NO8DO
AYUNTAMIENTO DE SEVILLA

Área de Hacienda, Turismo, Participación Ciudadana y Transformación Digital
Dirección General de Transformación Digital
Servicio de Coordinación Ejecutiva de Modernización y Transparencia

Nº Expediente: 6/2024

A LA JUNTA DE GOBIERNO

El marco de la relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos, se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Por otra parte, el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha norma, estando constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada. Esta disposición ha sido desarrollada a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El Real Decreto 311/2022, de 3 de mayo, tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. La misma, define en su artículo 12 la política de seguridad de la información, como el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta, recogiendo en su apartado 2, la necesidad de que cada Administración Pública cuente con una política de seguridad formalmente aprobada por el órgano competente.

El Ayuntamiento de Sevilla, ya contaba con una política de seguridad, no obstante la trayectoria legislativa sufrida por el Esquema Nacional de Seguridad desde la anterior política y el avance en el uso de las tecnología por la ciudadanía hacen necesario adatar la Política de Seguridad de la Información a la nueva realidad.

Entre esta realidad se encuentra el ámbito de aplicación de la nueva Política de Seguridad de la Información, por cuanto mediante Acuerdo adoptado en Junta de Gobierno de fecha 27 de julio de 2018, se aprobó la Red Corporativa de Telecomunicaciones del ámbito municipal de Sevilla, denominada RED HISPALNET. De ahí la necesidad de aprobar la presente Política de seguridad, como un documento Transversal u horizontal aplicable a todos los Organismos Autónomos y Empresas municipales adheridas a la citada Red.

A través de este documento se pretende por un lado definir y regular la Política de seguridad de la información que se ha de aplicar a todas las entidades que integran la Red HISPALNET, así como establecer el reparto de funciones y responsabilidades en materia de seguridad de la información. Una vez aprobado este documento, todas y cada una de las Entidades que conforman la RED HISPALNET y conforme se establece en el presente documento, deberán redactar y aprobar su propia Política de Seguridad, en el plazo indicado, pero siempre respetando las indicaciones establecidas dentro del marco global reflejado en este documento.

El propio Real Decreto Decreto 311/2022, cuando habla de seguridad de sistemas lo hace con carácter general, refiriéndose a sistemas de información, extendiéndose

igualmente a los que contengan datos personales a los que les sea aplicable la normativa sobre protección de datos personales. De ahí que la presente Política de Seguridad de la información abarca tanto la Seguridad TIC como la de Protección de datos personales, estableciéndose también en este documento las funciones y responsabilidades tanto en materia de seguridad TIC como en materia de protección de datos.

Es por ello que en cumplimiento de la necesidad impuesta por el Real Decreto 311/2022, de 3 de mayo, de que se disponga en cada Administración Pública con una política de seguridad formalmente aprobada por el órgano competente y visto el informe emitido por el Servicio de Coordinación Ejecutiva de Modernización y Transparencia, y en uso de las facultades atribuidas por Resolución 546, de 20 de Junio de 2023, se propone la adopción de los siguientes

ACUERDOS

PRIMERO.- Aprobar la Política de seguridad de la Información de los Organismos que conforman la Red Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, que se adjunta al presente Acuerdo.

SEGUNDO.- Crear el Comité Director de Seguridad de la Información de la RED HISPALNET, recogido en el documento de Política de Seguridad de la Información de la RED HISPALNET, con las funciones, composición y funcionamiento que en el mismo se indican.

TERCERO.- Publicar la Política de seguridad de la Información de los Organismos que conforman la RED HISPALNET, en el Boletín Oficial de la Provincia de Sevilla, en los Portales de Transparencia de cada uno de los Organismos que conforman la RED HISPALNET, así como en la Intranet municipal para su acceso a todos los empleados municipales.

CUARTO.- Instar a las Entidades que conforman la RED HISPALNET a que en los plazos indicados en la Política de Seguridad de la RED HISPALNET nombren a los Responsables que se indican en la misma y aprueben sus política de seguridad de la información vertical

QUINTO.- Dar traslado del presente Acuerdo junto con el documento de Política de Seguridad a toda las Entidades que conforman la RED HISPLANET.

En la fecha indicada a pie de firma

EL TENIENTE DE ALCALDE DELEGADO DE HACIENDA, TURISMO, PARTICIPACIÓN CIUDADANA Y TRANSFORMACIÓN DIGITAL

Fdo. Juan Francisco Bueno Navarro

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	2/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	2/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

NO8DO
AYUNTAMIENTO DE SEVILLA

Área de Hacienda, Turismo, Participación
Ciudadana y Transformación Digital
Dirección General de Transformación Digital

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS ORGANISMOS QUE CONFORMAN LA RED CORPORATIVA DEL AYUNTAMIENTO DE SEVILLA, DENOMINADA RED HISPALNET

Los avances tecnológicos en los campos de la informática y las telecomunicaciones, de la sociedad de la información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos. Son los poderes públicos los responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros y para ello se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En cumplimiento del Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad, que exige que los responsables de la información, los sistemas y servicios electrónicos apliquen las medidas de seguridad mínimas, el Ayuntamiento de Sevilla y sus Organismos ya disponían de una Política de Seguridad, pero dado el vertiginoso avance en el uso de los medios electrónicos y el crecimiento del Ayuntamiento de Sevilla en las presentaciones electrónicas de documentos, la seguridad de la información alcanza un papel relevante, siendo necesario revisar la anterior Política para garantizar la seguridad de la ciudadanía en sus relaciones con el Ayuntamiento y los organismos que conforman la RED HISPALNET,

En aras de ofrecer a la ciudadanía las condiciones de confianza necesarias en el uso de los medios electrónicos, dado el continuo aumento de la ciberdelincuencia, se pretenden establecer a través de este documento las medidas necesarias para la preservación de la integridad de los derechos fundamentales y, en especial, los relacionados con la intimidad y la protección de datos de carácter personal, dando así un paso mas en la defensa de los derechos de los ciudadanos, ante la creciente preocupación de éstos por la falta de control sobre sus propios datos.

Tal y como establece la Estrategia de Ciberseguridad de la Unión Europea, nuestra libertad y prosperidad dependen, cada vez más, de un ciberespacio abierto, protegido y seguro, correspondiendo a las Administraciones Públicas un papel destacado en la custodia del mismo. De este modo las normas que han ido marcando los hitos para la adaptación de la nueva Política de seguridad de la Información de los Organismos que conforman la Red Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, son las siguientes:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 6/2020, de 11 de noviembre, de firma electrónica.

Página 202 de un total de 248
Página 3 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 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
- 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.
- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional.
- El Real Decreto 12/2018, de 7 de septiembre, de seguridad de la redes y sistemas de información regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- 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.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
- 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.
- Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	4/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	4/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Página 203 de un total de 248
Página 4 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

-

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	5/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	5/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Página 204 de un total de 248
Página 5 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

CAPÍTULO I. Disposiciones generales

Artículo 1. Objeto.

