recogido en el art. 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Dichas medidas de seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, persiguen la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos para permitir a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad (ENS) es de aplicación a las entidades que conforman las Administraciones Públicas y a los organismos públicos y entidades de derecho público vinculadas o dependientes de las mismas; y en cuanto a las entidades de derecho privado dependientes o vinculadas, se aplicará cuando ejerzan potestades administrativas atribuidas estatutariamente y en las materias en que les sea de aplicación la normativa presupuestaria, contable, de control financiero, de control de eficacia y contratación.

Conforme al art. 11 de la norma, todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de una política de seguridad que articule la gestión continuada de la misma y que será aprobada por el titular del órgano superior correspondiente. A fin de cumplir estas obligaciones y de acuerdo a los principios básicos y requisitos mínimos legalmente exigidos, la Diputación Provincial de Córdoba, a través de la Empresa Provincial de Informática S.A. (EPRINSA), ha remitido a este Ayuntamiento un modelo de Política de Seguridad de la Información, que ha sido informado por el Jefe de Sección de Informática y Telecomunicaciones de este Ayuntamiento, con fecha 10-06-2021, en los siguientes términos:

*"En relación a la solicitud de informe sobre la propuesta de Política de Seguridad de la Información remitida por la Diputación Provincial de Córdoba el funcionario abajo firmante Jaime Fernández Martínez, Ingeniero Informático con puesto de Jefe de Sección de Informática y Telecomunicaciones de este Excmo. Ayuntamiento según su saber y entender emite el presente*

*INFORME*

*Antecedentes.*

*1. Legislación a aplicar*

*La transformación digital del Sector Público ha de ir acompañada de medidas organizativas y técnicas de seguridad que protejan la información manejada y los servicios prestados, proporcionadas a los riesgos provenientes de acciones malintencionadas o ilícitas, particularmente de las ciberamenazas, errores o fallos y accidentes o desastres.*

*La **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** recoge entre los derechos de las personas en sus relaciones con las Administraciones Públicas, establecidos en su artículo 13, el relativo "a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas". A la vez que la seguridad figura entre los principios de actuación de las administraciones públicas, así como la garantía de la protección de los datos personales, según lo*

*establecido en la **Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público** en su artículo 3 que trata los principios generales relativos a las relaciones de las administraciones por medios electrónicos.*
*Para dar respuesta a todo lo anterior, el artículo 156 de la Ley 40/2015 recoge **el Esquema Nacional de Seguridad (ENS)** que "tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".*
*El ENS fue establecido anteriormente por el artículo 42 de la Ley 11/2007 y está regulado por el Real Decreto 3/2010, de 8 de enero.*

## *2. Guías y documentos a considerar.*

*Para cumplir con las obligaciones legales derivadas del ENS y la legislación en materia de Protección de Datos de carácter personal, los ayuntamientos deben contar con una **Política de Seguridad de la Información** que refleje "declaración de las reglas que se deben respetar para acceder a la información y a los recursos dentro de una entidad".*
*Para orientar en la confección de la política el CCN-CERT publica las guías CCN-STIC de la serie 800. En este caso, las guías a tener en cuenta son la CCN-STIC-801 «Esquema Nacional de Seguridad – Responsabilidades y funciones» y CCN-STIC-805 «Esquema Nacional de Seguridad de la Información».*
*A su vez, la FEMP publicó una «Guía estratégica en seguridad para entidades Locales – ENS» para facilitar la adopción del ENS a las entidades locales y, en particular a los ayuntamientos.*

