SORIA

En la Casa Consistorial "Doce Linajes" de la Ciudad de Soria a fecha de 2 de julio de 2.024, el Ilmo. Sr. Alcalde-Presidente, D. Carlos Martínez Mínguez, adopto la resolución de aprobar el texto modificado de la Política de Seguridad de la Información del Ayuntamiento de Soria adaptado a los cambios introducidos en el Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

POLÍTICA DE SEGURIDAD DEL AYUNTAMIENTO DE SORIA

Sumario

La Seguridad de los Sistemas

El Ayuntamiento de Soria como Administración Local depende en gran medida de los sistemas de tecnología y comunicaciones para alcanzar sus objetivos y poder desarrollar de manera adecuada las competencias que por ley debe desarrollar.

El desarrollo de las tecnologías de la información y comunicación ha tenido un gran impacto en la forma y el contenido de las relaciones que como Administración debemos desarrollar con la ciudadanía y las entidades del sector privado.

BOPSO-109-18092024

Consagrado en nuestro entorno, el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación que recae sobre el sector público – incluido este Ayuntamiento-, de dotarse de los medios y sistemas necesarios para que ese derecho sea ejercitable plenamente, debemos constituir como normalizado y habitual la gestión de los procedimientos íntegramente electrónicos, en base a los principios de eficacia y eficiencia, con el impacto en aminoración de costes y como garantía de derechos y de cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados.

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 sin olvidar la trazabilidad y autenticidad que en mayor medida afecta a la información.

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 que sustentan toda la función pública, 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.

En este entorno, se hacía necesario que el legislador considerara la necesidad de adecuar y alinear la estrategia de seguridad del sector público e impusiera un criterio unificador y estableciese las condiciones necesarias de confianza en el uso de los medios electrónicos, declarándolo como principio vertebrador de la actividad pública. Surgió así 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, en cumplimiento de lo que dispuso en su momento la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Dicho Real Decreto, venía a regular una de las piezas fundamentales de la denominada Administración Electrónica y la seguridad de los sistemas de información del Sector Público.

Vista la necesidad de armonizar los criterios públicos e impulsar el procedimiento electrónico, el legislador trabajó en la unificación normativa dando como resultado la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, la cual incorpora una referencia expresa al Esquema Nacional de Seguridad en su artículo 156: "El Esquema Nacional de Seguridad 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". Como culmen de la evolución legislativa, el Real Decreto 3/2010, viene a ser modificado por el Real Decreto 311/2022.

En consecuencia, esto implica que 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, incluyendo aquellos que son prestados por entidades externas.

Por tanto, debemos entender la seguridad como un todo completo y transversal, considerando el impacto de los servicios públicos y de los procesos internos de este Ayuntamiento, en la privacidad y protección de datos de la ciudadanía, siendo preciso integrar la estricta normativa vigente -el Reglamento (UE) 2016/679, Reglamento General de Protección de Datos- RGPD-, con los requisitos y principios de seguridad de Real Decreto 311/2022.

BOPSO-109-18092024

Visto todo lo anterior, se debe considerar que el Esquema Nacional de Seguridad será aplicado a los sistemas de información de este Ayuntamiento, para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados. Por tanto, los diferentes departamentos deben cerciorarse de que la seguridad 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, sin obviar la privacidad por defecto y responsabilidad proactiva. Los requisitos de seguridad y las inversiones y costes necesarios para adecuar nuestros sistemas a la normativa, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, en la gestión de proveedor conforme a lo establecido en el Decreto 311/2022 y Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Este Ayuntamiento debe poner en marcha en toda su actividad, los principios básicos y requisitos mínimos, y desarrollar una implementación de las medidas operativas y de protección de los sistemas, promoviendo la cultura de seguridad desde las posiciones más altas hacia los últimos eslabones. Se considerará que el sistema está compuesto por los elementos considerados por el propio Esquema Nacional de Seguridad; hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros.