El presente documento tiene por objeto establecer la política de Seguridad de la Información de los Organismos que conforman la RED Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, en adelante, Política de Seguridad de la RED HISPALNET, que se aplicará a la gestión y tratamiento de la información a través de los activos tecnológicos de software, hardware y de comunicaciones, que tengan encomendadas todas y cada una de las entidades que forman parte de dicha RED, conformando junto con la normativa que lo desarrolle el marco regulador transversal de la seguridad de la información de la RED .

Sin perjuicio de las directrices establecidas en el marco normativo transversal de la seguridad de la información de la RED, cada Entidad incluida en el ámbito de aplicación de este documento, desarrollará y aprobará el documento de Política de Seguridad de la Información de su Entidad, así como las normas y procedimientos, adecuando, en su caso, las directrices comunes a sus particularidades. Estas políticas de seguridad de cada Entidad y sus normas y procedimientos, tendrán la consideración de vertical o segundo nivel a lo largo de este articulado.

Artículo 2. Definiciones y estándares.

A los efectos previstos en este Decreto, las definiciones han de ser entendidas en el sentido indicado en el Glosario de términos incluido como Anexo I al presente documento.

Artículo 3. Ámbito de aplicación.

El presente documento será de aplicación a todas las entidades que en cada momento formen parte de la RED Corporativa de Telecomunicaciones del ámbito municipal de Sevilla, denominada RED HISPALNET, conforme al acuerdo de creación adoptado por la Junta de Gobierno, de fecha 27 de julio de 2018.

Artículo 4. Objetivos de la política de seguridad de la información de la RED HISPALNET.

La política de seguridad de la información del Ayuntamiento de Sevilla, persigue la consecución de los siguientes objetivos:

1. Garantizar que las redes y sistemas de información que conforman la RED HISPALNET posean el adecuado nivel de seguridad, disponibilidad y resiliencia frente a cualquier tipo de amenaza.
2. Garantizar a la ciudadanía, que sus datos serán gestionados de acuerdo con los estándares y buenas prácticas en seguridad de la información y protección de datos personales.
3. Salvaguardar la información que se genera en ejecución de la actividad propia de cada entidad de la RED HISPALNET.

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

4. Aumentar el nivel de concienciación en materia de seguridad de la información y de protección de datos personales de todas las entidades a las que es de aplicación el presente documento, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
5. Establecer las bases de un modelo integral de gestión de la seguridad de la información y sin olvidar la protección de datos personales en la RED HISPALNET, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
6. Garantizar el cumplimiento de la legislación vigente en materia de seguridad de la información, incluyendo especialmente la protección de datos personales y la ciberseguridad.

CAPÍTULO II. Principios de seguridad de la información de la RED HISPALNET

Artículo 5. Principios de la Política de Seguridad de la información de la RED HISPALNET.

Los principios son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con la gestión y tratamiento de la información a través de los activos tecnológicos software, hardware y de comunicaciones.

Estos principios, serán además de los establecidos en la normativa vigente en cada momento, los siguientes:

a) Principio de prevención. Se evitará o, al menos, se prevendrá en la medida de lo posible, que la información o los servicios se vean afectados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por las normas y leyes que le sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

b) Principio de detección. Dado que los servicios se pueden degradar rápidamente debido a incidentes que, en función de su gravedad, pueden producir desde una simple desaceleración hasta la detención de los mismos, se debe monitorizar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia. La monitorización es especialmente relevante para establecer líneas de defensa. Para ello, se implantarán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente, a efectos de detectar cuándo se produce una desviación significativa de los parámetros de servicio marcados.

c) Principio de reacción. Deberá minimizarse el tiempo de respuesta requerido, de forma que el impacto de los incidentes de seguridad sea el menor posible, para lo cual se establecerán mecanismos para actuar eficazmente frente a los incidentes de seguridad, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de

Página 208 de un total de 248
Página 9 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.

d) Principio de recuperación. Se deberá garantizar en la medida de lo posible la disponibilidad de los servicios ofrecidos a la ciudadanía, en función de la criticidad de los mismos, priorizando la continuidad de los servicios en el caso de un incidente de seguridad.

e) Principio de seguridad en el ciclo de vida completa de la gestión y tratamiento de la información a través de los activos TIC. Las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Las medidas de seguridad deberán establecerse para todas las fases del ciclo de vida de los servicios y sistemas, es decir, desde el diseño y concepción de los mismos, su implantación definitiva, la posterior operación y gestión y finalmente, su retirada.

f) Principio de licitud, lealtad y transparencia. Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

g) Principio de limitación de la finalidad. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

h) Principio de minimización de datos. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

i) Principio de exactitud. Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

j) Principio de limitación del plazo de conservación. Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de datos personales. Podrán conservarse durante períodos más largos siempre que se trate exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

K) Principio de integridad y confidencialidad. Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

l) Principio de no discriminación algorítmica. Los datos personales relativos a una persona física no serán objeto de una decisión, que pueda incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar.

m) Cualquier otro principio que le sea aplicable normativamente

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

CAPÍTULO III. Organización de la seguridad de la información de la RED HISPALNET.

Artículo 6. Responsabilidad compartida.

La preservación de la seguridad de la información de la RED HISPALNET será considerada objetivo común de todas las personas al servicio de las entidades que integran la RED HISPALNET, siendo todas ellas responsables del uso correcto de los activos tecnológicos, software, hardware y comunicaciones puestos a su disposición.

Artículo 7. Estructura organizativa de la RED HISPALNET en materia de Seguridad de la Información.

La seguridad se concibe como un proceso integral, que comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas tecnológicos y de comunicaciones destinados al tratamiento y gestión de la información y las comunicaciones. Únicamente estableciendo una estructura organizativa transversal puede garantizarse no solo la seguridad de toda la RED Corporativa, sino la de cada una de las entidades que la integran. Con este fin de seguridad transversal se establece una estructura organizativa que cubre tanto los aspectos de seguridad de la información relacionados con la gestión TIC de la misma, como los relacionados con la protección de datos personales. Por ello, la estructura consta de un Comité Director de Seguridad de la información de la RED HISPALNET que cubre ambos aspectos y dependiendo de este Comité otras dos estructuras paralelas, una destinada específicamente a la Seguridad TIC y otra, destinada, a la Protección de Datos Personales.

De este modo la estructura organizativa estará compuesta por los siguientes agentes:

1. Comité Director de Seguridad de la información de la RED HISPALNET
2. Grupo Técnico de Seguridad de la información de la RED HISPALNET
3. Grupo Técnico de Protección de Datos Personales de la RED HISPALNET
4. Comité de Crisis
5. Responsable de Seguridad TIC de la RED HISPALNET
6. Delegado de Protección de Datos de la RED HISPALNET
7. Responsable de Información de la RED HISPALNET
8. Responsable de Servicios de la RED HISPALNET
9. Responsable de Sistemas de la RED HISPALNET
10. Responsable de Seguridad TIC de cada Entidad adscrita a la RED HISPALNET
11. Delegado de Protección de Datos de cada Entidad adscrita a la RED HISPALNET

El modelo organizativo establecido tiene el carácter de mínimo, en cuanto a que en las Políticas de Seguridad de la información de cada una de las entidades que integran la RED HISPALNET, deberán establecer la estructura organizativa interna para la Política de Seguridad de la Información vertical.

