Deputación DA CORUÑA
www.dacoruna.gal
BOLETÍN OFICIAL DA PROVINCIA DA CORUÑA
D.L.: C-1-1958
BOP
BOLETÍN OFICIAL DE LA PROVINCIA DE A CORUÑA
MARTES, 2 DE DECEMBRO DE 2025 MARTES, 2 DE DICIEMBRE DE 2025 | BOP NÚMERO 231

ADMINISTRACIÓN LOCAL

MUNICIPAL

VEDRA

Secretaría-Intervención

Aprobación da Política de Seguridade da Infomación do Concello de Vedra

ANUNCIO

Aprobación da modificación da Política de Seguridade da Información do Concello de Vedra (Expediente núm. 2024/X999/0000044)

O Pleno do concello, en sesión ordinaria celebrada o día 26.11.2025, aprobou a modificación da Política de Seguridade da Información do Concello de Vedra, aprobada con data 24.04.2024 (BOP núm. 85/24, do 02 de maio), nos seus apartados 4 (Marco Normativo), 6 (Modelo de Gobernanza) e 7 (Protección de datos) que pasan a ter o seguinte contido:

"4.- MARCO NORMATIVO

O marco normativo que afecta ao desenvolvemento das actividades e competencias do Concello de Vedra, en materia de administración electrónica, e que esixe a implantación de medidas de seguridade nos sistemas de información, atópase recollido nun documento independente denominado RE-02 Rexistro de normas Xurídicas do Marco Legal e Regulador v3.xlsx.

Dito documento recopila a lexislación aplicable, así como as normas sectoriais, autonómicas e complementarias que resulten de aplicación, incluídas as Instrucións Técnicas de Seguridade aprobadas por resolución da Secretaría de Estado de Administracións Públicas e as guías de seguridade publicadas polo Centro Criptolóxico Nacional (CCN) no marco do Esquema Nacional de Seguridade.

A responsabilidade de manter actualizado o marco normativo correspóndelle ao Concello de Vedra, garantindo que dito documento independente estea dispoñible e accesible para todos os órganos e persoal suxeito ao ámbito de aplicación da presente política.

6.- MODELO DE GOBERNANZA

Para garantir o cumprimento do Esquema Nacional de Seguridade e establecer a organización da seguridade da información no Concello de Vedra, designaranse roles de seguridade e constituirase un Comité de Seguridade da Información.

6.1.- Roles ou perfís de seguridade

Para garantir o cumprimento e a adaptación das medidas esixidas regulamentariamente creáronse roles ou perfís de seguridade e designáronse os cargos ou órganos que os ocuparán, do seguinte xeito:

Responsable da Información: Alcalde -Presidente.

Responsable dos Servizos: Alcalde -Presidente.

Responsable de Seguridade: Secretaría -intervención.

Responsable do Sistema: Concelleiro de novas tecnoloxías.

6.2.- Comité de Seguridade da Información

Constituíuse un Comité de Seguridade da Información, como órgano colexiado, e está formado polos seguintes membros:

-Presidente/a: Alcalde –Presidente do concello.

-Secretario/a : Secretaría –Intervención do concello.

-Vogais:

- Responsable de Seguridade: Secretaría –Intervención do concello.
- Responsable do Sistema: Concelleiro de novas tecnoloxías.
- Delegado de Protección de Datos (DPD): empresa adxudicataria en cada momento con funcións de asesoramento e supervisión en materia de protección de datos.

Número de anuncio 2025/7958

Os responsables da información e dos servizos serán convocados en función dos asuntos a tratar.

Así mesmo, e con carácter opcional, poderán incorporarse aos labores do Comité grupos de traballo especializados, xa sexan de carácter interno, externo ou mixto.

Os membros do Comité serán renovados cada catro anos ou con ocasión de vacante.

6.3.- 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 á 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 e elaborar documentación do sistema.
- Determinar a categoría do sistema, en función das valoracións da información e os servizos realizados polos seus respectivos responsables.
- 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 á información ou prestación do servizo se ten 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 tipoloxía e a xestión do sistema de información establecendo os criterios de uso e os servizos dispoñibles no mesmo.
- Confirmar 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 o require, na elaboración e implantación dos plans de mellora da seguridade e, chegado o caso, nos plans de continuidade.
- Levar a cabo as funcións de administrador da seguridade do sistema.
- A xestión, configuración e actualización, de ser o 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 da 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.

