POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Autor: Responsable de Seguridad **Organización:** TEC SOLUCIONES DE NEGOCIO S.L.U.	**Validado por:** Responsable del Servicio **Organización:** TEC SOLUCIONES DE NEGOCIO S.L.U.	**Aprobado por:** Directora General 03904794S ISABEL BARROSO (R: B45585726) Firmado digitalmente por 03904794S ISABEL BARROSO (R: B45585726) Fecha: 2023.09.19 13:41:02 +02'00' **Organización:** TEC SOLUCIONES DE NEGOCIO S.L.U.
Fecha: 04-09-2023	**Fecha:** 04-09-2023	**Fecha:** 19-09-2023

Descripción: Política de Seguridad de TEC SOLUCIONES DE NEGOCIO S.L.U.

Control de Versiones:

Versión	Fecha	Descripción del cambio
1.0	05-02-2019	Creación del documento.
1.1	11-02-2019	Revisión por EstudNET (Jorge).
1.2	24-05-2019	Adaptación a TEC.
1.3	18-09-2019	a) Se indica el posicionamiento de la organización de todos los requisitos mínimos establecidos en el RD3/2010 – ENS [apartado a) a o) del artículo 11 (que corresponden con los artículos 12 a 26) b) Se detalla los mecanismos de coordinación y resolución de conflictos. c) Se precisa el procedimiento para designar (en todos los casos) y renovar los roles o funciones de seguridad. d) Se identifican las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
2.0	30-08-2021	a) Adaptación a nueva denominación social e imagen corporativa. b) Se actualiza “Marco Normativo” con Real Decreto 43/2021 c) Se actualiza Organigrama nominal de “Organización y roles de Seguridad de la Información”.
2.1	20-06-2023	Se actualiza la Política al nuevo RD 311/2022

3.0	04-09-2023	Se pone en limpio el documento, eliminando control de cambios y comentarios, para pasar a aprobación por Dirección.

Índice

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado y aprobado el día 19 de septiembre de 2023 por el Comité de Seguridad de la información de TEC SOLUCIONES DE NEGOCIO. S.L.U.

Esta revisión de la Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva política.

2. INTRODUCCIÓN

El objetivo de la seguridad de la información es garantizar la calidad de ésta y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante incidentes.

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

La Información es uno de los activos más importantes para una organización y, por tanto, debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se transmita, almacene o procese.

El objetivo del presente documento es establecer un modelo de actuación, denominado Política de Seguridad, dentro del marco regulatorio legal y vigente, como ***el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*** (en adelante, ENS) con el que se garantice una protección adecuada de los activos de información y la prestación continuada de los servicios, de modo tal que *TEC* esté preparada para prevenir, detectar, reaccionar y recuperarse ante incidentes de seguridad. Para esto, será necesario contar con las medidas de seguridad necesarias para mantener un nivel de riesgo aceptable, así como realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva ante los incidentes que puedan surgir.

Esta política de seguridad, que se establece de acuerdo con los principios básicos más adelante descritos, se desarrolla aplicando los siguientes **requisitos mínimos**:

a) Organización e implantación del proceso de seguridad. La seguridad en TEC compromete a todos los miembros de la organización. La política de seguridad, en consecuencia, identifica Los responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

b) Análisis y gestión de los riesgos. TEC realiza la gestión de riesgos de los sistemas de información que desarrolla, implanta y soporta, en el ámbito de la Administración Electrónica. Esta gestión se realiza por medio del análisis y tratamiento de los riesgos a los que están expuestos los sistemas, empleando MAGERIT, como metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los

riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

c) Gestión de personal. Todo el personal de TEC relacionado con la información y los sistemas de información, en el ámbito de la administración Electrónica, será formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones serán supervisadas para verificar que se siguen los procedimientos establecidos. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

d) Profesionalidad. La seguridad de los sistemas de información de TEC, en el ámbito de la administración Electrónica, estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidentes y desmantelamiento. El personal de TEC recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

e) Autorización y control de los accesos. El acceso a los sistemas de información de TEC, en el ámbito de la Administración Electrónica, deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones. Los sistemas de información de TEC, en el ámbito de la Administración Electrónica, se desarrollarán, mantendrán y soportarán en áreas separadas, dotadas de un procedimiento de control de acceso.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por los sistemas de información de TEC, en el ámbito de la Administración Electrónica, se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos 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. La certificación deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden

PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada. Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y a lo dispuesto en el artículo 16.

h) Mínimo privilegio. Los sistemas de información de *TEC*, en el ámbito de la Administración Electrónica, deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto:

   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, desde emplazamientos o equipos asimismo autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
   c. Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
   d. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

i) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en los sistemas de información de TEC, en el ámbito de la Administración Electrónica. Se deberá conocer en todo momento el estado de 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.

j) Protección de la información almacenada y en tránsito. En la estructura y organización de la seguridad los sistemas de información de TEC, en el ámbito de la Administración Electrónica, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de

la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) Prevención ante otros sistemas de información interconectados. El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del Anexo II, de la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones. 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.

l) Registro de actividad y detección de código dañino. Con la finalidad exclusiva de lograr el cumplimiento del objeto de la presente política y su normativa de desarrollo, 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, los sistemas de información de TEC, en el ámbito de la Administración Electrónica, registrarán las actividades 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.

m) Incidentes de seguridad. TEC establecerá un sistema de detección y reacción frente a código dañino. TEC, asimismo, dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos 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.

n) Continuidad de la actividad. Los sistemas de información de TEC, en el ámbito de la Administración Electrónica, 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.

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

3. MISIÓN

TEC es una empresa tecnológica del grupo Eurocaja Rural, cuya misión es prestar servicios a los ayuntamientos y demás entidades locales a través de sus programas Sistema Integral Administración Electrónica (***SiAe***) y el Gestión Integral de Ayuntamientos Web (***GiaWeb***), que permite realizar tanto la gestión administrativa interna de la entidad como el acceso por vía electrónica a los distintos servicios que las entidades locales ofrecen a los ciudadanos.

4. DEFINICIONES

A los efectos previstos en la presente política, las definiciones, palabras, expresiones y términos han de ser entendidos en el siguiente sentido:

- ***AUTENTICIDAD***: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

- ***CONFIDENCIALIDAD***: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- ***DISPONIBILIDAD***: Propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

- ***GESTIÓN DE RIESGOS***: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

- ***INFRAESTRUCTURA TECNOLÓGICA:*** aquellos recursos, físicos y lógicos, sobre los que se soportan los sistemas de información.

- ***INTEGRIDAD***: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

- ***MEDIDAS DE SEGURIDAD***: Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

- ***RIESGO***: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

- ***SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN***: Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de

gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- ***SISTEMA DE INFORMACIÓN***: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

- ***TRAZABILIDAD***: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Las unidades de TEC y sus responsables deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

5. PREVENCIÓN

Las unidades de TEC y sus responsables deben evitar o, en su caso, prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la presente política, las unidades de TEC y sus responsables deben:

- Autorizar los sistemas de información, antes de entrar en operación.

- Evaluar regularmente la seguridad de la información, 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.

6. DETECCIÓN

Dado que los servicios se pueden degradar debido a incidentes, que van desde una simple desaceleración hasta su detención total, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

7. RESPUESTA

Las unidades de TEC y sus responsables deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados por los organismos municipales.
- 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) de las administraciones públicas y/o sectoriales.

8. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los responsables de TEC deben desarrollar planes de continuidad de los sistemas de información, como parte del plan general de continuidad y recuperación de los servicios.

9. OBJETIVOS

La seguridad de la información se establece como uno de los pilares fundamentales de los servicios ofrecidos por TEC y tiene como objetivos los que siguen:

- Garantizar el cumplimiento de la legislación vigente, reglamentos y acuerdos con terceros en lo que afecta al tratamiento de la información.
- Asegurar la confidencialidad de los datos obtenidos y gestionados, asegurar la disponibilidad de los sistemas de la información en los servicios ofrecidos a los clientes, así como asegurar la integridad de la información, evitando alteraciones en la misma.
- Asegurar la continuidad en las operaciones de la empresa con el fin de permitir el normal funcionamiento de los servicios críticos, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo.
- Promover la competencia, la toma de conciencia y la formación en materia seguridad de la información.
- Establecer la responsabilidad de los empleados en relación con la notificación de las violaciones de seguridad; preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y cumplir las políticas y procedimientos inherentes a la Política de Seguridad de la Información sin excepciones.