Artículo 8. Comité Director de Seguridad de la Información de la RED HISPALNET.

1. Con el fin de implementar la Política de Seguridad de la información de los Organismos que conforman la RED Corporativa del Ayuntamiento de Sevilla y como órgano transversal de coordinación, gobierno y seguimiento en materia de Seguridad de la información en el ámbito de toda la RED Corporativa, se crea el Comité Director de Seguridad de la Información de la RED HISPALNET, que velará por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad y protección de datos.

2. El Comité Director de Seguridad de la Información de la RED HISPALNET estará compuesto por los siguientes miembros:

a) Presidente/a: La persona titular del Área con competencias en materia de Tecnología de la información.
Tendrá voto de calidad en la toma de decisiones del Comité.

b) Vocales:
- En el Ayuntamiento, el vocal será la persona titular de la Dirección General con competencias en materia de Tecnología de la Información, que a su vez sustituirá, en caso de ausencia, al Presidente.
- En el resto de Organismos que conforman la RED HISPALNET, será la persona que ostente la máxima titularidad en cada uno de ellos.
- La persona titular de la Coordinación General o Dirección General con competencias en materia de seguridad.
- El Jefe/a de la Policía Local.

Para cada uno de los vocales se designará un suplente, que lo sustituirá en caso de que acontezca una causa justificada. Estos suplentes serán nombrados con los mismos criterios que los titulares y sin que puedan tener nivel inferior a jefatura de servicio o similar.

c) Asesores:
- La persona responsable de seguridad TIC de la RED HISPALNET
- La persona responsable de Protección de Datos Personales de la RED HISPALNET
Estos asesores, asistirán a las reuniones con voz pero sin voto.

d) Secretaría: Será ejercida por una persona empleado público adscrita a un Servicio dependiente de la Dirección General con competencias en Tecnología de la Información, que convocará las reuniones del Comité y preparará los temas a tratar. Será nombrado por el Presidente del Comité.

3. El Comité Director de Seguridad de la Información de la RED HISPALNET, ejercerá las siguientes funciones:

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

a) Establece, coordina y lidera la estrategia en seguridad de la información transversal para todas las entidades adheridas a la RED HISPALNET.
b) Velar por el desarrollo, implantación, concienciación, formación y divulgación, así como por el cumplimiento y actualización de la política de seguridad de la RED HISPALNET.
c) Elevará al órgano competente para su aprobación, las posibles modificaciones a la presente Política de la Información de la RED HISPALNET.
d) Emitirá informe vinculante con carácter previo a la aprobación de la Política de seguridad de la información vertical de cada uno de los Organismos que conforman la RED HISPALNET, así como sus modificaciones, por el órgano competente.
e) Planificar y priorizar las iniciativas transversales necesarias para cumplir con las directrices, los objetivos y los principios básicos marcados en la presente Política de seguridad de la información. En especial, la elaboración, actualización y reevaluación periódica de los análisis de riesgos necesarios.
f) Proporcionar, dentro de los límites establecidos en los programas asignados en los presupuestos municipales anuales, al Área con competencias en Tecnología de la Información, los medios y recursos necesarios para posibilitar la realización de las iniciativas transversales planificadas.
g) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecúen en todo momento a las directrices marcadas por la política de seguridad de la información y de protección de datos personales, involucrando a todas las entidades de la RED.
h) Elevar las propuestas de revisión del marco normativo de seguridad de la información y protección de datos personales al órgano competente para su tramitación.
i) Impulsar iniciativas y proyectos relacionados con la seguridad de la información y la protección de datos en todas las entidades adheridas a la RED HISPALNET.
j) Establecer directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad de la información y protección de datos personales.
k) Definir y aprobar el modelo de relación con los responsables de seguridad de la información y protección de datos personales.
l) Supervisar, vigilar y controlar el cumplimiento de los requerimientos globales de seguridad y en lo relacionado con el cumplimiento del marco legal y regulatorio.
m) Ejercer las funciones tramitación, instrucción y propuesta de sanción en relación con cualquier conducta constitutiva de posible infracción de conformidad con la normativa en materia disciplinaria.
n) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.
o) Promover la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la seguridad de la información y de protección de datos personales.
p) Velar porque la seguridad de la información y la protección de datos personales se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 212 de un total de 248
Página 13 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

producción y posterior operación. En particular deberá velar por la creación y utilización de servicios horizontales que RED HISPALNET que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

q) Asegurar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecúa a lo establecido en la política de seguridad de la información

r) Supervisar el nivel de riesgo y tomar de decisiones en la respuesta a incidentes significativos de seguridad de la información que afecten o puedan afectar los activos TIC y a los datos personales.

4. Funcionamiento del Comité Director de Seguridad de la Información:

4.1.- Actuará como órgano colegiado y se regirá en todo lo que no esté previsto en el presente documento, por lo dispuesto en la Sección 3ª del Capítulo 2º del Título preliminar de la Ley 40/2015 de Régimen Jurídico de las Administraciones Públicas.

4.2.- El Comité Director podrá articular la creación de grupos de trabajo para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes.

4.3.- El Presidente/a del Comité podrá autorizar la asistencia a las reuniones de personas con conocimientos especializados en las materias que se fueren a tratar, que asistirán con voz, pero sin voto.

4.4.- El Comité Director de Seguridad de la RED HISPALNET, se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando lo decida su Presidente/a, a petición de cualquiera de los vocales.

Artículo 9. Grupo Técnico de Seguridad de la Información de la RED HISPALNET.

1. Con el fin de asesorar al Comité Director de Seguridad de la Información y coordinar las actividades comunes relacionadas con la seguridad de los sistemas TIC se articula el Grupo Técnico de Seguridad de la Información de la RED HISPALNET, con carácter asesor.

2. El Grupo Técnico de Seguridad de la Información de la RED HISPALNET estará compuesto por los siguientes miembros:

a) La persona que en cada momento ostente la titularidad del Servicio con competencias en materia de tecnología de la información del Ayuntamiento de Sevilla.
b) La persona designada responsable de Seguridad TIC de la RED HISPALNET.
c) Las personas designadas responsables de Seguridad TIC de cada una de las entidades de la RED HISPALNET.

3. El Grupo Técnico de Seguridad de la Información de la RED HISPALNET, ejercerá las siguientes funciones:

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 213 de un total de 248
Página 14 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

a) Coordinar el desarrollo de las directrices comunes en materia de seguridad TIC en todas las entidades de la RED.

b) Elaborar informes regulares del estado de la seguridad y de los incidentes significativos, de forma resumida y consolidada para su comunicación al Comité Director de Seguridad de la Información de la RED HISPALNET.

c) Proponer iniciativas de estrategias en seguridad de la información para todas las entidades adheridas a la RED HISPALNET.

d) Desarrollar iniciativas para el tratamiento de riesgos comunes de las entidades adheridas a la RED HISPALNET.

e) Elevar las iniciativas y proyectos comunes relacionados con la seguridad TIC, debatidos en el marco del Grupo Técnico de Seguridad, al Comité Director de Seguridad de la Información de la RED HISPALNET, para su análisis y aprobación.

f) Coordinar la elaboración de los planes de continuidad de las diferentes entidades, para asegurar una actuación sin fisuras en caso de que deban ser activados en escenarios de aplicación común.

g) Asegurar el compromiso de la RED HISPALNET con una efectiva gestión de la Seguridad de la Información y su mejora continua.

h) Cuantas otras le sean encomendadas por el Comité Director de Seguridad de la RED HISPALNET.

