

ADMINISTRACIÓN LOCAL

MUNICIPAL

SANTA COMBA

Política de Seguridade da Información do Concello de Santa Comba

ANUNCIO

Expediente Tedec: 2024/X999/000532

O Pleno da Corporación municipal en sesión ordinaria celebrada o 26 de xullo de 2024 aprobou, entre outros, este acordo extractado:

<<1.3.-PROPOSTA DA ALCALDÍA Ó PLENO DA CORPORACIÓN.

ASUNTO : Política de Seguridade da Información do Concello de Santa Comba
(Exp TEDEC 2024/X999/000532)

ACORDO

O Pleno da Corporación municipal; logo de ver o expediente; e de ver a proposta da alcaldía ó Pleno da Corporación. **ASUNTO: Política de Seguridade da Información do Concello de Santa Comba.** (Exp TEDEC 2024/X999/000532), asinada con data 16 de xullo de 2024; e o ditame favorable da Comisión informativa de Normalización lingüística, cultura, formación, educación, deportes, xuventude e comunicación do 22 de xullo de 2024; **por maioría simple dos presentes (votos a favor sete: 7 votos dos concelleiros do grupo m. do PSdeG-PSOE; votos en contra: ningún e abstencións cinco: 5 abstencións dos concelleiros do grupo m. do PP) e de conformidade coa proposta da alcaldía ó Pleno da Corporación. ASUNTO: Política de Seguridade da Información do Concello de Santa Comba.** (Exp TEDEC 2024/X999/000532), asinada con data 16 de xullo de 2024, que se transcribe, **aproba este acordo:**

PROPOSTA DA ALCALDÍA Ó PLENO DA CORPORACIÓN.

ASUNTO : Política de Seguridade da Información do Concello de Santa Comba
(Exp TEDEC 2024/X999/000532)

Esta Alcaldía propón ó Pleno a aprobación deste acordo :

Aprobar a Política de Seguridade da Información do Concello de Santa Comba :

Política de Seguridade da Información do Concello de Santa Comba

1. INTRODUCCIÓN

O Concello de Santa Comba depende dos sistemas TIC (Tecnoloxías da Información e das Comunicacións) para acadar os seus obxectivos, exercer as súas competencias e prestar os servizos que ten atribuídos. Estes sistemas deben ser administrados con dilixencia, adoptando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados que poidan afectar á dispoñibilidade, integridade ou confidencialidade da información tratada ou os servizos prestados.

O obxectivo da seguridade da información é garantir a confidencialidade, integridade, autenticidade e trazabilidade da información xunto coa prestación continuada dos servizos, actuando preventivamente, supervisando a actividade diaria e reaccionando con presteza aos incidentes.

Os sistemas TIC deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na confidencialidade, integridade, dispoñibilidade, uso previsto e valor da información e os servizos. Para defenderse destas ameazas, requírese unha estratexia que se adapte aos cambios nas condicións da contorna para garantir a prestación continua dos servizos. Isto implica que os departamentos deben aplicar as medidas mínimas de seguridade esixidas polo Esquema Nacional de Seguridade, así como realizar un seguimento continuo dos niveis de prestación de servizos, seguir e analizar as vulnerabilidades reportadas, e preparar unha resposta efectiva aos incidentes para garantir a continuidade dos servizos prestados.

Os diferentes departamentos deben asegurarse de que a seguridade TIC é unha parte integral de cada etapa do ciclo de vida do sistema, desde a súa concepción ata a súa retirada de servizo, pasando polas decisións de desenvolvemento ou adquisición e as actividades de explotación. Os requisitos de seguridade e a valoración do seu custo deben ser identificados e incluídos na planificación, na solicitude de ofertas, e en pregos de licitación para proxectos de TIC.

2. OBXECTIVOS DO CONCELLO DE SANTA COMBA

O Concello de Santa Comba, para a xestión dos seus intereses e das funcións e competencias que ten atribuídas en diferentes normas e convenios, promove actividades e presta servizos públicos que contribúen a satisfacer as necesidades e aspiracións da veciñanza. Para iso, pon á disposición da cidadanía a realización de trámites en liña co obxectivo de impulsar a tramitación electrónica dos procedementos administrativos, a mellora na prestación dos servizos e a participación da cidadanía nos asuntos públicos establecendo, deste xeito, novas vías de participación que garanten o desenvolvemento da democracia participativa e a mellora da eficacia e eficiencia da acción pública.