Número de anuncio 2025/7958

- Monitorizar o estado de seguridade proporcionado polas ferramentas de xestión de eventos de seguridade e mecanismos de auditoría técnica.

6.4.- Funcións 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 iso encargarase de:
- Coordinar os esforzos da diferentes áreas en materia de seguridade da información, para asegurar que estes sexan consistentes, aliñados coa estratexia decidida na materia, e evitar duplicidades.
- Propoñer plans de mellora da seguridade da información, coa súa dotación orzamentaria correspondente, priorizando as actuacións en materia de seguridade cando os recursos sexa limitados.
- Velar porque a seguridade da información se teña en conta en todos os proxectos dende 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 apoien 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 súa aprobación en coordinación coa Dirección Xeral.
- 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 dende 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.

6.5.- Procedementos de designación

A designación dos Responsables identificados nesta política foi realizada pola Alcaldía do Concello de Vedra e comunicada ás partes afectadas.

Os roles de seguridade serán revisados cada catro anos; no caso de que exista unha vacante, a mesma deberá ser cuberta no prazo dun mes, seguindo o mesmo procedemento.

6.6.- Resolución de conflitos

Se houbese conflito entre os responsables, será resolto polo Comité de seguridade da información.

7.- DATOS DE CARÁCTER PERSOAL

O Concello de Vedra no tratamento dos datos persoais, cumpre cos principios e obrigas da normativa vixente, entre outra o Regulamento 679/2016, 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 –RXPD-) e a Lei Orgánica 3/2018, do 5 de decembro, de Protección de datos persoais e garantía de dereitos dixitais, respectando, en todo caso, o dereito fundamental á protección de datos persoais, á intimidade e o resto de dereitos fundamentais recoñecidos tanto na lexislación e tratados internacionais como na Constitución vixente."

Para xeral coñecemento publícase o contido íntegro da Política de Seguridade da Información do Concello de Vedra, logo da modificación acordada:

Número de anuncio 2025/7958

POLÍTICA DE SEGURIDADE DA INFORMACIÓN DO CONCELLO DE VEDRA

1.- INTRODUCIÓN

O Concello de Vedra, depende dos sistemas TIC (Tecnoloxías de Información e Comunicacións) para alcanzar os seus obxectivos, exercer as súas competencias e prestar os servizos que ten atribuídos. Estes sistemas deben ser administrados con dilixencia, tomando 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 rastrexabilidade da información e a 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 confirmarse 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.MISIÓN DE CONCELLO DE VEDRA

O Concello de Vedra, para a xestión dos seus intereses e das funcións e competencias que ten encomendadas, promove actividades e presta servizos públicos que contribúen a satisfacer as necesidades e aspiracións da poboación.

Para iso pon a disposición desta a realización de trámites en liña co obxectivo de impulsar a participación da cidadanía nos asuntos públicos establecendo, deste xeito, novas vías de participación que garantan o desenvolvemento da democracia participativa e a mellora da eficacia e eficiencia da acción pública.

Deséxase potenciar doutra banda 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, crear a confianza necesaria entre cidadán e Concello nesta relación.

3.ALCANCE

Esta Política aplicarase aos sistemas de información do Concello de Vedra, 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

O marco normativo que afecta ao desenvolvemento das actividades e competencias do Concello de Vedra, en materia de administración electrónica, e que esixe a implantación de medidas de seguridade nos sistemas de información, atópase recollido nun documento independente denominado RE-02 Rexistro de normas Xurídicas do Marco Legal e Regulador v3.xlsx.

Dito documento recopila a lexislación aplicable, así como as normas sectoriais, autonómicas e complementarias que resulten de aplicación, incluídas as Instrucións Técnicas de Seguridade aprobadas por resolución da Secretaría de Estado de Administracións Públicas e as guías de seguridade publicadas polo Centro Criptolóxico Nacional (CCN) no marco do Esquema Nacional de Seguridade.

