BOLETÍN OFICIAL DE LA PROVINCIA DE GUADALAJARA
949 88 75 72
Administración: Excma. Diputación Provincial. Pza. Moreno, N.º 10.
Edita: DIPUTACIÓN PROVINCIAL Director: Jaime Celada López
BOP de Guadalajara, nº. 33, fecha: viernes, 15 de Febrero de 2019

AYUNTAMIENTOS

AYUNTAMIENTO DE ALOVERA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE ALOVERA

366

Aprobada mediante Resolución de Alcaldía número 2019-0311, la Política de Seguridad de la Información del Ayuntamiento de Alovera, en cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad de la Administración electrónica, se publica el texto íntegro que también podrá consultarse en el Tablón de Anuncios y en el Portal de Transparencia del Ayuntamiento de Alovera https://alovera.sedelectronica.es

Alovera, 12 de febrero de 2019.- La Alcaldesa, María Purificación Tortuero Pliego.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE ALOVERA

El Ayuntamiento de Alovera considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por tanto, la seguridad de la información como una responsabilidad asociada a su protección frente a las amenazas que puedan afectar a su autenticidad, integridad, disponibilidad, confidencialidad o trazabilidad.

Como parte de esa responsabilidad, el Ayuntamiento de Alovera define, a través de este Decreto, una política de seguridad de la información con el objetivo de dirigir y dar soporte a la gestión de la seguridad de la información mediante el

establecimiento de unas directrices básicas de acuerdo con los requisitos propios de seguridad y a la regulación aplicables.

1. Objeto.

El presente Decreto tiene por objeto definir la política en materia de seguridad de la información del Ayuntamiento de Alovera, así como el establecimiento del marco organizativo y operacional, garantizando a los ciudadanos la gestión de sus datos de forma segura y conforme a la legislación vigente en esta materia.

2. Ámbito de aplicación.

La política de seguridad de la información que se define mediante este Decreto será de aplicación en todo el Ayuntamiento de Alovera.

3. Misión de la Organización.

El Ayuntamiento de Alovera es la institución encargada del gobierno del municipio de Alovera. Sus competencias están recogidas en la ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

4. Marco normativo.

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Alovera, y, en particular, la prestación de sus servicios electrónicos a los ciudadanos, está integrado por las siguientes normas:

- Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.
- 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 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

5. Estructura organizativa.

La estructura organizativa de la gestión de la seguridad de la información en el Ayuntamiento de Alovera está compuesta por los siguientes agentes:

- El Responsable de la Información.
- El Responsable del Servicio.
- El Responsable de Seguridad.

- El Responsable del Sistema.
- El Administrador de la seguridad del sistema.
- La Comisión técnica de trabajo en materia de seguridad electrónica.

6. El Responsable de la Información.

1. El responsable de la información tiene la responsabilidad última del uso que se haga de una cierta información y de su protección y se corresponderá con la figura del Alcalde-Presidente de la Corporación.
2. Dentro del marco establecido en el anexo I 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, tiene la potestad de determinar los niveles de seguridad de la información.

7. El Responsable del Servicio.

1. El responsable del servicio tiene la responsabilidad última de la prestación de un cierto servicio y de su protección y se corresponderá con la figura del Alcalde-Presidente de la Corporación.
2. Dentro del marco establecido en el anexo I 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, tiene la potestad de determinar los niveles de seguridad de los servicios.

8. El Responsable de Seguridad.

1. El responsable de seguridad tendrá las siguientes atribuciones:
    a. Elaborar las propuestas de modificación y actualización de la política de seguridad de la información en el Ayuntamiento de Alovera.
    b. Coordinar el proceso de gestión de la seguridad.
    c. Desarrollar la Política de Seguridad de la Información.
    d. La supervisión del cumplimiento de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de la información.
    e. Promover las actividades de concienciación y formación en materia de seguridad.
    f. Proponer para su aprobación y seguimiento, los planes estratégicos, planes directores y líneas de actuación en materia de seguridad de la información.
    g. Proponer para su aprobación y seguimiento las políticas de auditoría para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
2. El responsable de seguridad se corresponderá con la figura del Alcalde-Presidente de la Corporación.

9. El Responsable del Sistema.

1. El responsable del sistema se corresponderá con la figura del Alcalde-Presidente de la Corporación.
2. Desarrollará, entre otras, las siguientes funciones:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b. Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c. Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.
d. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

3. El responsable del sistema podrá apoyarse en el administrador de la seguridad del sistema en el desempeño de sus funciones.
4. Dentro del marco establecido en 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 la facultad para determinar la categoría de los sistemas.

