Ayuntamientos

AYUNTAMIENTO DE ILLESCAS

En sesión ordinaria celebrada por el pleno de este Ayuntamiento en fecha 28 de marzo de 2019 se ha aprobado expresamente con carácter definitivo la redacción final del texto de la Política de seguridad de la información del Ayuntamiento de Illescas, en los términos en que figura en el expediente, la cual se transcribe:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE ILLESCAS

1. Objetivo

La Política de Seguridad de la Información (en adelante, Política de Seguridad) del Ayuntamiento de Illescas (en adelante, Ayuntamiento), es el instrumento en el que se apoya, identifica responsabilidades, establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las tecnologías de la información y de las comunicaciones.

La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el Ayuntamiento.

2. Alcance

La Política de Seguridad será de obligado cumplimiento para todos los órganos superiores y directivos del Ayuntamiento, así como para terceras partes que presten servicios a la Entidad Local; manejen su información y la actualicen en la prestación de los servicios que tienen contratados.

Esta Política de Seguridad estará disponible para consulta de todos ellos a través de la sede electrónica del Ayuntamiento y en el "Boletín Oficial" de la provincia de Toledo.

3. Marco normativo

El marco normativo de las actividades del Ayuntamiento en el ámbito de la Política de Seguridad está integrado por las siguientes normas:

a) 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.

b) Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

c) Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

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

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

f) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

g) Ley 59/2003, de 19 de diciembre, de firma electrónica.

h) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio.

i) Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

j) Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público

k) Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.

l) Ley 9/2014, de 9 de mayo, general de telecomunicaciones.

m) 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.

n) 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.

o) Ordenanza publicada en la página web respecto a ficheros de datos carácter personal publicada en el "Boletín Oficial" de la provincia de Toledo número 237, de fecha 16 de octubre de 2015

p) Normas aplicables a la administración electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información.

4. Principios y directrices

Los principios y directrices que deben de contemplarse a la hora de garantizar la seguridad de la información y asegurar que el Ayuntamiento cumpla sus objetivos, son los que se establecen en las siguientes normas:

a) 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.

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

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

d) 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.

e) 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.

4.1. Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

4.2. Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

4.3. Prevención, reacción y recuperación: La seguridad del sistema debe contemplar aspectos de prevención, detección, respuesta y recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o comprometa los servicios que presta.

El Ayuntamiento debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, sus órganos directivos deben implementar las medidas mínimas de seguridad determinadas por el ENS, por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Así mismo deberán tenerse en cuenta las medidas especificadas en el artículo 32 del Reglamento UE 2016/679, que deberán garantizar un nivel de seguridad adecuado al riesgo para tratamientos automatizados, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, en particular:

a) Para garantizar el cumplimiento de la Política de Seguridad, los órganos responsables deben:

–Autorizar los sistemas o los servicios antes de entrar en operación.

–Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

–Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.

b) Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, los órganos responsables 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.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, los órganos responsables deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

c) Los órganos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad. Con el fin de garantizar la disponibilidad de los servicios críticos, losórganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4.4. Líneas de defensa: 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:

–Ganar tiempo para una reacción adecuada.

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

–Minimizar el impacto final sobre el mismo.

4.5. 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.

4.6. La seguridad como función diferenciada: La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, siendo el responsable de la Información quien determinará los requisitos de la información tratada, el responsable del Servicio quien determinará los requisitos de los servicios prestados, y el Responsable de seguridad quien determinará las decisiones técnicas para satisfacer los requisitos de seguridad de la información y de los servicios.

5. Estructura

5.1. Política de Seguridad: La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel: Política de Seguridad.

b) Segundo nivel: Instrucciones o Normativa de Seguridad de la Información.

c) Tercer nivel: Procedimientos de Seguridad de la Información.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de la Entidad Local, sin necesidad de revisar su estrategia de seguridad.

5.2. Personal del Ayuntamiento: El personal del Ayuntamiento tendrá la obligación de conocer y cumplir, además de la Política de Seguridad, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Instrucciones y los Procedimientos de Seguridad de la información estarán disponibles y actualizados en la Intranet del Ayuntamiento.

5.3. Niveles de la Política de Seguridad:

–Primer nivel: Política de Seguridad, constituye el primer nivel la Política de Seguridad, recogida en el presente texto y aprobada por el Pleno del Ayuntamiento.