## *3. El papel de la Diputación Provincial de Córdoba.*

*El ENS en el párrrafo segundo del artículo 3.2. señala que «Los municipios podrán disponer de una política de seguridad común elaborada por Diputación (…) correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia».*
*En este sentido tiene especial sentido señalar la existencia del Convenio de Cooperación entre la Diputación Provincial de Córdoba y este Ayuntamiento en materia de gestión tributaria y recaudación, asesoramiento económico y asistencia informática celebrado el 8 de noviembre de 2018.*
*Sin embargo, a pesar del borrador de política de seguridad de la información remitido por EPRINSA la Diputación Provincial de Córdoba no ha previsto que su política de seguridad de la información, ni el comité de seguridad de la información tenga aplicación en los municipios de la provincia: solamente en la propia diputación y en su sector público institucional.*

## *Principios que deben inspirar la política de seguridad de la información.*

*En el artículo 4 del ENS se enumeran los principios básicos del ENS, los cuales deben inspirar la política de seguridad:*

1. *Seguridad integral.*
2. *Gestión de riesgos.*
3. *Prevención, reacción y recuperación.*
4. *Líneas de defensa.*
5. *Reevaluación periódica.*
6. *Función diferenciada.*

*En la política propuesta se recogen estos principios, a excepción de los claramente operativos (líneas de defensa).*
*Respecto a la función diferenciada, el artículo 10 del ENS establece que «En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad». Si bien en organizaciones pequeñas, como es el caso de los municipio de menos de 2.000 habitantes a los que la FEMP dedica una guía específica, se admite que se asignen estas funciones a una misma persona (el Alcalde), no es lo habitual en administraciones públicas de mayor tamaño como es el Ayuntamiento de Lucena.*

## *Definiciones.*

*En la política de seguridad de la información deben definirse los siguientes roles personales y colegiados:*

- ***Responsable de la Información**: persona que determina la información tratada. Es habitualmente una persona que ocupa un cargo de responsabilidad en la organización. Este cargo*

*asume la responsabilidad del uso que se haga de la información y, por tanto, de su protección. El Responsable de la Información es el responsable de cualquier error o negligencia que lleve a un incidente.*

- ***Responsable del Servicio**: encargado de establecer los requisitos del servicio en materia de seguridad. Puede ser una persona concreta o puede ser un órgano corporativo.*
- ***Responsable de Seguridad**: persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Esta responsabilidad es delegable.*
- ***Responsable del Sistema de Información**: persona que se encarga de la operación del sistema de la información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.*
- ***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.*
- ***Comité de Seguridad de la Información**: se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información, coordinando la seguridad de la información en la entidad.*

*Estos roles, como indica la guía CCN-STIC-801 se estructuran en tres niveles:*

*1. Nivel de Gobierno: en el que se encuentra el Responsable de la Seguridad de la Información.*

*2. Nivel Ejecutivo y de Supervisión: en el que se encuentran el Comité de Seguridad de la Información, el Responsable del Servicio y el Responsable de Seguridad y los Responsables de Entidades del Sector Público Institucional. Desde el punto de vista de la legislación de protección de datos de carácter personal también debería incluirse al Delegado de Protección de Datos.*

*3. Nivel Operacional: en el que se encuentran el Responsable de Seguridad de la Información y los encargados del tratamiento.*

## *Conclusiones.*

### *1. Alcance.*

*Se debe considerar que, de forma análoga a la política de seguridad de la información de la Diputación Provincial, el alcance de esta política de seguridad de la información debe extenderse no solo al Ayuntamiento sino a su sector público institucional.*

### *2. Organización de la seguridad .*

*Se propone la siguiente asignación de roles:*

*1. **Responsable de la Información**: el Alcalde como máxima autoridad del Ayuntamiento.*

*2. **Responsable del Servicio**: el Alcalde por su facultad de dictar resoluciones administrativas de obligado cumplimiento.*

*3. **Responsable de Seguridad**: la Concejal Delegada de Régimen Interior, o persona en quien delegue, como responsable del área funcional en la que se encuentran tanto la Secretaría General como la Sección de Régimen Interior y la Sección de Informática y Telecomunicaciones. Dado que en la presente delegación hay una delegación de alcaldía con la finalidad de impulsar la transformación digital, igualmente se propone que se delegue esta responsabilidad en la Concejal Delegada de Transparencia y Transformación Tecnológica.*