4. Funcionamiento del Grupo Técnico de Seguridad de la Información.

4.1. Actuará como órgano interno de asesoramiento al Comité Director de Seguridad de la RED HISPALNET.

4.2.Se reunirá con carácter ordinario cada seis meses y con carácter extraordinario cuando lo decida el Responsable de Seguridad TIC de la RED HISPALNET, o a petición de cualquiera de los Responsables de Seguridad TIC de cada una de las entidades de la RED HISPALNET dirigido a aquel.

4.3. A las reuniones del Grupo Técnico podrán asistir las personas de las entidades a la que pertenecen los responsables de seguridad TIC, a fin de que presten asesoramiento a algún tema concreto a tratar, siempre previa autorización del Presidente/a.

4.4. El responsable de Protección de Datos de la RED HISPALNET participará en las reuniones del Grupo Técnico de Seguridad TIC de la RED, cuando en el mismo vayan a abordarse cuestiones relacionadas con la protección de datos personales, pudiendo asistir a las mismas los responsables de protección de datos de las entidades de la RED HISPALNET que se determinen, para lo que serán convocados formalmente,

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	15/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	15/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Página 214 de un total de 248
Página 15 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

El Grupo Técnico de Seguridad TIC de la RED HISPALNET, articulará los mecanismos de colaboración y coordinación necesarios con los Responsables de Seguridad TIC de cada una de las entidades de la RED.

Artículo 10. Grupo Técnico de Protección de Datos Personales de la RED HISPALNET

1. Con el fin de organizar esa diversidad de figuras de Delegados de Protección de Datos Personales que conforman la Organización de la RED HISPALNET y adecuarlos a una actuación conjunta, coordinada y de apoyo, se articula la figura del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET, con carácter asesor.

2.- Formarán parte del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET:

1. La persona que en cada momento ostente la titularidad de la Dirección General con competencias en materia de Tecnología de la Información.
2. La persona designada como Delegado de Protección de Datos personales de la RED HISPALNET.
3. Las personas designadas como Delegados de Protección de Datos de cada uno de los Organismos que conforman la RED Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET.

3. El Grupo de Técnico de Protección de datos Personales de la RED HISPALNET, ejercerá las siguientes funciones:

a) Poner en común las actuaciones llevadas a cabo por cada uno de los Delegados/as de Protección de Datos dentro de su Organización, con el fin de estudiar la posibilidad de que las mismas tengan proyección en el resto de los entidades que conforman la RED HISPALNET. Especialmente, en lo referente a los documentos que éstos en el ejercicio de sus funciones, deben elaborar en su labor de concienciación a los empleados/as de la organización.
b) Poner en común las reclamaciones presentadas por la autoridad de control ante los Delegados de Protección de Datos de cada uno de los Organismos que conforman la RED HISPALNET, a fin de estudiar la necesidad de tomar medidas que eviten que se repitan en el futuro.
c) Recabar de los Delegados/as de Protección de Datos de cada entidad informes regulares de las actuaciones realizadas que redunden en la protección de datos personales y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación al Comité Director de Seguridad de la RED HISPALNET.
d) Elevar las iniciativas y proyectos comunes relacionados con la protección de datos, debatidos en el marco del Grupo Técnico, al Comité Director de Seguridad de la Información de la RED HISPALNET, para su análisis y aprobación.
e) Proponer la redacción de normas al Responsable de Protección de Datos Personales de la RED y Responsable de Seguridad TIC de la RED.

f) Velar porque se lleven a cabo las formaciones necesarias en materia de protección de datos a todo el personal al servicio de los organismos a los que aplica este documento.
g) Poner en conocimiento del Delegado de Protección de Datos del Organismo que corresponda, cualquier infracción en materia de protección de datos de la que tenga conocimiento.
h) Cuantas otras puedan contribuir a un mejor cumplimiento de la normativa en materia de protección de datos en toda la RED HISPALNET.

4. Funcionamiento del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.

4.1.- Asesorará al Comité Director de Seguridad de la Información de la RED HISPALNET, cuando así se le requiera.

4.2.- Se reunirá con carácter ordinario cada seis meses, con el fin de poner en común las actuaciones más relevantes que en materia de protección de datos se han llevado a cabo de manera individual en cada uno de los organismos a los que aplica este documento, a fin de tomar medidas que apliquen a todos los Organismos que integran la RED HISPALNET, velando así por el cumplimiento de la normativa en materia de protección de datos personales en todas las entidades que integran la RED y con carácter extraordinario, cuando lo decida el Delegado de Protección de Datos de la RED HISPALNET, o a petición de cualquiera de los Delegados de Protección de Datos de cada una de las entidades de la RED HISPALNET.

4.3.- Con el objeto de garantizar un conocimiento polivalente en cuanto a legislación específica y sectorial, su procedimiento administrativo y la tecnología aplicada a determinados tratamientos para tratar determinados asuntos, el Grupo podrá requerir la asistencia de personas que perteneciendo a su entidad puedan aportar criterios para la gobernanza interna de la protección de datos personales, tales como responsables de sede electrónica, de la transparencia, responsables TIC, responsables de la web, archivero/a municipal, servicios jurídicos, secretaría general y cualquier otro empleado/a municipal con conocimientos concretos en una materia específica.

El Grupo Técnico de Protección de datos Personales de la RED HISPALNET, no asumirá en ningún momento funciones propias que la legislación en materia de protección de datos, atribuye al Delegado de Protección de Datos. En consecuencia, serán éstos los que estén obligados a relacionarse con la autoridad de control, en relación a las cuestiones que afecten a la organización a la que están adscritos.

Artículo 11.Comité de Crisis.

1.- Para los casos de incidentes relacionados con la seguridad de la información que pongan en riesgo el funcionamiento global o parcial de cualquiera de los organismos que conforman la Red Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, provocando un riesgo que afecte de forma grave la prestación de servicios a la ciudadanía y a la seguridad de la información, la disponibilidad, integridad y confidencialidad de los datos personales, se creará el

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 216 de un total de 248
Página 17 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

Comité de Crisis, como órgano decisorio para la gestión unificada de toma de decisiones, definición de prioridades y planificación de la estrategia a seguir.

2.- Aunque en las políticas de seguridad de la información verticales de las entidades que integran la RED HISPALNET se recoja la posibilidad de que puedan constituirse Comités de Crisis para el caso de incidentes no graves, si se activa el Comité de Crisis transversal definido en este artículo, éste prevalecerá sobre cualquier otro y será el responsable de tomar el control de la situación.

