ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE ORCERA (JAÉN)

2018/5015 *Política de seguridad de este Ayuntamiento.*

Anuncio

POLÍTICA DE SEGURIDAD DEL AYUNTAMIENTO DE ORCERA

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 06 de noviembre de 2018 por el Pleno del Ayuntamiento de Orcera.

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

2. INTRODUCCIÓN

El Ayuntamiento de Orcera con el desarrollo de las Tecnologías de la Información depende en gran medida de los sistemas TIC (Tecnologías de Información y Comunicaciones) para llevar a cabo los trámites y servicios a la ciudadanía. 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 los departamentos 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.

Los diferentes servicios municipales deben 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.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

Los servicios municipales deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS[1)].

2.1. PREVENCIÓN

Los diferentes servicios y dependencias municipales deben 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 los departamentos deben implementar 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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, todos los servicios y dependencias municipales deben:

• Autorizar los sistemas antes de entrar en operación. (control de accesos).

• 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 las operaciones 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[2)].

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS[3)]. 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

Cada departamento o servicio municipal debe:

• Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

• Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

• Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias Informáticas (CERT)[4)].

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, todos los servicios y dependencias municipales deben desarrollar 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 se aplica a todos los sistemas TIC del Ayuntamiento de Orcera, sus organismos autónomos y en los que el Ayuntamiento desarrolla su actividad municipal y a todos los miembros electos y trabajadores del Ayuntamiento, sin excepciones.

4. MISIÓN

La principal misión del Ayuntamiento de Orcera y sus organismos dependientes y autónomos es dar respuesta a las necesidades y expectativas de sus ciudadanos mediante la prestación de servicios, de forma eficaz y eficiente, a través de un equipo humano profesional en cada área y empleando los medios y recursos técnicos más adecuados.

Esta misión y las acciones recurrentes para su consecución se rigen por los principios de Legalidad, autonomía local, transparencia y gestión responsable.

5. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Orcera y sus entidades vinculadas o dependientes en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al 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 al ámbito de la Administración Electrónica.

- Ley Orgánica 15/1999 de diciembre, 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 13 de diciembre, de Protección de Datos de Carácter Personal.

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

- Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

- 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 (Reglamento general de protección de datos).

Del mismo modo, formaran parte del marco regulador, cuantas normas aplicables a la Administración Electrónica del Ayuntamiento de Orcera sean aprobadas para el desarrollo o complementen las anteriores en el uso de su potestad de autorregulación y que se encuentren dentro del ámbito de aplicación esta Política de Seguridad de la Información.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN: FUNCIONES Y RESPONSABILIDADES

La Comisión de Seguridad de la Información (CSI) del Ayuntamiento de Orcera y sus organismos autónomos estará formado por una Presidencia, Secretaría y cuantos vocales sean necesarios, contando con asistencia técnica informática y de Sistemas:

Presidencia: Alcalde electo.

Secretaría: Secretario Municipal.

Vocal/es: Personal administrativo del Ayuntamiento, y en su caso el responsable de seguridad y los responsables delegados de Seguridad de cada Servicio, dependencia y/o organismo autónomo.

Personal técnico: Designación de personal funcionario o laboral en activo con aptitudes acreditadas.

La Secretaría de la CSI será el Secretario Municipal y tendrá como funciones:

- Convocar la Comisión de Seguridad de la Información en su edición regular y extraordinaria en su caso, recopilando la información pertinente.

- Incorporar en el orden del día las inquietudes de los responsables de seguridad de los distintos servicios para su discusión en las reuniones convocadas.

- Junto a los responsables de seguridad, debe estar al tanto de los cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten al Ayuntamiento, debiendo informarse de las consecuencias para las actividades del mismo, alertando a la Comisión de Seguridad de la Información y proponiendo las medidas oportunas de acción en el nuevo marco legal.

- En caso de desastre, se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de seguridad del Ayuntamiento.

La CSI reportará e informará al Pleno del Ayuntamiento de Orcera.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

La CSI tendrá las siguientes funciones:

- Coordinar todas las funciones de Seguridad de la Información del Ayuntamiento de Orcera.

- Velar por el cumplimiento de la normativa legal, regulatoria y sectorial.

- Velar por alineamiento de las actividades y los objetivos de seguridad de la Información llevadas a cabo por el Ayuntamiento y sus organismos.

- Elaboración y actualización de la Política de Seguridad de la Información y Sistemas, y éstas aprobadas por el Pleno Municipal.