*4. **Responsable del Sistema de Información**: el Jefe de Sección de Informática y Telecomunicaciones en línea con las funciones propias de este puesto de trabajo.*

*5. **Responsables de Entidades del Sector Público Institucional**: a los máximos responsables de las mismas o al personal directivo que se designe.*

*6. **El Comité de Seguridad de la Información** estará compuesto por:*

1. *El Responsable de la Información o concejal en quién delegue. Ejercerá la presidencia del comité.*
2. *El Responsable de Seguridad.*
3. *El Responsable del Sistema de Información que actuará como secretario.*
4. *Los Responsables de Entidades del Sector Público Institucional.*
5. *El Delegado de Protección de Datos.*

6. *El Secretario General de la Corporación.*

*El Comité de Seguridad de la Información debería reunirse con carácter ordinario, al menos, una vez al año y con carácter extraordinario cuando lo convoque el Responsable de la Información o el Responsable de Seguridad.*

*Los miembros del Comité podrán proponer al convocante, individual o colectivamente, la inclusión de asuntos en el orden del día. Para ello se solicitará por escrito y con una antelación mínima de 24 horas.*

*El Comité de Seguridad de la Información podrá asumir como propias las propuestas y dictámenes del Comité de Seguridad de la Información de la Diputación Provincial de Córdoba según lo indicado en el artículo 3.2 del ENS.*

*El Comité de Seguridad podrá invitar a participar con voz pero sin voto al Gerente de EPRINSA en sus funciones de Responsable de Seguridad de la Diputación Provincial, en el marco del citado convenio de colaboración suscrito entre este Ayuntamiento y la Diputación Provincial de Córdoba en materia de asistencia informática."*

Conforme al art. 11.2 del Real Decreto 3/2010, de 8 de enero, se consideran órganos superiores de cada Administración Pública a efectos de la aprobación de la política de seguridad, los "responsables directos de la ejecución de la acción de gobierno", órgano que en los Ayuntamientos se corresponde con este Alcaldía.

En su virtud, en ejercicio de las atribuciones que me vienen conferidas por la norma precedente, VENGO EN DISPONER:

**Primero**.- La designación de los siguientes cargos para ejercer las funciones en materia de política de seguridad de la información que se describen y cuyo contenido figura en la normativa de aplicación:

a) las funciones propias de Responsable de la Información y Responsable del Servicio serán asumidas por esta Alcaldía.

b) las funciones propias del Responsable de Seguridad serán asumidas por la Concejala Delegada de Transparencia y Transformación Tecnológica; y si no existiere este cargo, serán asumidas por el titular de la Delegación de Régimen Interior.

c) las funciones propias del Responsable del Sistema de Información serán asumidas por el Jefe de Sección de Informática y Telecomunicaciones.

d) los Presidentes del Consejo de Administración de las sociedades Suelo y Vivienda de Lucena, S.A. y Aguas de Lucena, S.L., así como el Presidente del Consejo de Administración de la Entidad Pública Empresarial Local "Aparcamientos Municipales de Lucena", serán los responsables de la política de seguridad de la información en sus respectivas entidades en la medida en que les sea de aplicación el ENS.

**Segundo**.- Crear el Comité de Seguridad de la Información de este Ayuntamiento, con la siguiente composición:

1. El Responsable de la Información o concejal en quien delegue. Ejercerá la presidencia.
2.- El Responsable de Seguridad.
3.- El Responsable del Sistema de Información. Actuará como secretario.
4.- Los Responsables de la politica de seguridad de la información del sector público institucional de este Ayuntamiento.
5.- El Delegado de Protección de Datos.

6.- El Secretario General del Ayuntamiento.