Por outra banda, deséxase potenciar o uso das novas tecnoloxías no concello e na propia cidadanía. Os principais obxectivos que se perseguen entre outros son: fomentar a relación electrónica da cidadanía co concello, e crear a confianza necesaria entre a veciñanza e o concello nesta relación.

3. ALCANCE

Esta política aplicarase aos sistemas de información do Concello de Santa Comba que están relacionados co exercicio de dereitos por medios electrónicos, co cumprimento de deberes por medios electrónicos ou co acceso á información ou ao procedemento administrativo e que se atopan dentro do ámbito de aplicación do Esquema Nacional de Seguridade (ENS).

4. MARCO NORMATIVO

A base normativa que afecta ao desenvolvemento das actividades e competencias do Concello de Santa Comba no que á administración electrónica se refire, e que implica a implantación de forma explícita de medidas de seguridade nos sistemas de información, está constituída pola seguinte lexislación:

- Lei 39/2015, do 1 de outubro, do Procedemento Administrativo Común das Administracións Públicas.
- Lei 40/2015, do 1 de outubro, de Réxime Xurídico do Sector Público.
- Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade.
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Resolución do 13 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade de conformidade co Esquema Nacional de Seguridade.
- Resolución do 7 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade de Informe do Estado da Seguridade.
- Resolución do 27 de marzo de 2018, da Secretaría de Estado de Función Pública, pola que se aproba a Instrución Técnica de Seguridade de Auditoría da Seguridade dos Sistemas de Información.
- Resolución do 13 de abril de 2018, da Secretaría de Estado de Función Pública, pola que se aproba a Instrución Técnica de Seguridade de Notificación de Incidentes de Seguridade.
- Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.
- Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (Regulamento xeral de protección de datos, RGPD).
 - Lei 36/2015, do 28 de setembro, de Seguridade Nacional.
 - Lei 6/2020, do 11 de novembro, reguladora de determinados aspectos dos servizos electrónicos de confianza.
 - Regulamento (UE) N° 910/2014 do Parlamento Europeo e do Consello, de 23 de xullo de 2014, relativo á identificación electrónica e os servizos de confianza nas transaccións electrónicas no mercado interior e polo que se derroga a Directiva 1999/93/CE (regulamento eIDAS).
 - Real Decreto 1308/1992, do 23 de outubro, polo que se declara ao Laboratorio do Real Instituto e Observatorio da Armada, como Laboratorio depositario do patrón nacional de Tempo e Laboratorio asociado ao Centro Español de Metroloxía.
 - Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico.
 - Lei 37/2007, do 16 de novembro, sobre a reutilización da información do sector público.
 - Real Decreto 1553/2005, do 23 de decembro, polo que se regula o documento nacional de identidade e os seus certificados de firma electrónica.
 - Lei 25/2007, do 18 de outubro, de conservación de datos relativos ás comunicacións electrónicas e ás redes públicas de comunicacións.

- Lei 56/2007, do 28 de decembro, de Medidas de Impulso da sociedade da información.
- Real Decreto 1494/2007, do 12 de novembro, polo que se aproba o Regulamento sobre as condicións básicas para o acceso das persoas con discapacidade ás tecnoloxías, produtos e servizos relacionados coa sociedade da información e medios de comunicación social.
- Real Decreto 1495/2011, do 24 de outubro, polo que se desenvolve a Lei 37/2007, do 16 de novembro, sobre a reutilización da información do sector público, para o ámbito do sector público estatal.
- Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno.
- Lei 25/2013, do 27 de decembro, de impulso da factura electrónica e creación do rexistro electrónico de facturas no sector público.
- Lei 7/1985, do 2 de abril, Reguladora das Bases do Réxime Local, modificada pola Lei 11/1999, do 21 de abril.
- Lei 16/1985, do 25 de xuño, do patrimonio histórico español (arquivo).
- Real Decreto Lexislativo 1/1996, do 12 de abril, polo que se aproba o texto refundido da Lei de Propiedade Intelectual.
- Real Decreto Lexislativo 5/2015, do 30 de outubro, polo que se aproba o texto refundido da Lei do Estatuto Básico do Empregado Público.
- Lei 9/2017, do 8 de novembro, de Contratos do Sector Público, pola que se traspoñen ao ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23/UE e 2014/24/UE, do 26 de febreiro de 2014.
- Lei 9/2014, do 9 de maio, xeral de telecomunicacións (vixente nos apartados sinalados na disposición derogatoria única da Lei 11/2022, do 28 de xuño).
- Real Decreto 203/2021, do 30 de marzo, polo que se aproba o Regulamento de actuación e funcionamento do sector público por medios electrónicos.
- Lei 11/2022, do 28 de xuño, xeral de telecomunicacións (segundo prazos entrada en vigor de disposición desta lei).
- Ordenanza municipal reguladora da administración electrónica do Concello de Santa Comba, aprobada por acordo del Pleno da Corporación en sesión celebrada o 26 de xaneiro de 2024 (corrección de erros aprobada por acordo do Pleno da Corporación en sesión celebrada o 22 de marzo de 2024) , publicada no BOP nº 117 de 18 de xuño de 2024 .
- Decreto do Alcalde do Concello de Santa Comba nº 1082 de adhesión á política de sinatura electrónica da Administración Xeral do Estado de data 15 de xullo de 2024.

