Asunto
RESOLUCIÓN DE MODIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE SIERO

Interesado

RESOLUCIÓN DE ALCALDÍA

En la reunión del Comité de Seguridad de la Información de este Ayuntamiento, celebrada con fecha 14 de febrero pasado, se acordó aprobar modificaciones al documento que contiene la política de seguridad municipal, al haberse producido desde su aprobación el 15 de noviembre de 2016, modificaciones legales relevantes que afectaban a dicha normativa.

No obstante, detectados algunos errores y omisiones como los que afectaban al Responsable Funcional de Tratamiento del Servicio de la Intervención Municipal, y a la omisión de determinadas leyes en el apartado 5 referido al "marco normativo", el Comité, en la reunión del pasado 29 de marzo acordó modificar dichos aspectos de la Política de Seguridad, y proceder a su publicación en la página Web.

En consecuencia, en el ejercicio de las atribuciones que me confiere el artículo 21 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

DECRETO:

Primero.- Aprobar el siguiente documento en el que se contiene la Política de Seguridad del Ayuntamiento de Siero tras las modificaciones acordadas:

1 OBJETIVO

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

2 ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Siero y sus organismos autónomos, que estén 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.

Todos los miembros del Ayuntamiento de Siero, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta "Política de Seguridad de la Información" y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

En adelante, cuando se haga referencia al Ayuntamiento de Siero, se entenderán incluidos sus organismos autónomos.

3 INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento de Siero, conocedor de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso "su propia Información" es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar 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 de los servicios prestados.

De este modo, todos los departamentos y/o áreas del Ayuntamiento de Siero, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte ntegral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

Por tanto, para el Ayuntamiento de Siero, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS. Para ello actuará en 4 direcciones fundamentales:

- **Prevención**: Para que la información o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de Siero implementará las medidas de seguridad establecidas por el Esquema Nacional de Seguridad (ENS), así como cualquier otro control adicional, que identifique como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados. Para garantizar el cumplimiento de la política, el Ayuntamiento de Siero se compromete formalmente a:
    - 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**: El Ayuntamiento de Siero establecerá controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS (reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.
- **Respuesta**: El Ayuntamiento de Siero establecerá las siguientes medidas:
    - Mecanismos para responder eficazmente a los incidentes de seguridad.
    - Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
    - Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

• **Recuperación**: Para garantizar la disponibilidad de los servicios, el Ayuntamiento de Siero dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

4 MISIÓN DEL AYUNTAMIENTO DE SIERO

El Ayuntamiento de Siero se compromete a poner a disposición de la ciudadanía la realización de trámites online con el objetivo de fomentar su relación electrónica con el Ayuntamiento, reduciendo así los tiempos de espera y de resolución de trámites solicitados. Asimismo pretende impulsar la participación en los asuntos públicos estableciendo, de este modo, nuevos cauces de comunicación entre los ciudadanos y la administración municipal, en tanto que más próxima.

5 MARCO NORMATIVO

El marco normativo en el que se desarrollan las actividades del Ayuntamiento de Siero, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, está integrado por las siguientes normas:

a) Real Decreto 3/2010 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.

b) Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

c) 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.

d) 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.

e) 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.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

f) 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.

g) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

h) Artículo 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

i) 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).

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

k) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

l) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

m) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

n) Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

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

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

q) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

r) 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.

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

t) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

u) Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

v) Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

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

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

y) Boletín Oficial del Principado de Asturias nº 275 de 27 de noviembre de 2009, por la que se aprueba la Ordenanza para la Administración Electrónica del Ayuntamiento de Siero.

Y por toda la demás legislación que resulte de aplicación, como la Ley de Patrimonio Histórico, de Protección de la Propiedad Intelectual etc.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Siero derivadas de las anteriores y publicadas en la sede electrónica comprendida dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad de la Información 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 "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Así mismo, el Comité 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 PRINCIPIOS Y REQUISITOS

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

El Ayuntamiento de Siero para lograr el cumplimiento de los artículos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado 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.

• Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) 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 emplazamientos o equipos, 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 no sean de interés, sean innecesarias e, incluso, aquellas inadecuadas al fin que se persigue.

d) 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.

• Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 20)

El Ayuntamiento de Siero ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

requerirán de una autorización formal. Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

- **Gestión de personal (artículo 14) y profesionalidad (artículo 15)**

Todos los miembros del Ayuntamiento de Siero, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Ayuntamiento de Siero, en particular al de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

- **Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)**

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y /o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información. 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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.

El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas. Las fases de este proceso se

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional. En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

- **Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)**

El Ayuntamiento de Siero ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de Siero implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

El Ayuntamiento de Siero establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Para garantizar la disponibilidad de los servicios, el Ayuntamiento de Siero dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

- **Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)**

El Ayuntamiento de Siero 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.

- **Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)**

El Ayuntamiento de Siero ha organizado su seguridad comprometiendo a todos los miembros de corporación, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

- **Autorización y control de los accesos (artículo 16)**

El Ayuntamiento de Siero ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

- **Protección de las instalaciones (artículo 17)**

El Ayuntamiento de Siero ha implementado mecanismo 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.

- **Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)**

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

El Ayuntamiento de Siero 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.

- **Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)**

El Ayuntamiento de Siero ha implementado mecanismos para proteger la información almacenado o en tránsito especialmente cuando esta 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.

También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias. De igual modo, se han implementado mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren, para garantizar que toda información en soporte no electrónico relacionada, estará protegida con el mismo grado de seguridad que la electrónica.

- **Registros de actividad (artículo 23)**

El Ayuntamiento de Siero ha habilitado 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 objeto del presente 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.

- **Mejora continua del proceso de seguridad (artículo 26)**

El Ayuntamiento de Siero actualizará y mejorará de forma continua el proceso de seguridad integral implantado, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

6.1 Organización de la Seguridad

La estructura organizativa de la Organización de la Seguridad de la Información en el Ayuntamiento de Siero es la siguiente:

6.1.1 Roles de Seguridad de la Información

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:

• **Persona delegada de Protección de Datos (DPD)**: Abogada Consistorial.

• **Responsables de la Información ENS y Responsables de los Servicios ENS. Responsables Funcionales de Tratamiento:**

1. Jefe de la Policía Local

2. Jefe del Servicio de Secretaría

3. Jefa de la Sección de Archivo

4. Coordinadora del área de Bienestar Social

5. Adjunta al Jefe del Servicio de Secretaría

6. Responsable del Servicio de Promoción Económica y Desarrollo Local

7. Responsable servicio asesoría de la Mujer

8. Director Mercado de Ganados

9. Responsable Oficina de Información al Consumidor

10. Jefa de la Sección de Contratación

11. Jefa de la Sección de Obras y Servicios

12. Jefe de la Sección de Patrimonio

13. Jefe del Servicio de Urbanismo

14. Jefa de la Sección de Planeamiento y Gestión

15. Jefa de la Sección de Licencias

16. Jefa de la Sección de Disciplina Urbanística

17. Jefa del Servicio de Tesorería

18. Jefa de la Sección de Tributos

19. Jefa del Servicio de Intervención

20. Responsable de Prevención y Riesgos Laborales

21. Jefe del Servicio de Obras y Arquitectura

22. Abogada Consistorial

23. Jefe Departamento TIC

24. Responsable del Servicio de Normalización Llingüística

25. Responsable de Selección de Personal

• **Responsable de Seguridad de la Información del ENS**. Funcionario que desempeña el puesto de Jefe de la Departamento TIC: D. Francisco Morís Martín.

• **Responsable del Sistema del ENS**: Técnico adscrito a la Departamento TIC: D. Jesús Estrada Luis.