El régimen de funcionamiento del Comité se ajustará a lo previsto para el mismo en el documento de Política de Seguridad que se adjunta como anexo.

**Tercero**.- Aprobar la Política de Seguridad de la Información de este Ayuntamiento que se acompaña a la presente resolución como anexo.

**Cuarto**.- Comunicar el presente decreto a las Concejalas Delegadas de Régimen Interior, y Transparencia y Transformación Tecnológica, Jefe de Sección de Informática y Telecomunicaciones, Presidentes de los Consejos de Administración de las entidades dependientes del Ayuntamiento, Delegado de Protección de Datos y Secretario General; y disponer la publicación del documento que contiene la Política de Seguridad en la página web de este Ayuntamiento y en la intranet corporativa.

El Alcalde
(fecha y firma electrónicas)

## ANEXO

### POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE LUCENA

#### 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, el Ayuntamiento de Lucena 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 del Ayuntamiento de Lucena hace pública su misión, visión 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.

**Misión:**

La gestión y el buen gobierno del municipio, dando respuestas a las necesidades y expectativas de los ciudadanos a través de la prestación de servicios de calidad y

garantizando en todo momento la seguridad de la información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción).

**Visión:**

Convertir el Ayuntamiento en un lugar seguro, en el que se cumplan con los principios y requisitos necesarios para una protección adecuada de la información, asegurando el cumplimento de las cinco dimensiones de la seguridad: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad.

Las diferentes áreas y servicios han de cerciorarse de que la seguridad de la información es una parte vital de los servicios públicos prestados por el Ayuntamiento de Lucena.

**Valores:**

Las áreas y servicios del Ayuntamiento de Lucena entienden la seguridad de la información como un valor que orienta la conducta de las personas hacia las buenas prácticas de seguridad por lo que 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 del Ayuntamiento de Lucena y su Sector Público Institucional, cualquiera que sea su clasificación jerárquica. Igualmente, se 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 esta norma, 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.
El Reglamento (EU) 679/2016, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos establece 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.

Según el artículo 10 del Real Decreto 3/2010, de 8 de enero que regula el ENS, en los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de seguridad.

- **Responsable de la Información**: Determina la información tratada. Es habitualmente una persona que ocupa un cargo de responsabilidad en la organización. Este cargo asume la responsabilidad del uso que se haga de la información y, por tanto, de su protección. El Responsable de la Información es el responsable de cualquier error o negligencia que lleve a un incidente.
- **Responsable del Servicio**: Es el encargado de establecer los requisitos del servicio en materia de seguridad. Puede ser una persona concreta o puede ser un órgano corporativo.
- **Responsable de Seguridad**: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Asimismo, la Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad, Responsabilidades y Funciones propone que estas responsabilidades se instrumenten por medio de comités, haciendo referencia concretamente al Comité de Seguridad de la Información que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.
Para gestionar y coordinar proactivamente la seguridad de la información, el Ayuntamiento de Lucena nombra su Comité de Seguridad de la Información que podrá asumir como propias las recomendaciones y dictámenes del Comité de Seguridad de la Información de Diputación Provincial de Córdoba. Para su asesoramiento técnico el ayuntamiento se apoyará en dicho Comité y en las Políticas, Normativas y demás documentación aprobadas por el mismo.

No obstante, el Ayuntamiento de Lucena designa la figura de **Responsable de la Información** que recae en la persona del Alcalde como máxima autoridad en el ayuntamiento, el cual velará por el adecuado tratamiento y custodia de la información y seguirá las directrices que marque el Comité de Seguridad de la Información.
Así mismo, designa la figura de **Responsable del Servicio** que recae en la persona del Alcalde por su capacidad de dictar resoluciones administrativas. Será responsable de los sistemas de información objeto de esta Política de Seguridad y tiene la potestad de determinar los requisitos de seguridad de los servicios prestados de

acuerdo con las directrices y recomendaciones que marque el Comité de Seguridad de la Información.