La presente política, en consecuencia, articula los objetivos orientados a proteger la información y los sistemas que la soportan frente a posibles amenazas, para reducir los daños provocados por los incidentes y asegurar la continuidad de los servicios, preservando las propiedades de la seguridad de la información, a saber:

- **Confidencialidad:** Garantizar que a la información y a los sistemas sólo acceden las personas debidamente autorizadas.
- **Integridad:** Garantizar la exactitud de la información y los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- **Disponibilidad:** Garantizar que la información y los sistemas puedan ser utilizados en la forma y tiempo requeridos.
- **Autenticidad:** Garantizar que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad**: Garantizar que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Las propiedades anteriores son esenciales, asimismo, para dar cumplimiento a la legislación vigente en materia de seguridad de la información y para la prestación de un servicio de calidad.

10. ÁMBITO DE APLICACIÓN

En virtud de lo expuesto en esta política y su normativa de desarrollo, serán definidas unas medidas de seguridad que se aplicarán a los servicios del Sistema Integral Administración Electrónica (SiAe) y el Gestión Integral de Ayuntamientos Web (GiaWeb).

11. MARCO NORMATIVO

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
- Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- 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 Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

12. VIGENCIA Y REVISIONES

La presente Política entrará en vigor el día de su aprobación por el Comité de Seguridad de la Información de TEC.

Este documento deberá *revisarse* en función de los cambios organizativos, legales o de negocio que se produzcan en cada momento, con el fin de mantener su pertinencia, suficiencia y eficacia y, en cualquier caso, al menos, una vez anualmente.

13. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

El Responsable de los Servicios y de la Información de *TEC* considera los recursos humanos, la información, las tecnologías y los recursos materiales que los soportan como principios básicos, motivo por el que garantizar su seguridad se considera un bien esencial en la estrategia de *TEC* y un habilitador imprescindible de la actividad de la organización.

Los siguientes principios básicos deberán ser tenidos en cuenta siempre que se adopten decisiones en materia de seguridad de la información:

a) Seguridad como proceso integral.
La seguridad ha de ser entendida como un proceso integral que involucra a todos y cada uno de los elementos humanos, técnicos, materiales y organizativos relacionados con el sistema.

b) Gestión de la seguridad basada en los riesgos.
El análisis y la gestión de riesgos es una parte esencial del proceso de seguridad. Los niveles de riesgo han de mantenerse dentro de unos niveles mínimos aceptables, mediante el despliegue de las medidas de seguridad apropiadas y permanentemente actualizadas, de modo tal que se establezca un equilibrio y proporcionalidad entre la naturaleza de los datos y los tratamientos realizados, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.

c) Prevención, detección, respuesta y conservación.
La seguridad del sistema debe contemplar los aspectos de prevención, detección y recuperación, para conseguir que las amenazas sobre el mismo no se materialicen o no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan. El sistema garantizará la conservación de los datos e informaciones en soporte electrónico, y mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

d) Existencia de Líneas de defensa.
El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de tal forma que, si una de ellas falla por causa de un incidente que no ha podido evitarse, se gane tiempo para una reacción adecuada, se reduzca la posibilidad de que el sistema se vea comprometido en su conjunto, y se minimice el impacto final sobre el mismo.

e) Vigilancia Continua y Reevaluación periódica.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos

permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Las medidas de seguridad adoptadas por TEC se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección

Mediante la aprobación de la presente política manifestamos la determinación y compromiso de TEC en alcanzar un nivel de seguridad adecuado a las necesidades del negocio que garantice la protección de los servicios y de la información de forma continuada y homogénea.