El Ayuntamiento de Soria, adoptando estos principios declara;

- Que la seguridad será un elemento integrado en los sistemas y servicios de la entidad, y se asegurará y se mantendrá la adecuada confidencialidad, integridad y disponibilidad de dichos activos de información, y se considerarán, igualmente, las dimensiones de autenticidad y trazabilidad.
- Que se aprueba y publica la presente política como elemento vertebrador y que consagra la Política de Seguridad del Ayuntamiento y que se establecerán políticas de seguridad, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios y terceros impactados.
- Que se adoptarán las medidas necesarias para proteger los activos de los sistemas de información frente a accesos no autorizados, modificaciones, comunicaciones o destrucciones, ya sean intencionadas o fortuitas, controlándose los accesos y generando una segregación adecuada.
- Que se mantendrá una monitorización adecuada y un seguimiento de la seguridad para lograr una evolución de la seguridad y una mejora del sistema.
- Que se mantendrá como elemento transversal en la seguridad, el principio de privacidad y protección de datos sobre los interesados afectados.

La Seguridad como proceso integral

Se implanta una estrategia para garantizar la seguridad del sistema y de los servicios y la información que lo sustentan, lo que implica necesariamente que todos los recursos deben disponer y aplicar las medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Prevención

El Ayuntamiento de Soria debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará

BOPSO-109-18092024

las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se establecen como medidas:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del Esquema Nacional De Seguridad.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del Esquema Nacional de Seguridad. 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.

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Respuesta

El Ayuntamiento de Soria:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras áreas o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente.

Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, el Ayuntamiento de Soria dispondrá de los medios y técnicas necesarias que permitan garantizar la recuperación de los servicios más críticos.

Ámbito de Aplicación

Considerando la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ámbito subjetivo de aplicación del Real Decreto 311/2022 se determinará atendiendo a lo recogido en el apartado segundo del artículo 156. Considerando el artículo 2 de la Ley 40/2015, esta administración queda obligada como entidad que integra la Administración Local, en sus relaciones ad intra (relaciones con otros componentes del sector público) y ad extra (con la ciudadanía y sector privado).

La presente Política, será de aplicación a todo el sistema de información, dirigido al ejercicio de las competencias que como Administración nos son declaradas, quedando afectado todo el

BOPSO-109-18092024

personal de la corporación y también a terceros que accedan al sistema o presten servicios a este Ayuntamiento y que están impactados por el Real Decreto 311/2022.

Quedan expresamente incluidos los procesos, tanto internos como externos, que sean necesarios para desarrollar y cumplir con las funciones públicas encomendadas.

Quedan afectados, todos los activos propiedad del Ayuntamiento implicados en el sistema de información, o en régimen de uso y que afecten de cualquier modo al mismo, considerándose en cualquier momento del ciclo de vida del sistema.

Quedan considerados como activos, todos los elementos que, en relación con la información tratada o servicios prestados, puedan ser directa o indirectamente atacados. Estos elementos por declaración directa del Anexo II del Esquema Nacional de Seguridad serán, hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros.

Se consideran incluidos como alcance de la presente política, los trámites y carpetas electrónicas del Ayuntamiento de Soria:

a) Todos los servicios electrónicos suministrados a la ciudadanía por este Ayuntamiento a través de su sede electrónica.
b) Las relaciones con otras administraciones e interconexiones con sistemas públicos.
c) La gestión de los derechos de la ciudadanía con este Ayuntamiento por medios electrónicos.
d) La gestión de la hacienda pública local.
e) Uso de los medios de identificación y firma electrónica de los interesados en el procedimiento administrativo, incluyendo su representación y los registros electrónicos de apoderamientos.
f) Acciones de Gobierno Abierto y cumplimiento del principio de transparencia pública.

Declaración de la Política de Seguridad de la Información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios del Ayuntamiento de Soria.

Es la política de esta entidad asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad e integridad, y en su caso mantienen las dimensiones de trazabilidad y autenticidad.
- La información está protegida contra accesos no autorizados.
- Su cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- Se establece la seguridad como función diferenciada, con responsable de información, responsable de servicio, responsable de seguridad y responsable del sistema.
- Cada usuario implicado en el sistema, y específicamente el personal empleado, es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- El Ayuntamiento de Soria implementa, mantiene y realiza un seguimiento, 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.

La Política será aprobada por el Órgano Superior Administración Local y difundida para que la conozcan todas las partes afectadas.