Tamén forman parte do marco normativo, entre outras, as restantes normas aplicables á Administración Electrónica do Concello de Santa Comba derivadas das anteriores e publicadas nas sedes electrónicas comprendidas dentro do ámbito de aplicación desta Política.

O mantemento do marco normativo será responsabilidade do Concello de Santa Comba e manterase nun Anexo a este documento, que incluíra as instrucións técnicas de seguridade de obrigado cumprimento, publicadas mediante resolución da Secretaría de Estado de Administracións Públicas e aprobadas polo Ministerio de Facenda e Administracións Públicas e aprobadas polo Ministerio de Facenda e Administracións Públicas, a proposta do Comité Sectorial de Administración Electrónica e a iniciativa do *Centro Criptolóxico Nacional* (CCN) tal e como se establece no Real Decreto.

Así mesmo, o Concello de Santa Comba tamén será responsable de identificar as guías de seguridade do CCN, que serán de aplicación para mellorar o cumprimento do establecido no Esquema Nacional de Seguridade.

5. CUMPRIMENTO DOS REQUISITOS MÍNIMOS DE SEGURIDADE

O Concello de Santa Comba, para lograr o cumprimento do Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade, que recolle os principios básicos e dos requisitos mínimos, implementou diversas medidas de seguridade proporcionais á natureza da información e dos servizos a protexer e tendo en conta a categoría dos sistemas afectados.

A seguridade como un proceso integral e mínimo privilexio

A seguridade enténdese como un proceso integral constituído por todos os elementos técnicos, humanos, materiais, xurídicos e organizativos, relacionados co sistema. A aplicación do Esquema Nacional de Seguridade ao Concello de Santa Comba estará presidida por este principio, que exclúe calquera actuación puntual ou tratamento conxuntural.

Prestarase a máxima atención á concienciación das persoas que interveñen no proceso e ás súas responsables xerárquicas, para evitar que a ignorancia a falta de organización e coordinación ou as instrucións inadecuadas constitúan fontes de risco para a seguridade.

Os sistemas de información deben deseñarse e configurarse outorgando os mínimos privilexios necesarios para o seu correcto desempeño, o que implica incorporar os seguintes aspectos:

- O sistema proporcionará a funcionalidade imprescindible para que a organización acade os seus obxectivos competenciais ou contractuais.
- As funcións de operación, administración e rexistro de actividade serán as mínimas necesarias, e asegurarse que só son desenvolvidas polas persoas autorizadas, desde emprazamentos ou equipos asemade autorizados, podendo esixirse, no seu caso, restricións de horarios e puntos de acceso facultados.
- Nun sistema de explotación eliminaráanse ou desactivaránse, mediante o control da configuración, as funcións que sexan innecesarias ou inadecuadas ao fin que se persegue. O uso ordinario do sistema ha de ser sinxelo e seguro, de forma que unha utilización insegura requira dun acto consciente por parte do usuario.
- Aplicaranse guías de configuración de seguridade para as diferentes tecnoloxías, adaptadas á categorización do sistema, para o efecto de eliminar ou desactivar as funcións que sexan innecesarias ou inadecuadas.

