Calahorra
Ayuntamiento

72778711H
MARÍA BELÉN
REVILLA (R:
P2603600D)

Firmado digitalmente por 72778711H MARÍA BELÉN REVILLA (R: P2603600D)
Motivo: DILIGENCIA.- La extiendo yo, la Secretaria, para hacer constar que el presente documento ha sido aprobado por Decreto de Alcaldia de 17 de mayo de 2023(expediente 6/2023/SE-GNL). Doy fe.
Fecha: 2023.05.19 13:19:50 +02'00'

Política de Seguridad de la Información del Ayuntamiento de Calahorra

Documento aprobado por Resolución de Alcaldía nº 1.115 de 17 de mayo de 2023.

ens
Esquema Nacional de
Seguridad

ÍNDICE

1.- Aprobación y entrada en vigor 3
2.- Introducción 3
3.- Misión y objetivos de la Política de Seguridad del Ayuntamiento de Calahorra 3
4.- Alcance 3
5.- Marco normativo 4
6.- Cumplimiento de los requisitos mínimos de seguridad 6
6.1.- La seguridad como un proceso integral y mínimo privilegio 6
6.2.- Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad 7
6.3.- Gestión de personal y profesionalidad 7
6.4.- Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos 8
6.5.- Incidentes de seguridad, prevención, detección, reacción y recuperación 8
6.6.- Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados 8
6.7.- Diferenciación de responsabilidades, organización e implantación del proceso de seguridad 9
6.8.- Autorización y control de los accesos 9
6.9.- Protección de las instalaciones 9
6.10.- Adquisición de productos de seguridad y contratación de servicios de seguridad 9
6.11.- Protección de la información almacenada y en tránsito y continuidad de la actividad 9
6.12.- Registro de actividad y detección de código dañino 10
6.13.- Infraestructuras y servicios comunes 10
6.14.- Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras 10
6.15.- Revisión de la política 11
7.- Modelo de gobernanza 11
7.1.- Roles o perfiles de seguridad 11
7.1.1.- Responsabilidades asociadas al Esquema Nacional de Seguridad 11
7.1.1.1- Funciones del Responsable de la Información 11
7.1.1.2.- Funciones del Responsable del servicio 12
7.1.1.3.- Funciones del Responsable de seguridad 12
7.1.1.4.- Funciones del Responsable del sistema 13
7.2.- Comité de Seguridad de la Información 13
7.2.1.- Composición del Comité de Seguridad 13
7.2.2.- Funciones del Comité de Seguridad de la Información 14
7.3.- Procedimientos de designación 14
7.4.- Resolución de conflictos 15
8.- Datos de carácter personal 15
9.- Instrumentos de desarrollo 15
10.- Terceras partes 15

1.- Aprobación y entrada en vigor

Texto aprobado el día 17 de mayo de 2023 por Resolución de Alcaldía del Ayuntamiento de Calahorra (nº 1.115).

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2.- Introducción

La información constituye un activo de primer orden para el Ayuntamiento de Calahorra, ya que resulta imprescindible para la prestación de los servicios públicos. Por su parte, las tecnologías de la información y las comunicaciones se han hecho imprescindibles para las administraciones públicas ya que contribuyen a la obtención, intercambio, tratamiento y almacenamiento de esa información.

Sin embargo, las mejoras que aportan las TIC al tratamiento de la información, vienen acompañadas de nuevos riesgos. Por esa razón es necesario introducir medidas específicas para proteger tanto la información, como los servicios que dependen de ella.

La seguridad de la información, tiene como objetivo proteger la información y los servicios, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable. El presente documento establece la Política de Seguridad de la Información del Ayuntamiento de Calahorra que constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Esquema Nacional de Seguridad.

Con ello se pretende lograr el alineamiento estratégico de la gestión de la seguridad de la información con las normas internacionales y las regulaciones legislativas existentes en la materia.

