

ADMINISTRACIÓN LOCAL

Ayuntamiento de Castro del Río

Núm. 132/2023

Gex 486/2023.

Asunto: Actualización de la Política de Seguridad de la Información al nuevo RD 311/2022, de 3 de mayo, que aprueba el Esquema Nacional de Seguridad.

Por Resolución de Alcaldía, de fecha 18/01/2023, se actualiza la Política de Seguridad de la Información al nuevo RD 311/2022, de 3 de mayo, que aprueba el Esquema Nacional de Seguridad en los términos que se recogen a continuación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN AYUNTAMIENTO DE CASTRO DEL RÍO Y SU SECTOR PÚBLICO INSTITUCIONAL

1. OBJETO

Los ciudadanos confían en que los servicios disponibles por medios electrónicos se presten en unas condiciones de seguridad equivalentes a las que se encuentran cuando se acercan personalmente a las oficinas de la Administración. Además, buena parte de la información contenida en los sistemas de información de las AA.PP. y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

En su empeño por garantizar que estos servicios cuenten con las máximas garantías en materia de seguridad, la Excm. Diputación Provincial de Córdoba desarrolla esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por el ENS en lo referente a:

- A. Organización e implantación del proceso de seguridad.
- B. Análisis y gestión de los riesgos.
- C. Gestión de personal.
- D. Profesionalidad.
- E. Autorización y control de los accesos.
- F. Protección de las instalaciones.
- G. Adquisición de productos de seguridad y contratación de servicios de seguridad.
- H. Mínimo privilegio.
- I. Integridad y actualización del sistema.
- J. Protección de la información almacenada y en tránsito.
- K. Prevención ante otros sistemas de información interconectados.
- L. Registro de la actividad y detección de código dañino.
- M. Incidentes de seguridad.

Por todo lo anteriormente expuesto, el Ayuntamiento de Castro del Río y su sector público institucional aprueba la siguiente Política de Seguridad y debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante, ENS), regulado en el Real Decreto 311/2022, de 3 de mayo, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Para que conste el compromiso del Ayuntamiento de Castro del Río hace pública su misión, visión y valores en materia de seguridad de la información.

Para que todo el personal y usuarios sean conscientes de las

obligaciones, normativas y procedimientos en materia de seguridad de la información, esta política y la normativa de seguridad estará a disposición de todos los usuarios autorizados en el portal del empleado o en la intranet corporativa.

Misión:

La gestión y el buen gobierno del municipio, dando respuestas a las necesidades y expectativas de los ciudadanos a través de la prestación de servicios de calidad y garantizando en todo momento la seguridad de la información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción).

Visión:

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

Las diferentes áreas y servicios han de cerciorarse de que la seguridad de la información es una parte vital de los servicios públicos prestados por el Ayuntamiento de Castro del Río y su sector público institucional atendiendo a los principios básicos que rige el Esquema Nacional de Seguridad.

Valores:

Las áreas y servicios del Ayuntamiento de Castro del Río y su sector público institucional entienden la seguridad de la información como un valor que orienta la conducta de las personas hacia las buenas prácticas de seguridad por lo que deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando así la continuidad en la prestación de los servicios con una calidad y seguridad adecuada.

2. ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios, empleados internos y externos del Ayuntamiento de Castro del Río y su sector público institucional cualquiera que sea su clasificación jerárquica. Igualmente, aplica a todos los sistemas de la información e infraestructuras de comunicación utilizadas para la realización de las funciones propias de las distintas entidades.

3. MARCO NORMATIVO

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece principios y derechos relativos a la seguridad en relación con el derecho de los ciudadanos a comunicarse con las AA.PP. a través de medios electrónicos; y su artículo 42 crea el Esquema Nacional de Seguridad. Aún estando derogada establece los principios de la seguridad de la información en la administración electrónica.

El Esquema Nacional de Seguridad (ENS), regulado inicialmente por el Real Decreto 3/2010, de 8 de enero, y posteriormente por su actualización por Real Decreto 311/2022, de 3 de mayo, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. Las normas técnicas complementarias de interoperabilidad desarrollan ciertos aspectos

tos técnicos.

Las Leyes 39/2015 y 40/2015 regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

La Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen (LRBRL) de aplicación a la administración local.

La Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía (LAULA).

Asimismo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, además de garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Reglamento (EU) 679/2016, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos establece la obligación de disponer medidas técnicas y organizativas para garantizar la confidencialidad, disponibilidad e integridad de la información. Asimismo dispone que dichas medidas han de ser proactivas y el responsable del tratamiento ha de ser capaz de demostrar que se siguen esas medidas y demostrar su aplicación.