BOPSO-109-18092024

Marco normativo

Según la legislación vigente, las principales normas aplicables al Ayuntamiento de Soria en materia de Seguridad de la Información son:

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos o Instrucción Técnica de Seguridad (ITS) de Notificación de Incidentes de Seguridad.
- Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad de los Sistemas de Información.
- Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.
- Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 (Directiva NIS).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- R.D. 311/2022 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- R.D. 1720/2007 Reglamento que desarrolla la Ley de protección de datos, en aquello que no resulte contrario al RGPD.
- Ley 59/2003 de Firma Electrónica.
- R.D. 281/2003 Reglamento Registro General de la Propiedad Intelectual.
- Ley 34/2002 Servicios de la Sociedad de la Información y Comercio Electrónico.
- Ley 15/1999 Protección de Datos de Carácter Personal, en aquellos puntos que pudieran mantenerse en vigor.
- R.D.L. 1/1996 Ley de la Propiedad Intelectual.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

El Ayuntamiento de Soria, mantendrá un listado complementando el presente. El Ayuntamiento de Soria cumple con la legislación citada y con todos sus requisitos.

BOPSO-109-18092024

Organización e implantación del proceso de Seguridad

Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información. De los integrantes del Comité de Seguridad se designará un Responsable de Seguridad y del Sistema.

Estará formado por un Presidente, un Secretario y un numero de vocales impares.

El Comité de Seguridad estará formado por el Responsable de Seguridad de la Información, el Responsable del Sistema y los Responsables de Información y Servicios. Formará parte del comité la persona que ostente las funciones de alcaldía o en su caso, por delegación, la persona que, ostentando cargo de concejalía, lo haga respecto a las competencias de innovación y administración digital. Formará parte del comité, además, el Delegado de Protección de Datos.

Podrán ser miembros invitados del comité asesores externos, para asesorar en materia de seguridad, tecnología, infraestructura, legalidad y cumplimiento.

La composición del Comité de Seguridad será la siguiente:

- Presidencia del Comité: Alcaldía o concejalía delegada
- Secretaria: Entre los integrantes del Comité
- Responsable de Seguridad: Designado entre los integrantes del Comité
- Responsable de Sistemas: Designado entre los integrantes del Comité
- Responsable de la Información: Designado entre los integrantes del Comité
- Delegado de Protección de Datos: Figura externa.
- Vocales con voz y voto: Representante de los Responsables de Servicios (Interventor), así como integrantes restantes del comité que puedan ser convocados.
- Invitados con voz y sin voto: Asesores externos.

El Comité de Seguridad reportará directamente al Órgano Superior Administración Local.

Son funciones del comité:

- Establecer los mecanismos de cooperación y coordinación en el Ayuntamiento de Soria en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información al Pleno.
- Promover la mejora continua de la gestión de la seguridad de la información.
- Elaborar la estrategia de evolución del Ayuntamiento de Soria en lo que respecta a seguridad de la información.
- Valorar la información y los servicios, sometido al Esquema Nacional de Seguridad y sea este el responsable de categorizar los sistemas. En concreto, determinará los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad Esquema Nacional de Seguridad.
- 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.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Órgano Superior Administración Local.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.

BOPSO-109-18092024

- 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.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad y promover los procesos de certificación y declaración correspondientes.
- 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.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta de manera transversal en los proyectos municipales 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Velar por el cumplimiento de la normativa de aplicación legal.
- Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.

Convocatoria

El Comité de Seguridad podrá formar parte de otros Comités, pero será el responsable de coordinar, evaluar y proponer mejoras para la Seguridad de Información y Servicios.

El Comité de Seguridad será convocado, al menos una vez al año, o siempre que aparezcan incidentes de seguridad graves y específicamente cuando surjan nuevas necesidades de seguridad que requieran su convocatoria.

Las reuniones del Comité y sus puntos serán recogidas en actas, en las que se incluirán los acuerdos adoptados. El Comité será convocado por la Secretaría, al menos, una antelación de 5 días hábiles. Cualquier miembro del comité podrá solicitar a la Secretaría la convocatoria del Comité, previa presentación de los asuntos que requieren de la misma.