Vixilancia continua, avaliación periódica e integridade, actualización do sistema e mellora continua do proceso de seguridade

A vixilancia continua por parte do Concello de Santa Comba permitirá a detección de actividades ou comportamentos anómalos e a súa oportuna resposta.

A avaliación permanente do estado da seguridade dos activos permitirá medir a súa evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

As medidas de seguridade avalíaranse e actualizaranse periodicamente, adecuando a súa eficacia á evolución dos riscos e os sistemas de protección, podendo chegar a unha reformulación da seguridade, se fose necesario.

A inclusión de calquera elemento físico ou lóxico no catálogo actualizado de activos do sistema, ou a súa modificación, requirirá autorización formal previa.

A avaliación e monitorización permanentes permitirán adecuar o estado de seguridade dos sistemas atendendo ás deficiencias de configuración, as vulnerabilidades identificadas e as actualizacións que lles afecten, así como a detección temperá de calquera incidente que teña lugar sobre os mesmos.

O proceso integral de seguridade implantado deberá ser actualizado e mellorado de forma continua. Para iso, aplicaranse os criterios e métodos recoñecidos na práctica nacional e internacional relativos á xestión da seguridade das tecnoloxías da información.

Xestión de persoal e profesionalidade

Todo o persoal propio e alleo relacionado cos sistemas de información do Concello de Santa Comba, dentro do ámbito do ENS, serán formados e informados dos seus deberes, obrigas e responsabilidades en materia de seguridade. A súa actuación será supervisada para verificar que seguen os procedementos establecidos.

O significado e alcance do uso seguro do sistema concretarase e plasmará nunhas normas de seguridade que serán aprobadas pola dirección ou o órgano superior correspondente. De igual modo, determinaranse os requisitos de formación e experiencia necesaria do persoal para o desenvolvemento do seu posto de traballo.

A seguridade dos sistemas de información estará atendida e será revisada e recibirá auditoría por persoal cualificado, dedicado e instruído en todas as fases do seu ciclo de vida: planificación, deseño, adquisición, construción, despregamento, explotación, mantemento, xestión de incidencias e desmantelamento.

De maneira obxectiva e non discriminatoria esixírase que as organizacións que proporcionan servizos ao concello contén con profesionais cualificados e cuns niveis idóneos de xestión e madurez dos servizos prestados.

Xestión da seguridade baseada nos riscos, análise e xestión de riscos

A análise e a xestión dos riscos será parte esencial do proceso de seguridade e será unha actividade continua e permanentemente actualizada.

A xestión dos riscos permitirá o mantemento dunha contorna controlada, minimizando os riscos a niveis aceptables. A redución a este niveis realizarase mediante unha apropiada aplicación de medidas de seguridade, de maneira equilibrada e proporcionada á natureza da información tratada, dos servizos a prestar e dos riscos aos que estean expostos.

Esta xestión realizarase por medio da análise e tratamento dos riscos aos que está exposto o sistema. Sen prexuízo do disposto no anexo II do ENS empregárase algunha metodoloxía recoñecida internacionalmente. As medidas adoptadas para mitigar ou suprimir os riscos deberán estar xustificadas e, en todo caso, existirá unha proporcionalidade entre elas e os riscos.

Incidentes de seguridade, prevención, detección, reacción e recuperación

O Concello de Santa Comba dispón de procedementos de xestión de incidentes de seguridade de acordo co previsto no artigo 33, a Instrución Técnica de Seguridade correspondente, e de mecanismos de detección, criterios de clasificación, procedementos de análises e resolución, así como das canles de comunicación ás partes interesadas.

A seguridade do sistema contemplará as accións relativas aos aspectos de prevención, detección e resposta, ao obxecto de minimizar as súas vulnerabilidades e lograr que as ameazas sobre o mesmo non se materialicen ou que, no caso de facelo, non afecten gravemente á información que manexa ou aos servizos que presta.

As medidas de prevención poderán incorporar compoñentes orientados á disuasión ou á redución da superficie de exposición, deben eliminar ou reducir a posibilidade de que as ameazas cheguen a materializarse.

As medidas de detección irán dirixidas a descubrir a presenza dun ciber-incidente.