La Ley de Seguridad de las Redes y Sistemas de la Información aprobada mediante Real Decreto-Ley 12/2018, de 7 de septiembre, que transpone al ordenamiento jurídico español la directiva europea sobre la materia, la conocida como Directiva NIS que establece un marco común de seguridad en la Red en toda la UE y refuerza las medidas de protección en el entorno virtual. Afecta, por un lado, a los operadores de servicios esenciales; es decir, aquellos necesarios «para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas, que dependan para su provisión de redes y sistemas de información», según la definición que recoge la propia norma; y por extensión, las infraestructuras críticas también verán incrementada su seguridad de la información. Establece la obligación de que las empresas notifiquen los incidentes de ciberseguridad. Los operadores de servicios esenciales tendrán que designar a una persona como responsable de la seguridad de la información para que ejerza las funciones de punto de contacto y coordinación con las autoridades competentes y CSIRT (equipos de respuesta a incidentes de seguridad) de referencia.

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Tiene como finalidad desarrollar la Directiva NIS, aprobada en 2018, en cuanto al marco institucional en la materia, la cooperación y coordinación, la gestión y notificación de incidentes, las medidas a implementar, la supervisión de los requisitos de ciberseguridad o la función del CI-SO.

4. ORGANIZACIÓN DE SEGURIDAD

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

-Responsable de la Información: Determina la información tra-

tada. Es habitualmente una persona que ocupa un cargo de responsabilidad en la organización. Este cargo asume la responsabilidad del uso que se haga de la información y, por tanto, de su protección. El Responsable de la Información es el responsable de cualquier error o negligencia que lleve a un incidente.

-Responsable del Servicio: Es el encargado de establecer los requisitos del servicio en materia de seguridad. Puede ser una persona concreta o puede ser un órgano corporativo.

-Responsable de Seguridad: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Asimismo, la Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad: Responsabilidades y Funciones propone que estas responsabilidades se instrumenten por medio de comités, haciendo referencia concretamente al Comité de Seguridad de la Información que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.

Para gestionar y coordinar proactivamente la seguridad de la información se constituye, como órgano de gestión, el Comité de Seguridad de la Información del Ayuntamiento de de Castro del Río y de su sector público institucional formado por los siguientes cargos:

-Responsable de la información que recae en la persona del Alcalde/sa como máxima autoridad en el Ayuntamiento, el/la cual velará por el adecuado tratamiento y custodia de la información, tendrá potestad de aprobar los requisitos de una información en materia de seguridad y tendrá capacidad ejecutiva para aprobar, planificar y trasladar estas necesidades al Pleno del Ayuntamiento y extensivo a su sector público institucional. Podrá convocar las reuniones del Comité. Será responsable directo de la ejecución de las medidas adoptadas por el comité y su seguimiento.

-Responsable de Seguridad de la Información que recae en la persona del concejal responsable de nuevas tecnologías o persona en quien este delegue, que será el encargado de coordinar y controlar las medidas que se definan por el Comité de Seguridad y se coordinará en sus funciones con el Responsable de Seguridad de la Información del propio Comité de Seguridad de la Información del Ayuntamiento.

Asesorará y tendrá potestad para determinar técnicamente los requisitos de seguridad de la información y de los servicios en materia de seguridad. Asimismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros del comité.

-Administrador de los sistemas de la información: Este cargo recaerá en la persona responsable del área de Informática del ayuntamiento y será miembro de este comité. Tendrán la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar coordinadamente al Responsable de la Información del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad y de la Seguridad de los sistemas de la información.

-Responsable del Servicio: Este cargo recaerá en la persona del Alcalde/sa como máxima autoridad en el ayuntamiento. Es el encargado de establecer los requisitos del servicio en materia de seguridad.

-Responsables de Entidades del Sector Público Institucional: Serán las personas responsables de los servicios o de la explotación de las distintas instituciones que establecen los requisitos, fines y medios para la realización de las tareas en las distintas instituciones. Además, tendrán la responsabilidad legal de vigilar el cumplimiento de las normas de seguridad dentro de su institución

e informar al Responsable de la Información del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

-Secretaría: Tendrá la obligación de supervisar que los procedimientos aprobados por el comité se ajusten a derecho y asesorar al Comité en esta materia. Además, levantará acta de las reuniones y seguirá las directrices que marque el Comité de Seguridad de la Información.

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

4.1 FUNCIONES DEL COMITÉ DE SEGURIDAD

Sus funciones son las siguientes:

-Responsabilidades derivadas del tratamiento de datos de carácter personal.

-Atender las inquietudes de la Corporación y de las diferentes áreas.

-Informar regularmente del estado de la seguridad de la información a la Junta de Gobierno.

-Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.