3.- Misión y objetivos de la Política de Seguridad del Ayuntamiento de Calahorra

El Ayuntamiento de Calahorra, para la gestión de sus intereses y de las funciones y competencias que tiene atribuidas en diferentes normas o convenios, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. Para ello pone a disposición de esta la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

4.- Alcance

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Calahorra, que están relacionados con el ejercicio de derechos por medios electrónicos, con el

cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

5.- Marco normativo

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Calahorra, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- 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.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- 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 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).
- Decreto 4/2023, de 15 de febrero, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja.
- Resolución 394/2021, de 16 de marzo, de la Consejería de Hacienda y Administración Pública, por la que se aprueba la política de firma electrónica y certificados de la Administración General y del sector público, de la Comunidad Autónoma de La Rioja.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Calahorra, derivadas de las anteriores y

publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política, entre otras.

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento de Calahorra, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el Real Decreto.

Así mismo, el Ayuntamiento de Calahorra, también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6.- Cumplimiento de los requisitos mínimos de seguridad

El Ayuntamiento de Calahorra, para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

6.1.- La seguridad como un proceso integral y mínimo privilegio

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

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

6.2.- Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento de Calahorra permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

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

6.3.- Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información del Ayuntamiento de Calahorra, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

6.4.- Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del Real Decreto 311/2022, de 3 de mayo, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

6.5.- Incidentes de seguridad, prevención, detección, reacción y recuperación

El Ayuntamiento de Calahorra, dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del Real Decreto 311/2022, de 3 de mayo, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

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

6.6.- Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento de Calahorra, mantendrá actualizada una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa sea comprometida permita desarrollar una reacción adecuada frente a los incidentes que no

han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

6.7.- Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento de Calahorra, organizará su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "MODELO DE GOBERNANZA" del presente documento.

6.8.- Autorización y control de los accesos

El Ayuntamiento de Calahorra, implementará mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

6.9.- Protección de las instalaciones

El Ayuntamiento de Calahorra, implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

6.10.- Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento de Calahorra, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

6.11.- Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de Calahorra, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

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

6.12.- Registro de actividad y detección de código dañino

El Ayuntamiento de Calahorra, con el propósito de satisfacer el objeto de este real decreto, 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, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá 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 una determinada actividad.

6.13.- Infraestructuras y servicios comunes

El Ayuntamiento de Calahorra, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

6.14.- Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento de Calahorra, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

6.15.- Revisión de la política

La revisión de la Política deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión del Ayuntamiento de Calahorra en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

En relación a las revisiones que puedan realizarse sobre la redacción del texto que constituye la Política, se distinguirán tres tipos de actividades:

- **Revisiones periódicas**, que se realizarán, **al menos, con una periodicidad anual.**
- **Revisiones sistemáticas**: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política.
- **Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual** o que haya causado un impacto en la seguridad de la información del Ayuntamiento de Calahorra.

7.- Modelo de gobernanza

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en el Ayuntamiento de Calahorra, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

7.1.- Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- **Responsable de Información:** Secretaria General
- **Responsable de los Servicios:** Concejal delegado responsable de al área de Informática o Tecnologías de la Información o Digitalización del Ayuntamiento de Calahorra
- **Responsable de Seguridad:** Técnico de Digitalización
- **Responsable del Sistema:** Coordinador de Informática.

7.1.1.- Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS.

7.1.1.1- Funciones del Responsable de la Información

El Responsable de la Información será designado por decreto de alcaldía por un periodo de 4 años. A tal efecto:

a) Determinará los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que él es responsable.
b) Valorará, para cada información contemplada en el análisis de riesgos, las diferentes dimensiones de la seguridad.

c) Aceptará los riesgos residuales, calculados en el análisis de riesgos respecto de la información.
d) Realizará el seguimiento y control de los riesgos con la ayuda del Responsable de Seguridad.

7.1.1.2.- Funciones del Responsable del servicio

El Responsable del Servicio será designado por decreto de alcaldía por un periodo de 4 años. A tal efecto:

a) Realizará, junto a los Responsables de la Información y el Responsable de Seguridad, los preceptivos análisis de riesgos y seleccionarán las salvaguardas que se han de implantar.
b) Aceptará los riesgos residuales, respecto de la información, calculados en el análisis de riesgos.
c) Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.
d) Suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

7.1.1.3.- Funciones del Responsable de seguridad

El Responsable de Seguridad será designado por decreto de alcaldía por un periodo de 4 años.