As medidas de resposta xestionaranse en tempo oportuno, estarán orientadas á restauración da información e dos servizos que puidesen verse afectados por un incidente de seguridade.

O sistema de información garantirá a conservación dos datos e información en soporte electrónico.

De igual modo, o sistema manterá dispoñibles os servizos durante todo o ciclo vital da información dixital, a través dunha concepción e procedementos que sexan a base para a preservación do patrimonio dixital.

Existencia de liñas de defensa e prevención ante outros sistemas de información interconectados

O Concello de Santa Comba está a implementar unha estratexia de protección do sistema de información constituída por múltiples capas de seguridade, constituídas por medidas organizativas, físicas e lóxicas, de tal forma que cando unha capa foi comprometida permita desenvolver unha reacción adecuada fronte aos incidentes que non puideron evitarse, reducindo a probabilidade de que o sistema sexa comprometido no seu conxunto e minimizar o impacto final sobre o mesmo.

Protexerase o perímetro do sistema de información, especialmente, cando o sistema do concello conéctase a redes públicas, tal e como se definen na lexislación vixente en materia de telecomunicacións, reforzándose as tarefas de prevención, detección e resposta a incidentes de seguridade.

En todo caso, analizaranse os riscos derivados da interconexión do sistema con outros sistemas e controlárase o seu punto de unión. Para a adecuada interconexión entre sistemas estarase ao disposto na Instrución Técnica de Seguridade correspondente.

Diferenciación de responsabilidades, organización e implantación do proceso de seguridade

O Concello de Santa Comba organiza a súa seguridade comprometendo a todos os membros da corporación mediante a designación de diferentes roles de seguridade con responsabilidades claramente diferenciadas, tal e como se recolle no apartado de “MODELO DE GOBERNANZA” desta Política.

Autorización e control dos accesos

O Concello de Santa Comba implementa mecanismos de control de acceso ao sistema de información, limitándoo aos usuarios, procesos, dispositivos e outros sistemas de información, debidamente autorizados, e exclusivamente ás funcións permitidas.

Protección das instalacións

O Concello de Santa Comba implementa mecanismos de control de acceso físico, previndo os accesos físicos non autorizados, así como os danos á información e aos recursos, mediante perímetros de seguridade, controis físicos e proteccións xerais en áreas.

Adquisición de produtos de seguridade e contratación de servizos de seguridade

Para a adquisición de produtos ou contratación de servizos de seguridade o Concello de Santa Comba terá en conta a utilización de forma proporcionada á categoría do sistema e o nivel de seguridade determinado, aqueles que teñan certificada a funcionalidade de seguridade relacionada co obxecto da súa adquisición.

Para a contratación de servizos de seguridade atenderase ao sinalado en canto á profesionalidade.

Protección da información almacenada e en tránsito e continuidade da actividade

O Concello de Santa Comba prestará especial atención á información almacenada ou en tránsito a través dos equipos ou dispositivos portátiles ou móbiles, os dispositivos periféricos, os soportes de información e as comunicacións sobre redes abertas, que deberán analizarse especialmente para lograr unha adecuada protección.

Aplicaranse procedementos que garantan a recuperación e conservación a longo prazo dos documentos electrónicos producidos polos sistemas de información comprendidos no ámbito de aplicación deste protocolo, cando iso sexa esixible.

Toda información en soporte non electrónico que sexa causa ou consecuencia directa da información electrónica á que se refire este real decreto, deberá estar protexida co mesmo grao de seguridade que esta. Para iso, aplicaranse as medidas que correspondan á natureza do soporte, de conformidade coas normas que resulten de aplicación.

Os sistemas disporán de copias de seguridade e estableceranse os mecanismos necesarios para garantir a continuidade das operacións en caso de perda dos medios habituais.

Registro de actividade e detección de código daniño

O Concello de Santa Comba, co propósito de satisfacer o obxecto deste protocolo, con plenas garantías do dereito á honra, á intimidade persoal e familiar e á propia imaxe dos afectados, e de acordo coa normativa sobre protección de datos persoais, de función pública ou laboral, e demais disposicións que resulten de aplicación, rexistrará as actividades dos usuarios, retendo a información estritamente necesaria para monitorizar, analizar, investigar e documentar actividades indebidas ou non autorizadas, permitindo identificar en cada momento á persoa que actúa.