–Segundo nivel: Instrucciones de Seguridad de la Información que desarrolla la Política de Seguridad mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información.

Las Instrucciones de Seguridad de la Información serán aprobadas por la persona titular de la Alcaldía-Presidencia, a propuesta del Comité de Seguridad de la Información del Ayuntamiento y desarrollarán, al menos las siguientes materias:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información.

h) Gestión de los incidentes de seguridad implantando los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad implantando los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

–Tercer nivel: Procedimientos de Seguridad de la Información, que está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobadas por el Responsable de Seguridad de la Información.

6. Organización de la seguridad

La organización de la seguridad en el Ayuntamiento queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

6.1. Pleno: El pleno del Ayuntamiento, mediante la aprobación de la presente Política de Seguridad, asegura el compromiso de las autoridades del Ayuntamiento en la aplicación del ENS.

Este compromiso se manifiesta mediante la aprobación de la Política de Seguridad de la Información, así como de todas aquellas modificaciones o actualizaciones de la misma que el Comité de Seguridad de la Información pueda proponer, en el ámbito de sus competencias.

6.2. Comité de Seguridad de la Información: La composición, funciones y responsabilidades del Comité son establecidas en el Reglamento de regulación, composición y funcionamiento del comité de seguridad de la información del Ayuntamiento de Illescas (en adelante Comité).

6.3. Responsable de la Información: La máxima responsabilidad de la información del Ayuntamiento recaerá en el Comité y se hará extensiva a los titulares de las distintos departamentos y áreas del Ayuntamiento, responsabilizándoles de la información afectada por la presente Política de Seguridad, en sus respectivos ámbitos de competencia.

Corresponde al responsable de la información establecer los requisitos de la información en materia de seguridad, y en particular:

a) Determinar los niveles de seguridad de la información tratada y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.

b) Realizar, junto a los responsables de los departamentos y áreas y el responsable de seguridad de la Información, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.

c) Aceptar los riesgos residuales respecto de la información calculada en el análisis de riesgos.

d) Realizar el seguimiento y control de los riesgos.

6.4. Responsable de seguridad: De conformidad con el acuerdo de pleno de 31 de enero de 2019 por el que se crea el Comité de Seguridad en el Ayuntamiento y el acuerdo de pleno de 28 de marzo de 2019 por el que se aprueba el Reglamento del Comité de Seguridad, corresponde al responsable de Seguridad establecer las medidas necesarias para cumplir los requisitos de seguridad establecidos por el responsable de la Información y el responsable de servicio. El responsable de Seguridad será designado por el Alcalde-Presidente del Ayuntamiento.

En el ejercicio de las citadas competencias, el responsable de seguridad desarrollará las siguientes funciones:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Analizar y elevar al Comité toda la documentación relacionada con las instrucciones de seguridad de la información para su aprobación.

c) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.

d) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

e) Elaborar informes periódicos de seguridad para el Comité, que incluirán los incidentes más relevantes de cada periodo.

f) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

g) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

6.5. Responsable de Sistemas: De conformidad con el acuerdo de pleno de 31 de enero de 2019 por el que se crea el Comité de Seguridad en el Ayuntamiento y el acuerdo de pleno de 28 de marzo de 2019 por el que se aprueba el Reglamento del Comité de Seguridad, corresponde al Responsable del Sistema las funciones que le son propias y establecer las medidas necesarias para cumplir los requisitos establecidos por el responsable de la Información y el responsable de Seguridad en cada uno de los sistemas de información y servicios. El responsable del Sistema será designado por el Alcalde-Presidente del Ayuntamiento.

En el ejercicio de las citadas competencias, el responsable de Sistemas desarrollará las siguientes funciones:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Analizar y elevar al Comité toda la documentación relacionada con las instrucciones de seguridad de la información para su aprobación.

c) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.

d) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

e) Elaborar informes periódicos de seguridad para el Comité, que incluirán los incidentes más relevantes de cada periodo.

f) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

g) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

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

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

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

k) 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.

6.6. Responsables delegados: Serán nombrados como responsables delegados de Servicio, cada uno de los titulares de los distintos departamentos y/o áreas del Ayuntamiento que por naturaleza son los responsables de cada servicio electrónico afecto a la presente Política de Seguridad, en quienes se delegará lo referente a sus respectivas dependencias y ámbitos de competencia, actuando como asesores y asistentes del Comité.