A su vez designa también la figura del **Responsable de Seguridad** de la Información que recae en la persona de la Concejal Delegada de Transparencia y Transformación Tecnológica, o persona en quien ésta delegue, que será la encargada de coordinar y controlar las medidas que se definan por el Comité de Seguridad y se coordinará en sus funciones con el Responsable de Seguridad de la Información del propio Comité de Seguridad de la Información. En defecto del cargo anterior, el Responsable de Seguridad de la Información será el concejal titular de la Delegación de Régimen Interior.

**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.

Por último, se designa la figura de **Responsable del sistema** que recae en la persona del Jefe de Sección de Informática y Telecomunicaciones, que se encargará de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad, así como adoptar las medidas correctoras adecuadas que emanen tanto de los informes de autoevaluación como de los informes de auditoría.

Contará dentro de su entidad, con los medios técnicos y humanos y con las atribuciones necesarias para poder desempeñar con eficacia las funciones que se les encomiendan.

### 4.1. COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN.

Sus **funciones** son las siguientes:

1. Responsabilidades derivadas del tratamiento de datos de carácter personal.
2. Atender las inquietudes de la Corporación y de las diferentes áreas.
3. Informar regularmente del estado de la seguridad de la información a la Junta de Gobierno Local.
4. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
5. Elaborar la estrategia de evolución del Ayuntamiento de Lucena y su Sector Público Institucional en lo que respecta a la seguridad de la información.
6. 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.
7. Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Comité de Seguridad.
8. Aprobar la normativa de seguridad de la información.
9. Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
10. Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
11. Monitorizar los principales riesgos residuales asumidos por la empresa y recomendar posibles actuaciones respecto de ellos.

12. 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.
13. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
14. Aprobar planes de mejora de la seguridad de la información. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
15. 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.
16. 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.
17. 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.
18. En caso de ocurrencia de incidentes de seguridad de la información aprobará el Plan de Mejora de la Seguridad.

Su **composición** será la siguiente:

- El Responsable de la Información o concejal en quién delegue. Ejercerá la presidencia del comité.
- El Responsable de Seguridad.
- El Responsable del Sistema de Información que actuará como secretario.
- Los Responsables de Entidades del Sector Público Institucional.
- El Delegado de Protección de Datos.
- El Secretario General de la Corporación.
- Podrá invitarse con voz, pero sin voto, al Gerente de EPRINSA en su calidad de Responsable de la Seguridad de la Diputación Provincial de Córdoba.

Su **funcionamiento** será el siguiente:

1. El Comité de Seguridad de la Información debería reunirse con carácter ordinario, al menos, una vez al año y con carácter extraordinario cuando lo convoque el Responsable de la Información o el Responsable de Seguridad.
2. Los miembros del Comité podrán proponer al convocante, individual o colectivamente, la inclusión de asuntos en el orden del día. Para ello se solicitará por escrito y con una antelación mínima de 24 horas.
3. El Comité de Seguridad de la Información podrá asumir como propias las propuestas y dictámenes del Comité de Seguridad de la Información de la Diputación Provincial de Córdoba según lo indicado en el artículo 11.2 del ENS respecto a la posibilidad de que los Ayuntamientos se acojan a las políticas de seguridad de la información aprobadas con carácter provincial.
4. Con el fin de agilizar los desarrollos del Comité que no requieran la presencia de todos los integrantes del mismo, se podrán designar grupos de trabajo

especializados compuestos tanto por miembros del propio Comité, otros miembros de la corporación, así como personal interno o externo.

## 5. CONCIENCIACIÓN

El Ayuntamiento de Lucena establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad de la Información, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo con esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad.
El Responsable de Información del Ayuntamiento en coordinación con el Comité de Seguridad, establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

## 6. GESTIÓN DEL RIESGO

El Ayuntamiento de Lucena 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 del Ayuntamiento de Lucena 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.