Co obxecto de preservar a seguridade dos sistemas de información, garantindo a rigorosa observancia dos principios de actuación das Administracións públicas, e de conformidade co disposto no Regulamento Xeral de Protección de Datos e o respecto aos principios de limitación da finalidade, minimización dos datos e limitación do prazo de conservación alí enunciados, o concello poderá, na medida estritamente necesaria e proporcionada, analizar as comunicacións entrantes ou saíntes, e unicamente para os fins de seguridade da información, de forma que sexa posible impedir o acceso non autorizado ás redes e sistemas de información, deter os ataques de denegación de servizo, evitar a distribución malintencionada de código daniño así como outros danos ás anteditas redes e sistemas de información.

Para corrixir ou, no seu caso, esixir responsabilidades, cada usuario que acceda ao sistema de información deberá estar identificado de forma única, de modo que se saiba, en todo momento, quen recibe dereitos de acceso, de que tipo son estes, e quen realizou unha determinada actividade.

Infraestruturas e servizos comúns

O Concello de Santa Comba terá en conta que a utilización das infraestruturas e dos servizos comúns das administracións públicas, incluídos os compartidos ou transversais, facilitará o cumprimento do disposto neste protocolo.

Perfís de cumprimento específicos e acreditación de entidades de implementación de configuracións seguras

O Concello de Santa Comba terá en conta a aplicación daqueles perfís de cumprimento específicos para Entidades Locais que sexan de aplicación.

6. MODELO DE GOBERNANZA

Para garantir o cumprimento do Esquema Nacional de Seguridade e establecer a organización da seguridade da información adaptada ás necesidades e particularidade deste concello, propónse unha designación de roles por bloques de responsabilidade: Goberno, Supervisión e Operación.

De acordo con esta estrutura, asígnanse as seguintes responsabilidades e funcións de seguridade:

Bloque de Goberno:

- Responsable de Goberno, cuxas funcións exercita a Alcaldía-Presidencia do concello, que integra os seguintes roles e funcións ENS:
- Comité de seguridade da información.
- Responsable da información.
- Responsable do servizo.

A Alcaldía-Presidencia pode delegar estes roles e/ou funcións nun concelleiro ou concelleiros.

Bloque Executivo e de Supervisión:

- Responsable de Supervisión, cuxas funcións exercita a Secretaría do Concello, e que integra o seguinte rol ENS:
- Responsable da Seguridade.

- Delegado Protección de Datos (DPD), cuxas funcións exercerá a persoa física ou xurídica contratista do servizo de Protección de Datos, apoiando á persoa Responsable de Supervisión, con funcións de asesoramento e supervisión en materia de protección de datos.

Bloque de Operación:

- Responsable de Operación, cuxas competencias exercita a persoa coas funcións de docente de integración dixital do Concello de Santa Comba e que integra o seguinte rol ENS:
- Responsable do Sistema.

6.1 RESPONSABILIDADES ASOCIADAS AO ESQUEMA NACIONAL DE SEGURIDADE

A continuación, detállanse e establécense as funcións e responsabilidades de cada un dos roles de seguridade ENS:

Funcións do Responsable da Información e dos Servizos

- Establecer e aprobar os requisitos de seguridade aplicables ao servizo e a información dentro do marco establecido no anexo I do Real Decreto do Esquema Nacional de Seguridade.
- Aceptar os niveis de risco residual que afecten ao Servizo e á Información.

Funcións do Responsable de Seguridade

- Manter e verificar o nivel adecuado de seguridade da Información manexada e dos servizos electrónicos prestados polos sistemas de información.
- Promover a formación e concienciación en materia de seguridade da información.
- Designar responsables da execución da análise de riscos, da declaración de aplicabilidade, identificar medidas de seguridade, determinar configuracións necesarias, elaborar documentación do sistema.
- Proporcionar asesoramento para a determinación da categoría do sistema, en colaboración co Responsable do Sistema.
- Participar na elaboración e implantación dos plans de mellora da seguridade e chegado o caso nos plans de continuidade, procedendo á súa validación.
- Xestionar as revisións externas ou internas do sistema.
- Xestionar os procesos de certificación.
- Elevar á Dirección a aprobación de cambios e outros requisitos do sistema.