Corresponde al Comité, como responsable de la Información establecer los requisitos del servicio en materia de seguridad, y en particular:

a) Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.

b) Realizar, junto a los responsables de la Información, el responsable de seguridad y el responsable de Sistemas, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.

c) Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.

d) Realizar el seguimiento y control de los riesgos.

e) Suspender, de acuerdo con el responsable de la Información, responsable de seguridad y el responsable de Sistemas, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

6.7. Resolución de conflictos: En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad, éste será resuelto por el Comité o por el Órgano competente de conformidad con lo previsto en los acuerdos de la Junta de Gobierno de organización y competencias y los estatutos del correspondiente organismo público, dando cuenta al Comité.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

7. Datos de carácter personal

El Ayuntamiento realiza tratamientos de datos de carácter personal. La relación de ficheros creados e inscritos en la Agencia Española de Protección de Datos (AEPD) están publicados en la dirección de internet: https://www.agpd.es de forma particular para cada una de las organismos y empresas que componen la entidad local.

El Ayuntamiento realiza sistemáticamente tratamientos en los que hace uso de datos de carácter personal. Estos tratamientos se recogen en el Documento de Seguridad de cada una de las entidades, tal y como establece el 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.

El registro de tratamientos será accesible por cada uno de los empleados del Ayuntamiento a través de la intranet del Ayuntamiento.

8. Concienciación y formación

En la aplicación de esta Política de Seguridad, deberá de prestarse la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

Todo el personal de la entidad local que esté relacionado con la información y los sistemas forma parte del plan de formación continuada, para así dar cumplimiento en la entidad local su compromiso de formar e informar de los deberes y obligaciones que tiene el personal en materia de seguridad.

Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos.

Por lo anterior, el personal del Ayuntamiento recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

9. Gestión de riesgos

El análisis y gestión de riesgos, evaluando las amenazas y los riesgos a los que están expuestos la información, los servicios y sistemas del Ayuntamiento, será la base para determinar las medidas de seguridad que se deben adoptar. El análisis de riesgos se realizará:

a) Regularmente, al menos una vez al año.

b) Cuando cambie la información manejada.

c) Cuando cambien los servicios prestados.

d) Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el anexo I del Real Decreto 3/2010, de 8 de enero.

e) Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el anexo I del Real Decreto 3/2010, de 8 de enero. Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad de la Información, asimismo, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. Terceras partes

El Comité establecerá canales para el reporte y la coordinación de los Comités y Grupos de Trabajo que estén operativos y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento preste servicios a otros organismos o ceda información a terceros, les hará partícipes de esta Política de Seguridad y de las Instrucciones y Procedimientos que atañan a dichos servicios o información, quedando sujetos a las obligaciones que en ellos se establezcan, sin perjuicio de que puedan desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias y se exigirá que el personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

En el caso de cesiones o comunicaciones de datos de carácter personal a terceros, aun cuando sean Administraciones Públicas, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y a la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, requiriéndose que la concienciación se realice también en lo relativo al adecuado cumplimiento de las normativas sobre protección de datos.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, de conformidad con lo dispuesto en los párrafos anteriores, será necesario que el Responsable de seguridad emita un informe en el que se precisen los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el responsable de la Información y Responsable de servicio correspondiente para poder continuar con la utilización del servicio o el manejo de la información.

11. Revisión

El Comité revisará anualmente la Política de Seguridad de la Información o cuando exista un cambio significativo que obligue a ello.

La revisión será aprobada por el pleno del Ayuntamiento y difundida para que la conozcan todas las partes afectadas, publicándola en el "Boletín Oficial" de la provincia de Toledo y en la sede electrónica del Ayuntamiento.

Lo que se publica en el "Boletín Oficial" de la provincia de Toledo, entrando en vigor según lo previsto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local. Asimismo, estará a disposición de los interesados en la página web del Ayuntamiento https://illescas.es y en el portal de transparencia de la sede electrónica de este Ayuntamiento http://illescas.sedelectronica.es.

Illescas, 15 de abril de 2019.–El Alcalde, José Manuel Tofiño Pérez.

N.º I.-2049