A responsabilidade de manter actualizado o marco normativo correspóndelle ao Concello de Vedra, garantindo que dito documento independente estea dispoñible e accesible para todos os órganos e persoal suxeito ao ámbito de aplicación da presente política.

5.CUMPRIMENTO DOS REQUISITOS MÍNIMOS DE SEGURIDADE

O Concello de Vedra 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, implementará diversas medidas de seguridade proporcionais á natureza da información e os servizos a protexer e tendo en conta a categoría dos sistemas afectados.

Número de anuncio 2025/7958

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 Vedra, 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 aos seus responsables xerárquicos, para evitar que, a ignorancia, a falta de organización e coordinación, ou de 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:

a) O sistema proporcionará a funcionalidade imprescindible para que a organización alcance os seus obxectivos competenciais ou contractuais.

b) As funcións de operación, administración e rexistro de actividade serán as mínimas necesarias, e asegurarase que só son desenvolvidas polas persoas autorizadas, desde emprazamentos ou equipos así mesmo autorizados; podendo esixirse, no seu caso, restricións de horario e puntos de acceso facultados.

c) Nun sistema de explotación eliminaranse ou desactivarán, 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.

d) 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, reavaliación periódica e Integridade, actualización do sistema e mellora continua do proceso de seguridade

A vixilancia continua por parte do Concello de Vedra 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 reavaliarán e actualizarán periodicamente, adecuando a súa eficacia á evolución dos riscos e os sistemas de protección, podendo chegar a unha reconsideración 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 persoal, propio ou alleo relacionado cos sistemas de información do Concello de Vedra, 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 se seguen os procedementos establecidos.

O significado e alcance do uso seguro do sistema concretarase e plasmarase 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 auditada 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 esixirase que as organizacións que nos proporcionan servizos conten con profesionais cualificados e cuns niveis idóneos de xestión e madurez dos servizos prestados.

Xestión da seguridade baseada nos riscos, análises 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.

Número de anuncio 2025/7958

A xestión dos riscos permitirá o mantemento dunha contorna controlada, minimizando os riscos a niveis aceptables. A redución a estes niveis realizarase mediante unha apropiada aplicación de medidas de seguridade, de maneira equilibrada e proporcionada á natureza da información tratada, dos servizos para 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, empregarase 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 Vedra, 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 dos leitos de comunicación ás partes interesadas.

A seguridade do sistema contemplará as accións relativas aos aspectos de prevención, detección e resposta, co 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 ciberincidente.

As medidas de resposta xestionaranse en tempo oportuno, estarán orientadas á restauración da información e aos 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 Vedra, implementará 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 controlarase 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 Vedra organizou 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” do presente documento.

Autorización e control dos accesos

O Concello de Vedra implementará 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 Vedra implementará 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 protección 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 Vedra terá en conta a utilización de forma proporcionada á categoría do sistema e ao 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.

Número de anuncio 2025/7958

Protección da información almacenada e en tránsito e continuidade da actividade

O Concello de Vedra 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 real decreto, cando iso sexa esixible.

Toda información en soporte non electrónico que fose causa ou consecuencia directa da información electrónica á que se refire este 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 dispoñerán de copias de seguridade e estableceranse os mecanismos necesarios para garantir a continuidade das operacións en caso de perda dos medios habituais.

Rexistro de actividade e detección de código daniño

O Concello de Vedra, co propósito de satisfacer o obxecto do decreto , 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.

Ao 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 Vedra terá en conta que a utilización de infraestruturas e servizos comúns das administracións públicas, incluídos os compartidos ou transversais, facilitará o cumprimento do disposto no decreto.

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

O Concello de Vedra 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 no Concello de Vedra, designaranse roles de seguridade e constituirase un Comité de Seguridade da Información.

6.1.- Roles ou perfís de seguridade

Para garantir o cumprimento e a adaptación das medidas esixidas regulamentariamente creáronse roles ou perfís de seguridade e designáronse os cargos ou órganos que os ocuparán, do seguinte xeito:

Responsable da Información: Alcalde -Presidente.

Responsable dos Servizos: Alcalde -Presidente.

Responsable de Seguridade: Secretaría -intervención.

Responsable do Sistema: Concelleiro de novas tecnoloxías.