Para que el Comité se encuentre válidamente constituido, deberán estar presentes: la Presidencia y la Secretaría, el Responsable de Seguridad, el Responsable de la Información y el Responsable de Sistemas.

En cuanto a los Responsables de los Servicios, no es necesario que asistan todos a las reuniones del Comité, solamente es obligatoria la asistencia del Interventor en su representación. El Comité de Seguridad se reserva la potestad de convocar a cualquier Responsable de Servicio, si fuese necesario.

Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

BOPSO-109-18092024

- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

Esta función puede ser absorbida por el Comité.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

Esta función puede ser absorbida por el Comité.

Responsable del Sistema

El Comité de Seguridad será el encargado de designar a los responsables de la cadena de seguridad. Así pues, será competencia del mismo la designación del Responsable del Sistema.

Tendrán una vigencia de dos años, pudiendo ser reelegidos por periodos idénticos de manera indefinida, siempre que se mantengan las condiciones asociadas a los perfiles requeridos.

Perfil:

Persona con perfil que pueda comprender la ejecución y el desarrollo de las operaciones sobre el sistema y con conocimiento de las áreas y servicios públicos, desde una parcela más técnica y práctica y operativa, y que conozca la arquitectura de la organización y las tecnologías aplicadas.

Funciones:

- Su función es desarrollar las operaciones sobre el sistema que mantengan la plena seguridad.
- 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 acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado o es conocedor de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, previa consulta con el Comité y el Responsable de la Seguridad, antes de ser ejecutada o posteriormente cuando las afecciones pusieran en riesgo la integridad, disponibilidad, confidencialidad, autenticidad o trazabilidad del sistema.
- Llevar a cabo las funciones del administrador de la seguridad del sistema.

La organización podrá designar un ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA que dependerá del Responsable de Sistemas, y desarrollará las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- 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.
- 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.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

BOPSO-109-18092024

- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- 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.
- 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.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Responsable de Seguridad

El Comité de Seguridad será el encargado de designar a los responsables de la cadena de seguridad. Así pues, será competencia del mismo la designación del Responsable de Seguridad.

Tendrán una vigencia de dos años, pudiendo ser reelegidos por periodos idénticos de manera indefinida, siempre que se mantengan las condiciones asociadas a los perfiles requeridos.

Perfil

Persona con visión y conocimiento de las competencias públicas del Ayuntamiento en áreas desarrolladas para cumplir con los fines públicos, que pueda comprender los riesgos que afronta la entidad, alineando los requisitos de seguridad con los requisitos de sus servicios y competencias.

Funciones

- Su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que lo establecido se ha llevado a cabo.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar ejecuciones de análisis de riesgos, revisiones de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Validar los planes de continuidad.
- Gestionar las revisiones externas o internas del sistema, incluyendo la recogida de indicadores específicos.
- Gestionar los procesos de certificación.
- Elevar a las Direcciones de primer nivel la aprobación de cambios y otros requisitos del sistema.

Por razones de operatividad, el Responsable de Seguridad podrá considerar la delegación de funciones, en Responsables de Seguridad Delegados, debiendo realizar designaciones individuales con cada función encomendad. El Responsable de Seguridad mantendrá la responsabilidad final.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad, y tendrán una dependencia funcional directa del Responsable de la Seguridad, a quien reportarán actuaciones y medidas.

Datos de Carácter Personal

El Ayuntamiento de Soria trata datos de carácter personal. Todos los sistemas de información del Ayuntamiento de Soria se ajustarán a las exigencias de la normativa de protección de datos

BOPSO-109-18092024

en vigor. Los datos se tratarán de manera lícita, leal, transparente, con fines determinados y explícitos, legítimos sin ser usados para fines posteriores incompatibles. Serán datos adecuados, pertinentes y limitados, exactos y actualizados. Serán tratados durante el tiempo necesario garantizándose la seguridad de los mismos.

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

Desarrollo de la política de seguridad de la información

Seguridad de la gestión de personal

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Todo el personal relacionado con el sistema y con la información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, debiendo ser controlados y sus acciones supervisadas.

Cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

El usuario con acceso concedido al sistema, pueda o no desarrollar acciones, estará sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accederá al sistema sin estar previamente informado de este extremo.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

La responsabilidad será exigible mediante el procedimiento disciplinario, que, como las pautas de seguridad, conocerá previamente el usuario. Este procedimiento estará alineado con la normativa de función pública o en su caso, de normativa laboral.

Autorización y control de los accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas

BOPSO-109-18092024

y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones o a la información del Ayuntamiento de Soria deberá ir siempre acompañado por un miembro responsable del Ayuntamiento de Soria que controlará en todo momento que la seguridad de los recursos está garantizada.

Protección de las instalaciones

Para que una seguridad lógica sea efectiva es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

El Ayuntamiento de Soria toma las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones y cuenta con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Gestión basada en procedimientos

La seguridad del sistema se documentará mediante procedimiento de operación que serán puestos a disposición de los usuarios implicados en el mismo. Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados. Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudieran tener el sistema. Estas podrán tener forma de procedimiento general o especificaciones técnicas acordes a los operadores del sistema y de la seguridad.

La cadena de suministro será controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Las redes serán gestionadas. Se incluirá cuando sea necesario, el cifrado o el control de comunicaciones.

Adquisición de productos de seguridad y contratación de servicios de seguridad

El Ayuntamiento de Soria tendrá en cuenta, para la adquisición de productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

Mínimo privilegio

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. 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.

Se considera la seguridad desde el diseño y por defecto. Se considera la privacidad desde el diseño y por defecto. Cuando existiera un Delegado de Protección de Datos, este será incluido siempre en la etapa más temprana del diseño y desarrollo de sistemas de información, cambios en la arquitectura o infraestructura, desarrollo de aplicaciones o herramientas, o líneas de negocio-actividades.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

El uso del sistema será sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

BOPSO-109-18092024

Para mantener el proceso de seguridad integral, se realizará una clasificación de la información-, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. La clasificación conllevará necesariamente una política de etiquetado y manipulación. La información personal estará integrada en el sistema y será categorizada.

Se deberá conocer en todo momento el estado de seguridad del sistema o de sus componentes, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

Gestión de comunicaciones y operaciones

El Ayuntamiento de Soria controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios.

Para evitar un uso malicioso de la red existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo con estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Por tanto, los datos serán guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente. Si la información se guarda en el disco duro de un PC, el usuario asignado a dicho PC es el responsable de realizar las copias de seguridad. Estas copias estarán claramente identificadas y se guardarán en sitio seguro.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de Soria implementará mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Se desarrollarán procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias del Ayuntamiento de Soria. De igual modo, se implementarán mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren los documentos, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

Prevención ante otros sistemas de información interconectados

El Ayuntamiento de Soria ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

BOPSO-109-18092024

Registro de actividad y detección de código dañino

El Ayuntamiento de Soria habilitará registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Todo ello con la finalidad exclusiva de lograr el cumplimiento del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

En concreto, el Ayuntamiento dispondrá de una solución integral de antivirus, tanto en puestos de trabajo como en servidores, que incorpore funcionalidades de EPDR (servicio de prevención, detección y respuesta de endpoints; primera línea de defensa en los puestos del Ayuntamiento, basada en la prevención y se complementa la protección, detectando código dañino, incorporando mecanismos de respuesta así como medidas para revertir los daños) y de integración con los cortafuegos perimetrales, para bloqueo de funcionalidades en caso de detección de amenazas.

Incidentes de seguridad

Cualquier persona que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Terceras partes

Cuando el Ayuntamiento de Soria 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Soria 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 de Seguridad de la Información 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.

BOPSO-109-18092024

Control del cumplimiento

La presente Política, una vez aprobada será dada a conocer a todo el personal del Ayuntamiento, y también a aquellos externos a los que sea de aplicación, y en la medida en que también es aplicable a los proveedores y colaboradores externos.

Vigencia

Esta política será efectiva desde la fecha de su aprobación y hasta que sea reemplazada por una nueva versión.

A partir de la fecha de entrada en vigor, quedarán derogadas todas las Políticas o normas anteriores que sobre la materia regulada en ella pudiesen contravenirla.

Soria, 16 de septiembre de 2024. – El Alcalde, Carlos Martínez Mínguez 1830

BOPSO-109-18092024