3.- Este Comité de crisis está compuesto por:

a) El Alcalde o Alcaldesa

b) La persona que ostente la titularidad del Área Municipal con competencias en materia de tecnologías de la información.

c) La persona que ostente la titularidad del Área Municipal con competencias en materia de Seguridad Ciudadana.

d) La persona que ostente la titularidad del Organismo que conforma la RED Corporativa del Ayuntamiento de Sevilla afectado.

4.- Este Comité estará asesorado cuando así sea requerido por el Comité de crisis por:

a) El Coordinador/a General de Alcaldía

b) Secretario/a General del Ayuntamiento

c) La persona titular de la Dirección General con competencias en tecnologías de la información del Ayuntamiento.

d) La persona titular de la Coordinación General o Dirección General con competencia en materia de seguridad del Ayuntamiento de Sevilla.

e) La persona titular de la Dirección General con competencias en materia de comunicación.

f) La persona titular de la Dirección General con competencia en materia de comunicación.

g) El Jefe/a de la Policía Local.

h) El responsable de Seguridad TIC de la RED HISPALNET

A las reuniones del Comité de Crisis podrán asistir, cuando así sean requeridos por éste, los Responsables de Seguridad TIC o los Delegados/as de Protección de Datos de cualquiera de las entidades que integran la RED HISPALNET, a fin de que presten asesoramiento a algún tema concreto.

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

3.- Son Funciones del Comité de Crisis las siguientes:

a) Aprobar y agilizar las medidas urgentes para la detección, contención y erradicación en caso de contingencia grave que afecte a la seguridad de la información de cualquiera de las entidades de la RED HISPALNET.

b) Centralizar y canalizar la información tanto en el plano interno como en el externo.

c) Repartir responsabilidades dentro de las diferentes áreas de gestión, para facilitar su resolución y la coordinación entre todas las partes involucradas

d) Dotar de coherencia y unidad a todas las acciones llevadas a cabo en los diferentes niveles de intervención que sean necesarios.

e) Evaluar, en cada momento, la estrategia que se lleva a cabo, sus acciones y resultados.

f) Detectar y prever acontecimientos y establecer los pasos a seguir en función del desarrollo de los hechos.

4.- Funcionamiento:

El Comité de Crisis se reunirá cuando se considere que concurren las condiciones y circunstancias necesarias para ello.

Artículo 12. Responsable de Seguridad TIC de la RED HISPALNET.

Para coordinar la Seguridad TIC de toda la RED HISPALNET, garantizando el principio de función diferenciada, el Comité Director de Seguridad de la Información nombrará a la persona responsable de seguridad TIC de la RED HISPALNET, a propuesta de su presidente/a. Esta persona será una de las personas responsables de Seguridad TIC de alguna de las entidades.

La persona responsable de seguridad TIC de la RED HISPALNET tendrá las siguientes funciones:

a) Asesorar, informar y realizar labores de soporte al Comité Director de Seguridad de la Información de la RED HISPALNET, así como de ejecución de las decisiones y acuerdos adoptados, por el Comité Director de Seguridad de la Información de la RED HISPALNET.
b) Diseñar y ejecutar los programas de actuación de carácter global, así como la dirección de los proyectos y servicios corporativos de seguridad TIC de la RED.
c) Establecer el orden del día de las reuniones del Grupo Técnico de Seguridad TIC de la RED HISPALNET.
d) Convocar al Grupo Técnico de Seguridad TIC de la RED HISPALNET
e) Analizar y proponer al Grupo Técnico de Seguridad TIC de la RED HISPALNET, cualquier medida que considere necesaria para satisfacer el cumplimiento en materia de seguridad TIC.
f) Velar por la correcta ejecución de los procedimientos y procesos operativos de seguridad, coordinando las medidas a adoptar por los diferentes responsables involucrados en la

Página 218 de un total de 248
Página 19 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

gestión de la seguridad TIC, analizando asimismo la adecuación de los mismos a la normativa establecida.

g) Definir y coordinar las medidas operativas, en función de las directrices marcadas por el Comité Director de Seguridad de la Información de la RED HISPALNET, realizando el seguimiento de las actuaciones relacionadas con la seguridad de la información a través de los activos tecnológicos, software, hardware y comunicaciones.

h) Coordinar los programas de formación y concienciación, apoyando al Grupo Técnico de Seguridad TIC de la RED en la definición de las acciones formativas necesarias para satisfacer los requisitos marcados por este.

i) Asesorar, en colaboración con los/as Responsables de los Sistemas, a los/as Responsables de la Información y a los/as Responsables de los Servicios en el proceso de la gestión de los riesgos, así como elevar un informe anual sobre el estado del proceso al Comité Director de Seguridad de la Información de la RED HISPALNET.

j) Proponer temas a tratar en las reuniones del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.

k) Promover y realizar el seguimiento de las auditorías periódicas que den cumplimiento a las obligaciones en materia de seguridad de la información y de los datos de carácter personal, de acuerdo al calendario aprobado por el Grupo Técnico de Seguridad TIC.

l) Analizar los informes de auditoría, elaborando las conclusiones que presentará al Grupo Técnico de Seguridad TIC, transmitiendo con posterioridad los resultados a las diferentes personas responsables para que adopten las medidas correctoras oportunas.

m) Elaborar informes periódicos de seguridad para el Grupo Técnico de Seguridad TIC, con inclusión y estudio de los incidentes más relevantes de cada período y la gestión realizada de los mismos, así como de los principales riesgos residuales asumidos por la organización, recomendando posibles actuaciones respecto de ellos.

n) Velar para que la documentación sea custodiada de forma adecuada a su grado de sensibilidad.

o) Diseñar procedimientos de gestión en la materia, redactar manuales, estándares y guías técnicas.

p) Colaborar con el Delegado/a de Protección de Datos de la RED HISPALNET, para procurar una coherente gestión de seguridad de la información de la RED.

q) Emitir los informes que considere necesarios sobre el estado en materia de seguridad de la RED HISPALNET, proponiendo mejoras enfocadas a la necesidad de formación del personal informático, necesidades normativas y procedimentales, necesidad de medios materiales o personales, entre otras.

r) Poner en conocimiento del Comité Director de Seguridad las violaciones de seguridad detectadas o que se ocasionen en cualquier Entidad de la RED, con afección o potencial afección a otras entidades, o bien puedan resultar de interés para la seguridad del conjunto.

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	20/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	20/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Página 219 de un total de 248
Página 20 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

s) Establecer las pautas metodológicas y criterios comunes para la realización de categorizaciones de sistemas de información, selección de medidas de seguridad, evaluaciones de impacto y análisis de riesgos.

t) Redactar, en colaboración con los/as Responsables de Seguridad TIC de cada uno de los Organismos que integran la RED HISPALNET, las normas, guías y procedimientos que resulten del presente documento, para su posterior aprobación por el órgano competente.

Artículo 13. Responsable de Protección de Datos Personales de la RED HISPALNET.

1. Para coordinar actuaciones en materia de Protección de Datos entre los Delegados/as de Protección de Datos Personales de cada una de los organismos que conforman la RED HISPALNET, se crea la figura de la persona Responsable de Protección de Datos Personales de la RED HISPALNET.