6.2.- Comité de Seguridade da Información

Constituíuse un Comité de Seguridade da Información, como órgano colexiado, e está formado polos seguintes membros:

- Presidente/a: Alcalde –Presidente do concello.
- Secretario/a : Secretaría –Intervención do concello.

Número de anuncio 2025/7958

- Vogais:
  - Responsable de Seguridade: Secretaría –Intervención do concello.
  - Responsable do Sistema: Concelleiro de novas tecnoloxías.
  - Delegado de Protección de Datos (DPD): empresa adxudicataria en cada momento con funcións de asesoramento e supervisión en materia de protección de datos.

Os responsables da información e dos servizos serán convocados en función dos asuntos a tratar.

Así mesmo, e con carácter opcional, poderán incorporarse aos labores do Comité grupos de traballo especializados, xa sexan de carácter interno, externo ou mixto.

Os membros do Comité serán renovados cada catro anos ou con ocasión de vacante.

6.3.- 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 á 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 e elaborar documentación do sistema.
- Determinar a categoría do sistema, en función das valoracións da información e os servizos realizados polos seus respectivos responsables.
- 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 á información ou prestación do servizo se ten 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 tipoloxía e a xestión do sistema de información establecendo os criterios de uso e os servizos dispoñibles no mesmo.
- Confirmar 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 o require, na elaboración e implantación dos plans de mellora da seguridade e, chegado o caso, nos plans de continuidade.
- Levar a cabo as funcións de administrador da seguridade do sistema.
- A xestión, configuración e actualización, de ser o 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.

Número de anuncio 2025/7958

- Aprobar os cambios na configuración vixente do sistema da 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.

6.4.- Funcións 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 iso encargarase de:
  - Coordinar os esforzos da diferentes áreas en materia de seguridade da información, para asegurar que estes sexan consistentes, aliñados coa estratexia decidida na materia, e evitar duplicidades.
  - Propoñer plans de mellora da seguridade da información, coa súa dotación orzamentaria correspondente, priorizando as actuacións en materia de seguridade cando os recursos sexa limitados.
  - Velar porque a seguridade da información se teña en conta en todos os proxectos dende 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 apoien 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 súa aprobación en coordinación coa Dirección Xeral.
  - 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 dende 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.

6.5.- Procedementos de designación

A designación dos Responsables identificados nesta política foi realizada pola Alcaldía do Concello de Vedra e comunicada ás partes afectadas.

Os roles de seguridade serán revisados cada catro anos; no caso de que exista unha vacante, a mesma deberá ser cuberta no prazo dun mes, seguindo o mesmo procedemento.

6.6.- Resolución de conflitos

Se houbese conflito entre os responsables, será resolto polo Comité de seguridade da información.

7.- DATOS DE CARÁCTER PERSOAL

O Concello de Vedra no tratamento dos datos persoais, cumpre cos principios e obrigas da normativa vixente, entre outra o Regulamento 679/2016, 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 –RXPD-) e a Lei Orgánica 3/2018, do 5 de decembro, de

Número de anuncio 2025/7958

Protección de datos persoais e garantía de dereitos dixitais, respectando, en todo caso, o dereito fundamental á protección de datos persoais, á intimidade e o resto de dereitos fundamentais recoñecidos tanto na lexislación e tratados internacionais como na Constitución vixente."

8.-DESENVOLVEMENTO DA POLÍTICA DE SEGURIDADE DA INFORMACIÓN

O cumprimento dos obxectivos marcados nesta Política de Seguridade leva 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 da presente Política corresponde ao Responsable de Goberno, propoñendo 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 preste servizos a outros organismos, ou manexe información doutros organismos, faráselles partícipe desta Política de Seguridade da Información. O Concello de Vedra 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 Vedra utilice servizos de terceiros ou ceda información a terceiros, faráselles partícipe desta Política de Seguridade e da Normativa de Seguridade existente que incumba aos devanditos servizos ou información. Esta 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 provean 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. Devandito informe deberá ser aprobado polos responsables de información e os servizos, con carácter previo ao comezo da relación coa terceira parte."

Vedra, 27 de novembro de 2025

O Alcalde

Asdo. Carlos Martínez Carrillo

2025/7958

Número de anuncio 2025/7958