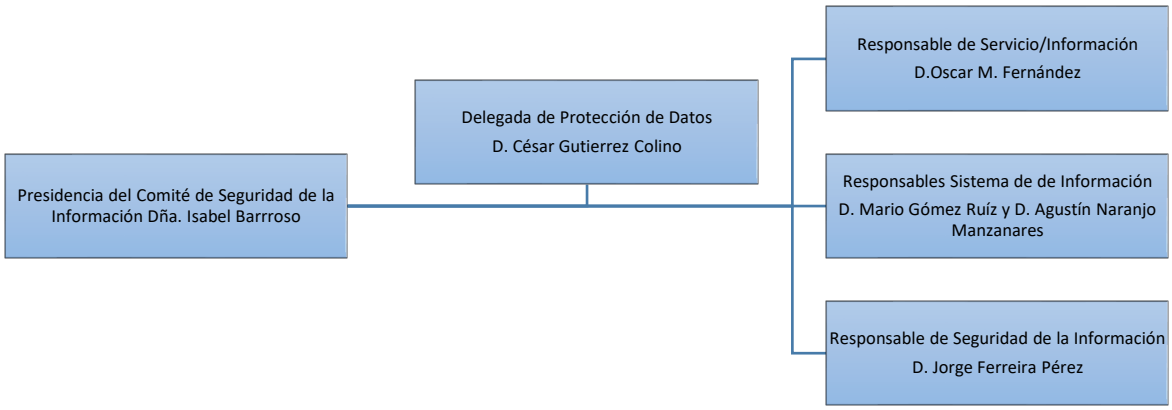
g) Diferenciación de responsabilidades

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

14. ORGANIZACIÓN Y ROLES DE LA SEGURIDAD DE LA INFORMACIÓN

La estructura organizativa de la gestión de la seguridad de la información de TEC está compuesta por las entidades siguientes:

- El Comité de Seguridad de la Información.
- El Responsable de la Información y del Servicio.
- El Responsable de Seguridad de la información
- El Responsable y Administrador del Sistema de Información
- La Persona Delegada de Protección de Datos


Presidencia del Comité de Seguridad de la Información Dña. Isabel Barrroso
Delegada de Protección de Datos
D. César Gutierrez Colino
Responsable de Servicio/Información
D.Oscar M. Fernández
Responsables Sistema de de Información
D. Mario Gómez Ruíz y D. Agustín Naranjo Manzanares
Responsable de Seguridad de la Información
D. Jorge Ferreira Pérez

15. FUNCIONES Y RESPONSABILIDADES

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

A. 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 los diferentes roles de seguridad y/o 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.
- 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 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 la 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 de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

B. 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
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.
- Funciones del Responsable de Seguridad
- 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 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.

C. FUNCIONES DEL RESPONSABLE DE SEGURIDAD

- Procurar que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.

- Realizar los análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones para que adopten las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artº. 27 y Anexo II.2 del ENS).
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

D. FUNCIONES DEL RESPONSABLE DEL SISTEMA DE INFORMACIÓN

- 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 su ciclo de vida.
- Elaborar 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.
- Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, 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 siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

E. FUNCIONES DE LA PERSONA DELEGADA DE PROTECCIÓN DE DATOS

- 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 de la normativa en materia de protección de datos personales y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- Supervisar el cumplimiento de lo dispuesto en la normativa en materia de protección de datos personales, 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 32;
- 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 y realizar consultas, en su caso, sobre cualquier otro asunto.

16. DESIGNACIÓN DE RESPONSABLES

El Responsable de la Información/Servicio será nombrados por la Dirección General de TEC.

El Responsable de Seguridad de la Información será nombrado, asimismo, por la Dirección General de TEC, teniendo también en cuenta la propuesta del Comité de Seguridad de la Información una vez constituido.

La Dirección General de TEC, como responsable de los servicios que se prestan electrónicamente, designará además a los Responsables de los Sistemas de Información, precisando sus funciones y responsabilidades en el marco establecido por la presente Política.

Las anteriores designaciones se revisarán cada 2 años o cuando queden vacantes.

17. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre las diferentes personas responsables que componen la estructura organizativa de la seguridad de la información en TEC, este será resuelto por el superior jerárquico de los mismos.

En caso de conflicto entre las personas responsables que componen la estructura organizativa de la seguridad de la información en TEC y los definidos en la normativa de protección de datos de carácter personal, prevalecerá la decisión que determine la persona responsable del tratamiento, asesorado por el delegado de protección de datos, que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

18. REPORTES

Los Responsable del Sistema de Información informan al Responsable de la Seguridad, en relación con:

- Los incidentes relativos a la seguridad del sistema
- Las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema de información
- Las acciones de configuración, actualización o corrección

Los Responsable del Sistema de Información informan al Responsable de la Información y del Servicio de las incidencias funcionales relativas al servicio.

El Responsable de la Seguridad de la información informa al Responsable de la Información y del Servicio de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

19. DATOS DE CARÁCTER PERSONAL

TEC realiza tratamientos en los que hace uso de datos de carácter personal.

Todos los sistemas de información de TEC se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de protección de datos de carácter personal.