6.1.2 Comité de Seguridad de la Información

Constituir el Comité de Seguridad de la Información, como órgano colegiado del Ayuntamiento de carácter consultivo, que estará formado por las siguientes personas:

¬ **Presidente**: Concejal delegado del área de Economía, Hacienda, Modernización y Administración Municipal, D. Alberto Pajares San Miguel.

¬ **Secretaria**: Adjunta al Jefe del Servicio de Secretaría, Dña. Lucía Prieto Fernández-Miranda.

¬ **Vocales:**

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

- Responsable de Seguridad de la Información ENS.
- Delegado de Protección de datos (DPD).
- Jefe del Servicio de Secretaría, en calidad de Asesor Jurídico.
- Responsable del Sistema ENS.

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

Para asegurar su imparcialidad, la Delegada de Protección de Datos y el Responsable del Sistema ENS, actuarán con voz y sin voto.

6.2 Responsabilidades asociadas al Comité de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad.

¬ Funciones del Responsable de la Información y de los Servicios:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información.
- Informar sobre los derechos de acceso al Servicio y a la Información.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Poner en comunicación del Responsable de Seguridad ENS, cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

¬ Funciones de Responsables Funcionales del Tratamiento:

- Velar por la adecuada realización de sus funciones, dentro del marco de seguridad adecuado, ayudando a difundir el conocimiento y la cultura de seguridad necesarias para el correcto tratamiento de los datos.
- Dar apoyo al Responsable del Tratamiento en la actualización del Registro de Actividad de Tratamiento RAT manejados en su área de responsabilidad, comunicándole cualquier alta, modificación o baja del Registro.

¬ Funciones del Responsable de Seguridad ENS:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

¬ **Las funciones del Responsable del Sistema ENS:**

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborando los procedimientos operativos necesarios.
- Definir la topología y la 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.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

6.3 Funciones del Delegado de Protección de Datos

Las funciones del Delegado de Protección de Datos (DPD), serán como mínimo:

¬ Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

¬ Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

¬ Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.

¬ Cooperar con la autoridad de control.

¬ Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

6.4 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

¬ Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas informando regularmente del estado de la Seguridad de la Información.

¬ Asesorar en materia de Seguridad de la Información.

¬ Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.

¬ Representar frente a terceros (entidades privadas y otras Administraciones Públicas) la figura de Responsables de la Información ENS y Responsables de los Servicios ENS. Responsables Funcionales de Tratamiento en acciones transversales.

¬ Promover la mejora continua del sistema de gestión de la Seguridad de la Información.

Para ello se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

6.5 Procedimientos de designación

Todos los nombramientos se revisarán cada cuatro años o con ocasión de vacante.

7 DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Siero solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

8 OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Siero, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del Ayuntamiento de Siero, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

9 GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

¬ Al menos una vez al año.
¬ Cuando cambien la información y/o los servicios manejados de manera significativa.
¬ Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.
2. Análisis de riesgos.
3. El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

10 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 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.

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 concejal competente por razón de la materia del Ayuntamiento de Siero.

11 TERCERAS PARTES

Cuando el Ayuntamiento de Siero 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 el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Siero utilice servicios de terceros o ceda información a terceros, se les hará partícipe 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 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 ENS que precise los riesgos en que se incurre y la forma de tratarlos.

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante."

Segundo.- La presente Resolución entrará en vigor el mismo día de su aprobación.

Tercero.- Comuníquese al Pleno de la Corporación y publíquese en la página web municipal.

Firmado digitalmente por:
El Alcalde de Siero
Ángel Antonio García González
09-04-2019 13:40

Plaza del Ayuntamiento s/n - Pola de Siero - Principado de Asturias - Tel.:985 725 424 - Fax:985 725 042 - CIF:P3306600B
Puede acceder al documento electrónico original a través de la Sede Electrónica del Ayuntamiento de Siero: sedeelectronica.ayto-siero.es