10. El Administrador de la seguridad del sistema.

1. El administrador de la seguridad del sistema (ASS) se corresponderá con el titular del Servicio de informática y tecnologías de la información y la comunicación.
2. Desarrollará, entre otras, las siguientes funciones:
   a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
   b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
   c. La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
   d. La aplicación de los Procedimientos Operativos de Seguridad.
   e. Aprobar los cambios en la configuración vigente del Sistema de Información.
   f. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
   g. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
   h. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
   i. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
   j. Informar a los responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
   k. Colaborar en la investigación y resolución de incidentes de seguridad,

desde su detección hasta su resolución.

3. El ASS podrá delegar o compartir la totalidad o parte de sus funciones con el personal técnico cualificado que, con el responsable del sistema, se acuerde en cada momento.

11. La Comisión técnica de trabajo en materia de seguridad electrónica.

1. La comisión técnica de trabajo en materia de seguridad electrónica estará compuesta por:

   - El Responsable de seguridad.
   - El Administrador de la seguridad del sistema.
   - El Técnico informático municipal.
   - El Técnico de archivo municipal.
   - El Técnico de empleo y desarrollo local.

2. Su función será asesorar al Responsable de seguridad en el desarrollo de la Política de Seguridad y proponer posibles cambios en ella.
3. Se reunirá de forma regular para evaluar el cumplimiento de la Política de Seguridad y detectar posibles deficiencias.

12. Estructura de la Política de Seguridad.

1. La Política de Seguridad es de obligado cumplimiento y se desarrollará en los siguientes niveles relacionados jerárquicamente:
   a. Primer nivel: Política de Seguridad de la Información. Está constituido por el presente Decreto y es de obligado cumplimiento.
   b. Segundo nivel: Instrucciones de Seguridad de la Información. Está constituido por el conjunto de instrucciones que desarrollan la política de seguridad. Cada conjunto de instrucciones abarcará un área o aspecto determinado y regulará qué se puede hacer y qué no desde el punto de vista de la seguridad sin entrar en detalles de implementación ni tecnológicos. Los documentos relativos a este segundo nivel deberán ser propuestos por el Responsable de Seguridad, con el asesoramiento de la Comisión técnica de trabajo en materia de seguridad electrónica, y aprobados por el Alcalde-Presidente.
   c. Tercer nivel: Procedimientos de Seguridad de la Información. Está constituido por el conjunto de directrices de carácter técnico o procedimental que dan respuesta a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos en ella establecidos. La responsabilidad de aprobación de estos procedimientos técnicos recaerá sobre el Responsable de Seguridad.
   d. Aparte de los documentos citados, la documentación de seguridad podrá contar, con otros documentos como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.
2. Los responsables pertenecientes a la estructura organizativa establecida en esta política de seguridad establecerán los mecanismos necesarios para compartir la documentación derivada de la misma, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad de la

información.

13. Protección de datos de carácter personal.

1. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.
2. En lo que se refiere a los tratamientos de datos de carácter personal, estarán referenciados en el correspondiente documento de seguridad donde se hará constar tanto los tratamientos afectados como los responsables correspondientes.

14. Gestión de riesgos.

1. La gestión de riesgos es parte esencial del proceso de seguridad y ha de realizase de manera continua sobre los sistemas de información con el objetivo de mantener los entornos controlados minimizando los riesgos hasta niveles aceptables.
2. La gestión de riesgos será preceptiva para los sistemas de información incluidos dentro del marco establecido por 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.
3. Los responsables de la información y del servicio son los propietarios de los riesgos sobre la información y sobre los servicios respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea. Para ello podrán contar en el proceso con la participación y asesoramiento del responsable de seguridad, del responsable del sistema y de la Comisión técnica de trabajo en materia de seguridad electrónica.
4. Para la realización del análisis de riesgos se podrán utilizar las herramientas establecidas para este fin por el servicio responsable de seguridad, que facilitan el seguimiento de la aplicación de las medidas de seguridad seleccionadas y proporcionan un valor de riesgos residual estabilizado y comparable entre diferentes sistemas de información.

15. Resolución de conflictos.

En caso de surgir conflictos entre los distintos agentes, éste debe ser resuelto por el Alcalde-Presidente, como superior jerárquico de los mismos.

16. Obligaciones del personal.

1. Todo el personal con responsabilidad en el uso, operación o administración de sistemas de tecnologías de la información y las comunicaciones recibirá formación para el manejo seguro de los sistemas. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos, así como la difusión entre los mismos de la Política de Seguridad de la Información.
2. Este personal tiene la obligación de cumplir la Política de Seguridad de la Información.
3. Cuando el Ayuntamiento utilice servicios de terceros o ceda información a terceros, se les hará partícipes de la presente Política de Seguridad y de las

Instrucciones y Procedimientos de Seguridad derivados. Los terceros quedarán sujetos a las obligaciones establecidas en estos documentos, debiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Disposición final única. Entrada en vigor.

Este Decreto entrará en vigor el día siguiente al de su publicación.