Funcións do Responsable do Sistema

- Paralizar ou dar suspensión ao acceso a información ou prestación de servizo se ten o coñecemento de que estes presentan deficiencias graves de seguridade.
- Desenvolver, operar e manter o sistema de información durante todo o seu ciclo de vida.
- Elaborar os procedementos operativos necesarios.
- Definir a topoloxía e a xestión do Sistema de Información establecendo os criterios de uso e os servizos dispoñibles no mesmo.
- Asegurarse de que as medidas específicas de seguridade se integren adecuadamente dentro do marco xeral de seguridade.
- Prestar ao Responsable de Seguridade da Información asesoramento para a determinación da Categoría do Sistema.
- Colaborar, se así se lle require, na elaboración e implantación dos plans de mellora da seguridade e, chegado o caso, nos plans de continuidade.
- Levar a cabo as funcións do administrador da seguridade do sistema:
 - A xestión, configuración e actualización, no seu caso, do hardware e software nos que se basean os mecanismos e servizos de seguridade.
 - A xestión das autorizacións concedidas aos usuarios do sistema, en particular os privilexios concedidos, incluíndo a monitorización da actividade desenvolvida no sistema e a súa correspondencia co autorizado.
 - Aprobar os cambios na configuración vixente do Sistema de Información.
 - Asegurar que os controis de seguridade establecidos son cumpridos estritamente.

- Asegurar que son aplicados os procedementos aprobados para manexar o Sistema de Información.
- Supervisar as instalacións de hardware e software, as súas modificacións e melloras para asegurar que a seguridade non está comprometida e que en todo momento se axustan ás autorizacións pertinentes.
- Monitorizar o estado de seguridade proporcionado polas ferramentas de xestión de eventos de seguridade e mecanismos de auditoría técnica.

6.2 FUNCIONES DO COMITÉ DE SEGURIDADE DA INFORMACIÓN

As funcións propias dun Comité de Seguridade da Información son as seguintes:

- Atender as solicitudes, en materia de Seguridade da Información, da Administración e dos diferentes roles de seguridade e/ou áreas informando regularmente do estado da Seguridade da Información.
- Asesorar en materia de Seguridade da Información.
- Resolver os conflitos de responsabilidade que poidan aparecer entre as diferentes unidades administrativas.
- Promover a mellora continua do sistema de xestión da Seguridade da Información. Para isto encárgase de:
 - Coordinar os esforzos das diferentes áreas en materia de Seguridade da Información para asegurar que estes esforzos sexan consistentes, estean aliñados coa estratexia decidida na materia e evitar duplicidades.
 - Propor plans de mellora da Seguridade da Información, coa súa dotación orzamentaria correspondente, priorizando as actuacións en materia de seguridade cando os recursos sexan limitados.
 - Elaborar e revisar regularmente a Política de Seguridade da Información para a súa aprobación polo órgano competente.
 - Velar porque a Seguridade da Información sexa tida en conta en todos os proxectos desde a súa especificación inicial ata a súa posta en operación. En particular deberá velar pola creación e utilización de servizos horizontais que reduzan duplicidades e apoiem un funcionamento homoxéneo de todos os sistemas TIC.
 - Realizar un seguimento dos principais riscos residuais asumidos pola Administración e recomendar posibles actuacións respecto deles.
 - Realizar un seguimento da xestión dos incidentes de seguridade e recomendar posibles actuacións respecto deles.
 - Elaborar e revisar regularmente a Política de Seguridade da Información para a súa aprobación polo órgano competente.
 - Elaborar a normativa de Seguridade da Información para a súa aprobación en coordinación coa Dirección.
 - Verificar os procedementos de seguridade da información e demais documentación para a súa aprobación.
 - Elaborar programas de formación destinados a formar e sensibilizar ao persoal en materia de Seguridade da Información e en particular en materia de protección de datos de carácter persoal.
 - Elaborar e aprobar os requisitos de formación e cualificación de administradores, operadores e usuarios desde o punto de vista de Seguridade da Información.
 - Promover a realización das auditorías periódicas ENS e de protección de datos que permitan verificar o cumprimento das obrigas da Administración en materia de seguridade da Información.

Estas funcións poderán ser delegadas noutros órganos da entidade.

6.3 PROCEDIMENTO DE DESIGNACIÓN

A designación dos roles responsables identificados nesta Política realízase pola Alcaldía-Presidencia do Concello de Santa Comba e notificase de xeito fidedigno ás partes afectadas.