2. La persona Responsable de Protección de Datos Personales de la RED HISPALNET será nombrado por el Comité Director de Seguridad de la Información de la RED HISPALNET a propuesta de su Presidente/a, entre los Delegados/as de Protección de Datos de los organismos que conforman la RED HISPALNET.

3.- El Responsable de Protección de Datos Personales de la RED HISPALNET tendrá las siguientes funciones:

a) Labores de soporte, asesoramiento e información al Comité Director de Seguridad de la Información de la RED HISPALNET así como de ejecución de las decisiones y acuerdos adoptados.

b) Diseño y ejecución de los programas de actuación de carácter global, así como la dirección de los proyectos y servicios corporativos de protección de datos personales de la RED HISPALNET.

c) Establecer el orden del día de las reuniones del Grupo Técnico de Protección de datos de la RED HISPALNET.

d) Convocar al Grupo Técnico de protección de datos personales de la RED HISPALNET.

e) Analizar y proponer al Grupo Técnico de Protección de Datos Personales de la RED, cualquier medida que considere necesaria para satisfacer el cumplimiento en materia de protección de datos personales.

f) La promoción y concienciación de una cultura de protección de datos dentro de toda la organización de la RED HISPALNET, coordinando los programas de formación y concienciación, apoyando al Grupo Técnico de Seguridad de la Información de la RED HISPALNET en la definición de las acciones formativas necesarias para satisfacer los requisitos marcados por éste.

g) Proponer temas a tratar en las reuniones del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.

h) Asesorar, en colaboración con los correspondientes Delegados/as de Protección de Datos de los organismos que conforman la RED HISPALNET, a los/as Responsables de los tratamientos de datos personales, en aquellas cuestiones que puedan plantearse en materia de protección de datos.

i) Comunicar a la Autoridad de Control competente, cualquier incidente que afecte simultáneamente a más de una Entidad de la RED HISPALNET.

j) Poner en conocimiento del Comité Director de Seguridad la violación de seguridad de datos personales detectada o que se ocasione en cualquier Entidad de la RED.

k) Velar porque se publique el inventario de tratamientos de datos personales de cada una de las entidades que integran la RED HISPALNET suministrando a las personas interesadas la información exigida en la normativa sobre protección de datos.

l) Elaborar informes a propuesta del Comité Director de Seguridad.

m) Actuar como interlocutor/a, en materia de protección de datos, entre el Comité Director de Seguridad TIC de la RED y Grupo Técnico de Protección de Datos personales de la RED.

n) Emitir los informes que considere necesarios sobre el estado en materia de protección de datos personales de la RED HISPALNET, proponiendo mejoras enfocadas a la necesidad de formación del personal de los diferentes Unidades, necesidades normativas y procedimentales, necesidad de medios materiales o personales, entre otras.

o) Redactar, en colaboración con los Delegados/as de protección de Datos de cada uno de los organismos que integran la RED HISPALNET, las normas, guías y procedimientos que resulten del presente documento, para su posterior aprobación por el órgano competente.

p) Cuantas otras puedan contribuir al cumplimiento de la LOPDGDD y RGPD y demás normas sobre protección de datos de forma transversal en todas las entidades de la RED.

Artículo 14. Responsables de Información de la RED HISPALNET.

1. La persona responsable de la información de la RED HISPALNET, para cualquier información o servicio que no esté vinculado a un área de ninguno de los organismos que conformen la RED HISPALNET, será la persona que ostente la titularidad de la Dirección General con competencias en Tecnología de la Información.

Para cualquier otra información o servicio será la persona titular de la Dirección General con competencias para determinar la gestión de la información y de los servicios

2. Tendrá como mínimo las siguientes funciones:

a) Ayudar a determinar los requisitos de seguridad de la información, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

Página 221 de un total de 248
Página 22 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

b) Proporcionar la información necesaria a la persona Responsable de Seguridad de la RED para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de los Servicios y de los Sistemas de la RED HISPALNET.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

Artículo 15. Responsable de Servicio de la RED HISPALNET.

1. La persona responsable de servicio de la RED HISPALNET, será la persona titular con competencia en la dirección general que decida sobre las características de los servicios a prestar.

2. Tendrá como mínimo las siguientes funciones:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la persona Responsable de la Seguridad de la RED, para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los/as Responsables de la Información y de los/as Responsables de los Sistemas de la RED.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

Artículo 16. Responsables de sistemas de la RED HISPALNET.

1. Responsables de los sistemas de la RED HISPALNET, serán las personas adscritas a cualquiera de las entidades que forman parte de la RED HISPALNET, designada al efecto por la persona titular de la Dirección General del Ayuntamiento que ostente las competencias en tecnología de la información.

2. Tendrá como mínimo las siguientes funciones:

a) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información que apliquen de forma transversal, durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

b) Ser el/la primer/a responsable de la seguridad de los sistemas de información que dirige, velando porque la seguridad de la información esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar porque el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Política de Seguridad TIC de la RED HISPALNET. Para todo ello podrá contar con el asesoramiento de la persona Responsable de la Seguridad TIC de la RED.

c) Creación, mantenimiento y actualización permanente de la documentación de seguridad de los sistemas de información, con el asesoramiento del Responsable de la Seguridad TIC de la RED.

d) Asesorar en la definición de la tipología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

e) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

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

g) Asesorar en colaboración con la persona Responsable de Seguridad TIC de la RED HISPALNET, a los/as Responsables de la Información y a los/as Responsables de los Servicios de la RED HISPALNET, en el proceso de gestión de riesgos.

h) Informar al responsable de seguridad TIC de la RED HISPALNET sobre los incidentes de seguridad, vulnerabilidades y anomalías en la gestión de la seguridad de la información.

i) Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los/as responsables de la información afectada, del servicio afectado y con el/la Responsable de la Seguridad TIC, antes de ser ejecutada y en su caso, trasladada la persona responsable de protección de datos personales de la RED HISPALNET si estos datos pudieran verse comprometidos

Artículo 17. Responsable de Seguridad TIC de cada Entidad adscrita a la RED HISPALNET.

1. Cada una de las entidades de la RED HISPALNET, dentro de la estructura organizativa que establezca la Política de Seguridad que deben dictar, deberán incluir como mínimo la figura del Responsable de Seguridad TIC de la Entidad correspondiente.

2. Sin perjuicio de las funciones que le puedan atribuir cada Entidad de la RED HISPALNET en sus respectivas Políticas de Seguridad TIC, la persona Responsable de Seguridad TIC de cada una de las entidades, tendrá como mínimo las siguientes atribuciones:

a) Supervisar, dentro de su Entidad, el cumplimiento de la Política de Seguridad y los documentos que la desarrollan.

b) La coordinación en materia de seguridad TIC dentro de su Entidad.

c) Asistir al Grupo Técnico de Seguridad TIC de la RED HISPALNET y prestar asesoramiento y soporte en todas aquellas cuestiones que afecten al ámbito de su Entidad.

d) Poner en conocimiento de la persona Responsable de seguridad TIC de la RED HISPALNET, los incidentes de seguridad que ocurran en su propia Entidad.