20. ACCESO A LA INFORMACIÓN

Todos aquellos usuarios que traten información de TEC y de sus clientes, que no sea de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente necesarios para desempeñar su contenido, será con credenciales suministradas por TEC.

Para los casos de acceso a la información pública, se realizará mediante certificados digitales reconocidos.

En consecuencia, el acceso a los sistemas de información estará controlado y limitado exclusivamente a los usuarios, procesos, dispositivos y sistemas de información que estén autorizados, de forma que el acceso quede restringido exclusivamente a las funciones permitidas.

21. GESTIÓN DE INCIDENTES DE SEGURIDAD

Las unidades de TEC y sus responsables deben dar respuesta a los incidentes de seguridad mediante las medidas organizativas y operativas adecuadas.

Los incidentes de seguridad pueden ser detectados proactivamente, por los Responsable o administradores del sistema del sistema de información, por inspección o alarmas remitidas automáticamente al correo de TEC, procediéndose a centralizar la recogida, análisis y gestión de los incidentes identificados.

Asimismo, cualquier usuario debe trasladar incidentes, sugerencias y/o debilidades que puedan tener relación con la seguridad de la información y las directrices contempladas en la presente política comunicándolas al correo expreso.

22. GESTIÓN DE RIESGOS

Las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad, que deberá mantenerse permanentemente actualizado.

La evaluación de riesgos identifica las amenazas y vulnerabilidades, y debe ser suficientemente amplia como para abarcar los principales factores internos y externos, tales como tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones de seguridad.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de otros o ser causados por terceras personas.

Todos los sistemas sujetos a esta Política deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

23. DESARROLLO NORMATIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cuerpo normativo sobre seguridad de la información será de obligado cumplimiento y se desarrollará en tres niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de documentación de seguridad son los siguientes:

a) Primer nivel normativo: el presente documento que da soporte a la política de seguridad de la información de TEC.

b) Segundo nivel normativo: las políticas específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC).

   Las Políticas Específicas desarrollan con un mayor grado de detalle la Política dentro de un ámbito determinado.

   Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto aspecto, desde el punto de vista de la seguridad, tales como: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

   Las políticas y normas serán aprobadas por el Comité de Seguridad de la información de TEC

c) Tercer nivel normativo: los Procedimientos e Instrucciones Técnicas STIC.

   Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos y responsabilidades en ella establecidos.

   Los Procedimientos e Instrucciones Técnicas STIC serán aprobados por el Comité de Seguridad por el Comité de Seguridad de la información de TEC.

Adicionalmente, la documentación de seguridad podrá contar, bajo criterio de la persona Responsable de Seguridad, con documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, entre otros aspectos.

El Responsable de Seguridad se responsabilizará de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

El Comité de Seguridad de la información de TEC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo en la medida de lo posible en todo el ámbito de aplicación de la PSI.

24. OBLIGACIONES DE LOS USUARIOS

Todo el personal de TEC tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del *Comité o Responsable de Seguridad de la Información* disponer de los medios necesarios para que la información llegue a los afectados.

Todo el personal de la TEC debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.

Se establecerá un programa de concienciación para los nuevos miembros de TEC.

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.

25. RELACIÓN CON TERCERAS PARTES

Cuando TEC preste servicios a otros organismos o maneje información de estos, el responsable de esa relación les hará partícipes de esta política de seguridad y de las normas e instrucciones derivadas.

Se establecerán canales de comunicación y coordinación entre los *respectivos Comités o Responsables de Seguridad de la Información*, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Asimismo, cuando TEC utilice servicios de terceros o ceda información a terceros, el responsable de esa relación les hará igualmente partícipes de esta política de seguridad y de la normativa e instrucciones de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de prevención, detección, 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.

En concreto, los terceros deberán garantizar el cumplimiento de políticas de seguridad basadas en estándares auditables y someterse a controles y revisiones de terceros que certifiquen el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción y borrado que el tercero cancela y elimina los datos pertenecientes a TEC a la finalización del contrato.

Cuando algún aspecto de esta política de seguridad no pueda ser satisfecho por una tercera parte, se requerirá un informe del *Responsable de Seguridad de la Información* que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de Seguridad de la Información antes de seguir adelante.

03904794S ISABEL BARROSO (R: B45585726)
Firmado digitalmente por 03904794S ISABEL BARROSO (R: B45585726)
Fecha: 2023.09.19 13:29:48 +02'00'