Os roles de seguridade serán revisados cada catro anos. As vacantes deberán ser cubertas no prazo dun mes, seguindo o mesmo procedemento.

6.4 RESOLUCIÓN DE CONFLICTOS

Os conflitos entre os roles Responsables serán resolto polo Comité de Seguridade da Información.

7. DATOS DE CARÁCTER PERSOAL

O Concello de Santa Comba, en canto ao tratamento de datos persoais cumpre cos principios e obrigas da normativa vixente, entre outra o Regulamento 679/2016, do Parlamento Europeo e do Consello, de 27 de abril de 2016, relativo ao tratamento de datos persoais e á libre circulación destes datos que derroga a Directiva 95/46/CE (RGPD) e a Lei Orgánica 3/2018, de 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais, respectando, en calquera caso, o dereito fundamental á protección de datos persoais, á intimidade e o resto de dereitos fundamentais recoñecidos na lexislación vixente e tratados internacionais como na Constitución.

8. DESENVOLVEMENTO DA POLÍTICA DE SEGURIDADE DA INFORMACIÓN

O cumprimento dos obxectivos marcados nesta Política de Seguridade lévase a cabo mediante o desenvolvemento de documentación que compoñen as normas e procedementos de seguridade asociados ao cumprimento do Esquema Nacional de Seguridade. Para a súa organización definiuse unha Norma para a Xestión da Documentación, que establece as directrices para a organización, xestión e acceso.

A revisión anual desta Política corresponde ao Responsable de Goberno, proponendo no caso de que sexa necesario melloras da mesma, para a súa aprobación por parte do mesmo órgano que a aprobou inicialmente.

9. TERCEIRAS PARTES

Cando se presten servizos a outros organismos, ou se manexe información doutros organismos, faráselles partícipes desta Política de Seguridade da Información. O Concello de Santa Comba definirá e aprobará as canles para a coordinación da información e os procedementos de actuación para a reacción ante incidentes de seguridade, así como o resto das actuacións que o concello leve a cabo en materia de Seguridade en relación con outros organismos.

Cando o Concello de Santa Comba utilice servizos de terceiros ou ceda información a terceiros, faráos partícipes desta Política de Seguridade e da Normativa de Seguridade existente que atinxa aos ditos servizos ou información. Dita terceira parte quedará suxeita ás obrigas establecidas na mencionada normativa, podendo desenvolver os seus propios procedementos operativos para satisfacela. Estableceranse procedementos específicos de comunicación e resolución de incidencias.

Garantirase que o persoal de terceiros estea adecuadamente concienciado en materia de seguridade, polo menos ao mesmo nivel que o establecido nesta Política de Seguridade.

De igual modo, tendo en conta a obriga de cumprir co disposto nas Instrucións Técnicas de Seguridade recollida na Disposición adicional segunda (Desenvolvemento do Esquema Nacional de Seguridade) do Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade, e en consideración á Instrución Técnica de Seguridade, de conformidade co Esquema Nacional de Seguridade, onde se establece que os operadores do sector privado que presten servizos ou fornezan solucións ás entidades públicas, aos que resulte esixible o cumprimento do Esquema Nacional de Seguridade, deberán estar en condicións de exhibir a correspondente Declaración de Conformidade co Esquema Nacional de Seguridade cando se trate de sistemas de categoría BÁSICA, ou a Certificación de Conformidade co Esquema Nacional de Seguridade, cando se trate de sistemas de categorías MEDIA ou ALTA.

Cando algún aspecto desta Política de Seguridade non poida ser satisfeito por unha terceira parte segundo se require nos parágrafos anteriores, requirirase un informe do Responsable de Seguridade que precise os riscos en que se incorre e a forma de tratalos. O dito informe deberá ser aprobado polos responsables da información e os servizos, con carácter previo ao inicio da relación coa terceira parte.

10. APROBACIÓN E ENTRADA EN VIGOR

Este documento será aprobado polo Pleno da Corporación do Concello de Santa Comba.

Esta Política de Seguridade da Información será efectiva desde a data de aprobación e ata que sexa substituída por una nova Política.

Santa Comba, 1 de agosto de 2024

O Alcalde.

Alberto Romar Landeira.