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 223 de un total de 248
Página 24 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

e) La investigación y monitorización de los incidentes de seguridad, en el ámbito de su Entidad.

f) Establecer en el ámbito de su Entidad, las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del Esquema Nacional de Segurida.

g) Preparar los temas relacionados con su Entidad, a tratar en las reuniones del Grupo Técnico de Seguridad TIC de la RED HISPALNET, aportando información puntual para la toma de decisiones.

h) Responsable de la ejecución en el ámbito de su Entidad de las decisiones del Grupo Técnico de Seguridad TIC de la RED HISPALNET.

i) Desarrollo y seguimiento de los programas de formación y concienciación en su Entidad

Artículo 18. Delegado/a de Protección de datos de cada uno de los Organismos que conforman la RED HISPALNET.

1. Cada uno de los organismos que conforman la RED HISPALNET, en cumplimiento de la obligatoriedad que el Reglamento General de Protección de Datos impone de designar un Delegado/ade Protección de Datos, cuando los tratamientos lo lleven a cabo una autoridad u organismo público, nombrará a su propio Delegado/a de Protección de Datos, de conformidad con las indicaciones que respecto a los mismos recogen tanto el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, como la Ley Orgánica 3/2018, de 5 de diciembre.

Del nombramiento del Delegado/a de Protección de Datos deberán dar cuenta al Consejo de Transparencia y Protección de Datos de Andalucía, como autoridad de control competente en la materia, en cumplimiento de lo dispuesto en la normativa sobre protección de datos personales.

2. Sin perjuicio de las funciones que le atribuye expresamente la normativa sobre protección de datos y las que pueda atribuirle el Organismo al que están adscritos, tendrá como mínimo las siguientes funciones.

a) La promoción y concienciación de una cultura de protección de datos dentro de su propia Entidad.
b) Poner en conocimiento del Delegado/a de Protección de Datos Personales de la RED HISPALNET, las cuestiones relacionadas con la protección de datos que aplican al organismo al que están adscritos, para que éste pueda ejercer las funciones de coordinación que se le atribuyen en el artículo 12.
c) Poner en conocimiento del Delegado/a de Protección de Datos Personales de la RED HISPALNET los incidentes sobre protección de datos personales que detecte en su Organismo.

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

d) Velar porque esté publicado y actualizado el Registro de Actividades de Tratamiento del Organismo del que depende y que se cumpla, el deber de información recogido en el artículo 11 de la Ley Orgánica 3/2018, de 5 de octubre, de protección de datos personales y garantías de los derechos digitales y en el artículo 13 del Reglamento de la UE.
e) Elaborar los informes que demande el Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.
f) Colaborar con el Delegado/a de Protección de Datos Personales de la RED HISPALNET en el diseño e implantación de las normas que desarrollen el presente documento en cuanto a la protección de datos personales.
g) Cuantas otras funciones contribuyan al cumplimiento de la normativa en materia de protección de datos.

Artículo 19. Resolución de conflictos.

1. De acuerdo con el Principio de Jerarquía que rige en la Administraciones Públicas, en caso de conflicto entre los diferentes responsables y/o entre diferentes servicios, éste será resuelto por el superior jerárquico de los mismos.

2. En defecto de lo anterior, prevalecerá la decisión del Grupo Técnico de Seguridad TIC de la RED HISPALNET, elevando aquellos casos en los que no tenga suficiente autoridad para decidir al Comité Director de Seguridad de la Información de la RED HISPALNET.

CAPÍTULO IV. Organización de los Registros de Actividades de Tratamiento de la RED HISPALNET

Artículo 20.- Tratamiento de datos personales.

Los tratamientos de datos personales deberán realizarse dentro del ámbito de competencias de cada responsable del tratamiento y deberán estar atribuidas por decretos de estructura orgánica o por acuerdos que vinculen a las partes y de los que se derive la función de cada una de ellas en lo relativo a los tratamientos de datos personales.

Artículo 21. Registro de Actividades de Tratamiento.

1.- Cada Organismo que conforma la RED HISPALNET Ayuntamiento deberá aprobar su propio Registro de Actividades de Tratamiento, en el que deben registrarse todas las actividades en las que se traten datos personales. El citado Registro deberá incluir al menos la información indicada en la normativa sobre protección de datos.

2.- El Registro de Actividades de Tratamiento será accesible, como mínimo, desde el Portal de Transparencia del Ayuntamiento de Sevilla.

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	26/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	26/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Página 225 de un total de 248
Página 26 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

Artículo 22. Colaboración sobre actuaciones en materia de Seguridad de la Información y la gestión de la protección de datos.

Dada que la Seguridad de la Información y la Protección de Datos Personales son dos áreas que están muy interconectadas, con implicaciones tecnológicas y organizativas y en su gestión, concurren dos tipos de actores: los/as responsables de seguridad TIC y los/as delegados/as de protección de datos, se establece como criterio de relación entre los mismos, el principio de cooperación y colaboración en todas aquellas actuaciones que afecten a los campos de actuación de ambas partes, de forma que se consensuarán las decisiones a tomar, respetando las competencia de cada uno.

CAPÍTULO V. Desarrollo de la Política de Seguridad

Artículo 23. Desarrollo de la Política de Seguridad de la Información de la RED HISPALNET: Plan Director de Seguridad de la información de la RED HISPALNET.

1. Las medidas sobre la seguridad de la información, de obligado cumplimiento, se desarrollarán en cuatro niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior. Esta estructura de cuatro niveles se determina tanto para la Política de Seguridad de la Información de la RED HISPALNET, como para las políticas verticales, que deberán recogerla y determinar los órganos de aprobación correspondientes. Su desarrollo se agrupará, al menos en las categorías de política, normativa, procedimientos y guías técnicas. Dichas medidas conformarán el Plan Director de Seguridad de la información de la RED HISPALNET, tanto en su vertiente TIC como en la de protección de datos personales.

Todos estos niveles prestarán especial atención a las exigencias derivadas de la normativa vigente en materia de seguridad de la información como en materia de protección de datos de carácter personal.

Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de Seguridad de la Información de los Organismos que conforman la RED HISPALNET Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET. Este primer nivel, está constituido por el presente documento, el cual es de obligado cumplimiento en todos los Organismos que conforman la RED HISPALNET.

b) Segundo nivel: Normas de seguridad en materia TIC y de protección de datos de carácter personal. Son de obligado cumplimiento en todos los Organismos que conforman RED HISPALNET. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

Página 226 de un total de 248
Página 27 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

c) Tercer nivel: Procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad y con la protección de datos personales. Son dependientes de las normas de seguridad.

d) Cuarto nivel: Guías técnicas. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad o que redunden en beneficio de una mayor garantía de protección de datos personales

2. El Comité Director de Seguridad de la Información de la RED HISPALNET establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de homogeneizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad de la RED HISPALNET.

La siguiente tabla resume el marco de desarrollo y la responsabilidad de su aprobación:

Nivel	Documento	Aprueba
Primero	Política de Seguridad de la RED HISPALNET	Alcalde o Alcaldesa u órgano en que delegue.
Segundo	Normas de Seguridad en materia TIC y de protección de datos personales	Alcalde o Alcaldesa, Junta de Gobierno, Pleno, la persona que ocupe una Delegación de Área, en función del rango de la norma
Tercero	Procedimientos	Titular de la Dirección General que en cada momento tenga atribuidas las competencias en materia de Tecnología de la Información o en protección de datos personales.
Cuarto	Documentación Técnica	El titular de la Jefatura de Servicio o puesto similar que pertenezca a la Dirección General con competencias en materia de Tecnología de la Información o en protección de datos personales.