- Recabar de los distintos responsables de Seguridad en los diferentes servicios y organismos municipales los informes regulares del estado de la Seguridad.

- Coordinar y dar respuesta a las inquietudes e incidencias transmitidas por los Responsables de Seguridad.

- Definir y asignar los roles y criterios para lograr las garantías que se estimen pertinentes para la delegación de tareas en materia de seguridad.

6.2. ROLES: NOMBRAMIENTOS, FUNCIONES Y RESPONSABILIDADES

El Ayuntamiento Pleno, a través de recomendación de la CSI, nombrará a un Responsable de Seguridad de la Información de entre el personal del Ayuntamiento o bien personal externo. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Al Responsable de Seguridad de la Información le corresponden las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad.

- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Para ello, son de su responsabilidad las tareas de:

- Determinación de la categoría del sistema de Información
- Realizar el análisis de riesgos
- Establecer Medidas de seguridad adicionales
- Redactar la Documentación de seguridad del sistema
- Elaborar la Normativa de seguridad (Aprueba la CSI)
- Aprobar los Procedimientos operativos de seguridad
- Informar del Estado de la seguridad del sistema
- Elaborar los Planes de mejora de la seguridad y Planes de concienciación y formación
- Validar los Planes de continuidad

Asistirá como apoyo informativo a la Comisión de Seguridad de la Información; puede estar identificado con el Delegado de Protección de Datos, ampliando así los roles establecidos

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

por el RGPDP.

Es posible la delegación de funciones y tareas del Responsable de Seguridad del Sistema en los Responsables Delegados de Seguridad, realizándose por parte de la Comisión de Seguridad de la Información, indicando en este nombramiento el ámbito y las funciones que les son delegadas.

En su caso, para las cuestiones operacionales, el Ayuntamiento Pleno nombrará a un Responsable de Sistemas con capacitación técnica suficiente. La persona designada figurará en la documentación de seguridad del sistema de información. Sus responsabilidades, son:

- 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.

- Puede recomendar 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.

Algunas de sus tareas para ejecutar estas responsabilidades son:

- Elaborar los Procedimientos operativos de seguridad
- Redactar Planes de mejora de la seguridad y Planes de continuidad
- En caso de necesidad acometerá la suspensión temporal del servicio/s
- En el Ciclo de vida de los sistemas redactará la especificación, arquitectura, desarrollo, operación, cambios necesarios.

Esta figura puede ser suplida por su correspondiente designada en cada departamento o servicio municipal responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión de la Comisión de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Ayuntamiento Pleno y difundida para que la conozcan todas las partes afectadas y ciudadanía.

7. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Orcera trata datos de carácter personal.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información del Ayuntamiento de Orcera se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. 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 una vez al año
- 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, la CSI establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. La CSI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa a las políticas de seguridad del Ayuntamiento de Orcera en diferentes materias en vigor en el momento de la aprobación de esta Política:

Protección de datos.

Otras referencias a otras políticas en materia de seguridad.

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.

La normativa de seguridad estará disponible en internet (http://orcera.sedelectronica.es o en http://www.orcera.es/servicios-y-tramites/reglamentos-ordenanzas.html) e impresa en la sede del Ayuntamiento de Orcera en Plaza de la Iglesia, 1 de Orcera.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros electos y personal del Ayuntamiento de Orcera 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros del Ayuntamiento de Orcera atenderán a una sesión de concienciación

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del Ayuntamiento, 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.

11. TERCERAS PARTES

Cuando el Ayuntamiento de Orcera preste servicios a otros organismos o maneje 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 el Ayuntamiento utilice servicios de terceros o ceda 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.

[1)] *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. BOE núm. 25, de 29 de enero de 2010:*

Art.7: Prevención, reacción y recuperación.

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

[2)] *Real Decreto 3/2010, de 8 de enero, (…)*

Artículo 9. Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

[3)] *Real Decreto 3/2010, de 8 de enero, (…)*

Artículo 8. Líneas de defensa.

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

[4)] CERT: Un Equipo de Respuesta ante Emergencias Informáticas *(CERT, del inglés Computer Emergency Response Team)* es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Orcera, a 14 de Noviembre de 2018.- El Alcalde-Presidente, Juan Francisco Fernández López.

cve: BOP-2018-5015
Verificable en https://bop.dipujaen.es