-Elaborar la estrategia de evolución del Ayuntamiento y su Sector Público Institucional en lo que respecta a la seguridad de la información.

-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 Comité de Seguridad.

-Aprobar la normativa de seguridad de la información.

-Ser informado sobre los procedimientos de Seguridad de la información de los integrantes del sector público institucional los cuales tienen obligación de tener.

-Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.

-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 por la empresa y recomendar posibles actuaciones respecto de ellos.

-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 auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

-Aprobar planes de mejora de la seguridad de la información de la empresa. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

-Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

-Establecer medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información.

-En caso de ocurrencia de incidentes de seguridad de la infor-

mación aprobará el Plan de Mejora de la Seguridad.

Para su asesoramiento técnico el ayuntamiento se apoyará en el Comité de Seguridad de la Información de la Diputación de Córdoba y de su sector público institucional y en las Políticas, Normativas y demás documentación aprobadas por el mismo.

Resolución de conflictos:

El Comité de Seguridad de la Información, se encargará de resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización. En caso de que el Comité no tuviera capacidad o autoridad para la resolución de determinados conflictos, lo elevará a Presidencia para su resolución.

5. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en la entidad (empleados, proveedores y subcontratistas), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS. Esta documentación estará permanentemente accesible a través de los medios que el Ayuntamiento de Castro del Río estime convenientes.

6. CONCIENCIACIÓN

El Ayuntamiento de Castro del Río establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad de la Información de Diputación, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo a esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad.

El Responsable de Información del Ayuntamiento en coordinación con el Comité de Seguridad, establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

7. GESTIÓN DEL RIESGO

El Ayuntamiento de Castro del Río realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgo, siguiendo las directrices expuestas por el ENS en su artículo 7, de modo que se puedan anticipar los riesgos existentes. Este análisis de riesgo y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el comité desarrollará un procedimiento de Análisis de Riesgos y Evaluación de Impacto Potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad del análisis y cuándo se realizará de modo excepcional.

8. COMPETENCIA PARA LA APROBACIÓN DE LAS POLÍTICAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

La competencia para la aprobación de las políticas, normas y procedimientos de Seguridad se estructurará de la siguiente for-

ma:

Política de Seguridad de la Información y Política de Protección de Datos: Serían aprobadas por el Pleno del Ayuntamiento de Castro del Río:

-Normativa de Seguridad de la Información: Tanto el Ayuntamiento de Castro del Río como todo el Sector Público Institucional propondrá su propia Normativa de Seguridad (ratificada por su presidente/órgano rector) y esta será luego aprobada/ratificada por el Comité de Seguridad en la siguiente reunión del mismo.

-Procedimientos de Seguridad de la Información: Tanto el Ayuntamiento de Castro del Río como todo el Sector Público Institucional aprobará sus propios procedimientos de Seguridad de la información (aprobados por el responsable de la entidad) e informará de su aprobación al Comité de Seguridad en la siguiente reunión del mismo.

Toda esta documentación deberá ser publicada en cada uno de los portales de información de cada entidad para general conocimiento de todo el personal.

9. PROTECCIÓN DE DATOS PERSONALES

El Ayuntamiento de Castro del Río únicamente recogerá datos personales cuando sean adecuados, pertinentes y no excesivos, y estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas técnicas y organizativas pertinentes para el cumplimiento de la legislación en materia de protección de datos.

Estas medidas, tal y como se indica en la disposición adicional primera de la Ley 3/2018, de 5 de diciembre, sobre Protección de Datos y Garantía de Derechos Digitales, se corresponderán con las descritas en el Esquema Nacional de Seguridad, que estarán definidas en las políticas, normativas y procedimientos que correspondan.

10. GESTIÓN DEL RIESGO

El Ayuntamiento de Castro del Río y su Sector Público Institucional realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgo, siguiendo las directrices expuestas por el ENS en su artículo 6, de modo que se puedan anticipar los riesgos existentes. Este análisis de riesgo y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el Comité desarrollará un procedimiento de Análisis de Riesgos y Evaluación de Impacto Potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad

del análisis y cuándo se realizará de modo excepcional.

El análisis de riesgos que realice el Ayuntamiento de Castro del Río atenderá igualmente y de manera concreta a aquellos que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.

11. TERCERAS PARTES

Cuando el Ayuntamiento de Castro del Río y su Sector Público Institucional preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Castro del Río y su Sector Público Institucional utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad 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.

12. REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso del Ayuntamiento de Castro del Río con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad para adaptarse a cambios en el entorno legislativo, técnico u organizativo.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del órgano competente.

Castro del Río, 18 de enero de 2023. Firmado electrónicamente por el Alcalde-Presidente, Julio José Criado Gámiz.