3. Cada una de los Organismos que conforman la RED HISPALNET, deberán elaborar los documentos que desarrollen la Política de seguridad de la información de forma vertical y que

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

conformarán el Plan Director de Seguridad de la Información de la Entidad a la que aplique, determinando en la misma la persona titular competente para su aprobación.

4. Todos las personas empleadas de todos y cada uno de los organismos que conforman la RED HISPALNET, tendrá la obligación de conocer y cumplir, además de esta Política de Seguridad de la información y las que se desarrollen en el marco de cada Organismo, todas las directrices generales, normas, procedimientos y guías técnicas de seguridad de la información que puedan afectar a sus funciones, siendo responsabilidad del Comité Director de la RED HISPALNET disponer de los medios necesarios para que la información llegue a los afectados/as.

5. Se utilizará un lenguaje no sexista en la elaboración y redacción de las resoluciones y documentos técnicos que se deriven, así como en aquellos otros que desarrollen la Política de Seguridad de la información en cada una de los organismos y empresas incluidos en el ámbito de aplicación de la presente Política de Seguridad.

6. Cada uno de los Grupos Técnicos de Seguridad TIC y de Protección de Datos Personales de los Organismos que integran la RED HISPALNET, establecerán los mecanismos necesarios para compartir la documentación derivada de su desarrollo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política de Seguridad de la Información.

Artículo 24. Gestión de los riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

2. La persona Responsable de Seguridad TIC de la RED HISPALNET, es la persona encargado de que se realice el preceptivo análisis de riesgos y se propongan las medidas de seguridad a aplicar, calculando los riesgos residuales.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos personales, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos. Este trabajo se llevará a cabo en colaboración con la persona Responsable de Protección de datos de la RED HISPALNET.

3. La perosna Responsable de Seguridad TIC de la RED HISPALNET es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

4. Los/as Responsables de la Información y del Servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 228 de un total de 248
Página 29 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

control, sin perjuicio de la posibilidad de delegar esta tarea. Corresponde igualmente a éstos realizar la categorización de los sistemas, conforme a lo establecido en el Esquema Nacional de Seguridad.

5. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad TIC de la RED HISPALNET que elevará informe al Comité de Director de Seguridad de la RED HISPALNET.

6. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación de éste, elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en la Ley Orgánica 3/2018, de 5 de diciembre.

7.- Los/as Responsables del Tratamiento de datos personales podrán solicitar el asesoramiento en la realización de análisis de riesgos y evaluaciones de impacto de tratamientos de datos personales a los respectivos Delegados/as de Protección de datos de cada una de las entidades integradas en la RED HISPALNET, dentro de los límites competenciales que legalmente corresponde a cada uno.

Artículo 25 Operación de la seguridad de la Información.

1. La operación de la seguridad de la información, se desarrollará a través del Centro de Ciberseguridad de la RED HISPALNET, que estará constituido por todos aquellos recursos tecnológicos de la seguridad de la información y de la seguridad de protección de datos personales, con independencia de su titularidad, y la gestión técnica y de asesoramiento a los mismos, destinada a prestar los servicios de seguridad de la información de cualquier tipo.

2. La Delegación con competencia en materia TIC del Ayuntamiento de Sevilla llevará a cabo cuantas actuaciones sean precisas para la adecuada realización de cualquier operación de seguridad, en concreto, realizar la licitación de los concursos públicos para la selección y contratación de la infraestructura y los servicios que sean necesarios.

ANEXO I. Glosario de términos.

Activo de tecnologías de la información y comunicaciones (TIC): cualquier información o sistema de información que tenga valor para la organización. Incluye datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	30/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	30/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		

Ciberincidente o Incidente de seguridad TIC: Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta. Suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de la información.

Contingencia grave: Incidente de seguridad TIC cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.

Plan director de seguridad: Estrategia y conjunto de iniciativas planificadas, plasmadas en un documento escrito, cuyo objetivo es alcanzar un determinado nivel de seguridad en la organización.

Política de seguridad de la información: Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información y comunicaciones.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Sistema de información: Conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.

Sistema de información crítico: Sistema de información cuyo adecuado funcionamiento es indispensable para el funcionamiento de la organización y el cumplimiento de sus obligaciones fundamentales.

Seguridad de la información: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos

Disposición Adicional Primera. Nombramientos de responsables

En el plazo de 2 meses a contar desde la aprobación de la presente Política de Seguridad de la Información cada una de los Organismos que la integran deberán proponer al Alcalde el nombramiento de las perosnas Responsables de Seguridad TIC y Delegados/as de Protección de Datos de cada una de las Organismos que conforman la RED HISPALNET.

De los citados nombramientos deberán dar cuenta para su conocimiento al Comité Director de Seguridad de la RED HISPALNET.

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Página 230 de un total de 248
Página 31 de 32
CVE: BOP-SE-2024-231032
Nº 231 - miércoles 27 de noviembre de 2024
BOLETÍN OFICIAL DE LA PROVINCIA DE SEVILLA

Disposición Adicional Segunda. Aprobación de las Políticas verticales de cada una de las entidades que conforman la RED HISPALNET.

1.- En el plazo de tres meses a contar desde la publicación en el Boletín Oficial de la Provincia del presente documento, los Organismos que conforman la RED HISPALNET deberán tener aprobadas sus respectivas Políticas de Seguridad verticales.

2. Aquellas entidades que carezcan de medios suficientes para crear una estructura como la que se exige en el presente documento podrán adherirse a las del Ayuntamiento de Sevilla, previo Acuerdo del Comité Director de Seguridad de la RED HISPALNET.

Disposición final. Publicidad de la Política de seguridad de la RED HISPALNET

El presente documento por el que se establece la Política de Seguridad de los Organismos que conforman la RED HISPALNET Corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, una vez aprobado se publicará, además de en el Boletín Oficial de la Provincia de Sevilla, en los Portales de Transparencia de cada una de las entidades que conforman la citada RED HISPALNET, así como en la Intranet del Ayuntamiento para su acceso a todos los empleados.

Código Seguro De Verificación	LiG3eEoyfHb1GXQrrs1GPg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	15/07/2024 11:56:24
Observaciones		Página	32/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/LiG3eEoyfHb1GXQrrs1GPg==		

Aprobado por la Junta de Gobierno de la ciudad de Sevilla, en sesión ordinaria celebrada el día 26/07/2024
EL SECRETARIO DE LA JUNTA

Código Seguro De Verificación	mKHM40a8aiWn8kkOAytgSg==	Estado	Fecha y hora
Firmado Por	Juan Francisco Bueno Navarro	Firmado	26/07/2024 11:04:55
Observaciones		Página	32/32
Url De Verificación	https://www.sevilla.org/verifirmav2/code/mKHM40a8aiWn8kkOAytgSg==		