Tendrá las siguientes funciones:

a) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
c) Impulsar el cumplimiento del cuerpo normativo definido en el apartado 3, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.
d) Mantener un inventario actualizado de las normas de primer y segundo nivel detalladas en el apartado 8, de los nombramientos derivados de la presente orden, así como de los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.
e) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
f) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.
g) Promover la mejora continua en la gestión de la seguridad de la información.
h) Impulsar la formación y concienciación en materia de seguridad de la información.
i) Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
j) Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.
k) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría,

elaborando las conclusiones a presentar a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

l) Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, asigne a los responsables de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse «responsables de seguridad delegados», dependientes funcionalmente del responsable principal, que serán responsables de las actuaciones que se les deleguen.

7.1.1.4.- Funciones del Responsable del sistema

El Responsable del Sistema, será designado por decreto de alcaldía por un periodo de 4 años. Será el titular del órgano con competencias en materia de sistemas y tecnologías de la información, y tiene las siguientes funciones:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
d) Colaborar en la investigación y resolución de incidentes de seguridad.
e) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, el responsable del Sistema podrá designar «responsables de sistema delegados», dependientes funcionalmente del responsable principal, que se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. El responsable principal seguirá siendo el responsable final.

7.2.- Comité de Seguridad de la Información

7.2.1.- Composición del Comité de Seguridad

- **Presidente/a:** Concejal delegado responsable de al área de Informatica o Tecnologías de la Información o Digitalización del Ayuntamiento de Calahorra (Responsable de la Servicios).
- **Secretario/a:** Responsable de Seguridad.
- **Vocales:** Secretaria General (Responsable de los Información), Técnico responsable de la Agenda Digital municipal y un funcionario del área de informática (Responsable del Sistema), distinto del que asume funciones de Secretario/a.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

7.2.2.- Funciones del Comité de Seguridad de la Información

Al Comité de Seguridad de la Información del Ayuntamiento de Calahorra le corresponden funciones de asesoramiento, consultoría y propuesta en materia de seguridad de la información. Su constitución y la designación de sus miembros se realizará por el pleno del Ayuntamiento de Calahorra por un periodo de 4 años.

En particular le corresponde:

a) Informar regularmente del estado de la seguridad de la información al Ayuntamiento de Calahorra.
b) Promover la mejora continua del sistema de gestión de la seguridad de la información.
c) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
d) Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información, para que sea aprobada por el Ayuntamiento de Calahorra.
e) Proponer la aprobación de la normativa de seguridad de la información.
f) Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
g) Proponer planes de mejora de la seguridad de la información de la organización.
h) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información, que sea requerida tras el cese en la utilización del mismo.
i) Divulgar la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas.

El Comité de Seguridad de la Información del Ayuntamiento de Calahorra se reunirá, con carácter ordinario, una vez al semestre y podrá reunirse con carácter extraordinario en alguno de los siguientes supuestos:

a) A instancia del Presidente.
b) Cuando aparezcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad, que requieran la participación de los componentes del Comité.

El Comité de Seguridad de la Información, ajustará su funcionamiento a las previsiones relativas a los órganos colegiados contenidas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

7.3.- Procedimientos de designación

La constitución de los Responsables identificados en esta Política y la designación de sus miembros será realizada por Alcaldía del Ayuntamiento de Calahorra, y comunicada a las partes afectadas.

La designación del Comité de Seguridad de la Información será llevada a cabo por el pleno del Ayuntamiento de Calahorra, y comunicada a las partes afectadas.

Los roles de seguridad serán revisados cada cuatro años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

7.4.- Resolución de conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité de Seguridad de la Información.

8.- Datos de carácter personal

Cuando un sistema al que afecte el Esquema Nacional de Seguridad maneje datos de carácter personal le será de aplicación lo dispuesto en 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, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en lo que le afecte.

En desarrollo de los principios de la vigente normativa de protección de datos, entre otros, los de minimización, confidencialidad o proactividad, el Ayuntamiento ha definido un marco de actuación en la Política de Protección de Privacidad, que se puede consultar en https://calahorra.es/principal/politica-de-proteccion-de-datos/

9.- Instrumentos de desarrollo

El cumplimiento de los objetivos marcados en esta Política se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se definirá una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

10.- Terceras partes

Cuando el Ayuntamiento de Calahorra preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento de Calahorra, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Ayuntamiento lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de Calahorra, 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 ataña 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.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

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. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.