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

ADMINISTRACIÓN LOCAL

MUNICIPAL

CARRAL

Política da seguridade da información do Concello de Carral

ANUNCIO

EXPEDIENTE: 2024/G013/000002

O Pleno do Concello de Carral, na sesión ordinaria celebrada o 29 de xullo de 2024 acordou aprobar Política de seguridade da información do Concello de Carral (a cal entrou en vigor o mesmo día de aprobación polo pleno) co seguinte contido:

PRIMEIRO .- Aprobar a Política de seguridade da información do Concello de Carral co seguinte contido

1.- INTRODUCIÓN

O Concello de Carral depende dos sistemas TIC (Tecnoloxías de Información e Comunicacións) para alcanzar os seus obxectivos. 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 calidade 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 as necesidades de financiamento 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 CARRAL

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

Para iso pon ao dispor desta a realización de trámites online 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 eficacia 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 Carral 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 alcance do Esquema Nacional de Seguridade (ENS).

4.-MARCO NORMATIVO

A base normativa que afecta o desenvolvemento das actividades e competencias do Concello de Carral no que a administración electrónica refírese, e que implica a implantación de forma explícita de medidas de seguridade nos sistemas de información, está constituída pola seguinte lexislación:

Número de anuncio 2024/5806

• 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 3/2011, 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 deroga a Directiva 95/46/CE (Regulamento xeral de protección de datos, RGPD).

• Lei 36/2015 26 setembro de seguridade nacional

• Lei 6/2020 do 11 de novembro reguladora de determinados aspectos dos servizos electrónicos de confianza

• Regulamento (UE) 910/2014 do Parlamento Europeo e do Consello do 23 de xullo de 2014 relativo a identificación elect´ronica dos servizos de confianza nas transaccións electrónicas no mercado interior e polo que se deroga a directiva 1999/93/CE (regulamento eIDAS)

• Real decreto 1308/1992 do 23 de outubro polo que se delcara 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 reutilización da información do sector público.

• Lei 57/2003, do 16 de decembro, de medidas para a modernización do goberno local.

• Real Decreto 1553/2005, do 23 de decembro, polo que se regula o documento nacional de identidade e os seus certificados de sinatura electrónica.

• Lei 37/2007, do 16 de novembro, sobre reutilización da información do sector público.

• 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 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 9/2014, do 9 de maio, Xeneral de Telecomunicacións (vixente nos apartados sinalados na disposición derrogatoria única da lei 11/2022 do 28 de xuño)

• Lei 11/2022 de 2/8 de xuño xeral de telecomunicacións

• Lei 7/1985, do 2 de abril, Reguladora das Bases do Réxime Local, modificada pola lei 11/1999, do 21 de abril.

• 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.

Número de anuncio 2024/5806

• Lei 9/2017, do 8 de novembro, de Contratos do Sector Público, pola que se transpoñen ao ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23/UE e 2014/24/UE, de 26 de febrer de 2014.

• Real Decreto-lei 14/2019, do 31 de outubro, polo que se adoptan medidas urxentes por razóns de seguridade pública en materia de administración dixital, contratación do sector público e telecomunicacións.

• Lei 9/2017, do 8 de novembro, de Contratos do Sector Público, pola que se transpoñen 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.

• Política de sinatura electrónica do Concello de Carral

• Ordenanza de Administración Electrónica do Concello de Carral.

Tamén forman parte do marco normativo as restantes normas aplicables á Administración Electrónica do Concello de Carral derivadas das anteriores e publicadas nas sedes electrónicas comprendidas dentro do ámbito de aplicación da presente Política.

O mantemento do marco normativo será responsabilidade do Concello de Carral e manterase nun Anexo a este documento. Incluídas 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, a proposta do Comité Sectorial de Administración Electrónica e a iniciativa do Centro Criptológico Nacional (CCN) tal e como se establece en Rd 311/2022.

Así mesmo, o Concello de Carral tamén será responsable de identificar as guías de seguridade do CCN, referenciadas no mencionado artigo, 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 Carral 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 para 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 Carral 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, constituír 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 alcance os seus obxectivos competenciais ou contractuais.

• 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.

• 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.

• 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, reevaluación periódica e Integridade, actualización do sistema e mellora continua do proceso de seguridade

A vixilancia continua por parte do Concello de Carral 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.

Número de anuncio 2024/5806

As medidas de seguridade se reevaluarán 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 monitoraxe permanentes permitirán adecuar o estado de seguridade dos sistemas atendendo as 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 a persoa, propio ou alleo relacionado cos sistemas de información do Concello de Carral dentro do ámbito do ENS, serán formados e informados dos seus deberes, obrigacións 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 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 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.

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/II do ENS 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 Carral dispón de procedementos de xestión de incidentes de seguridade 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, ao obxecto de minimizar as súas vulnerabilidades e lograr que as ameazas sobre o mesmo non materialícense ou que, no caso de facelo, non afecten gravemente á información que manexa ou aos servizos que aguzosa.

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 os 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 Carral 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

Número de anuncio 2024/5806

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 se conecta a redes públicas, tal e como se definen na Lei 9/2014, do 9 de maio, Xeneral 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 Carral 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 "ORGANIZACIÓN DA SEGURIDADE" do presente documento.

Autorización e control dos accesos

O Concello de Carral 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 Carral 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 Carral 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 Carral prestará especial atención á información almacenada ou en tránsito a través dos equipos ou dispositivos portátiis 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 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 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 Carral co propósito de satisfacer o obxecto deste real 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 monitorar, 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 preditas redes e sistemas de información.

Número de anuncio 2024/5806

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 Carral 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 Real Decreto 3/2011, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade. neste real decreto.

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

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

6.-ORGANIZACIÓN DA SEGURIDADE

Para garantir o cumprimento do Esquema Nacional de Seguridade e establecer a organización da seguridade da información, adaptada ás necesidades e particularidade deste Concello, tendo en conta a estrutura actual , organización e persoal do Concello de Carral o decreto no que se organiza a seguridade do Concello de Carral segue un marco de goberno baseado en bloques de responsabilidades polo que se propón unha designación de roles por bloques de responsabilidade : goberno, supervisión e operación .

6.1.-Bloque de goberno:

Responsable de goberno cuxas funcións serán exercidas polo Alcalde Presidente e integra os seguintes roles e funcións do ENS:

-Comité de seguridade da información

-Responsable de información .

-Responsable do servizo .

A Alcaldía-Presidencia poderá delga restes roles e/ou funcións nun/unha uns/unhas concelleiros/as.

6.2.- Bloque executivo /supervisión

6.2.1.- Responsable da Supervisión cuxas funcións serán desempeñadas por (Secretario /a Habilitado Nacional do Concello de Carral que contará co asesoramento necesario a solicitar á Deputación Provincial e axentes externos que poida contratar o Concello de Carral e teñan coñecementos específicos nesta materia) que integra o seguinte Rol ENS:

-Responsable de seguridade

6.2.2.-Delegado/a de Protección de datos que apoiará o responsable de supervisión con funciónes de asesoramento e supervisión en materia de protección de datos rol a desempeñar por Persoa fisica ou xurídica contratada para estes servizos polo Concello de Carral)

6.3.-Bloque de operación , ocupado por persoal adscrito ao posto de informático da RPT do Concello de Carral que integra as seguintes funcións asociadas ao ENS.

Responsable do Sistema.

Contará co asesoramento necesario a solicitar á Deputación Provincial e axentes externos que poida contratar o Concello de Carral e teñan coñecementos específicos nesta materia)

6.4.- 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 o 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.

Número de anuncio 2024/5806

• 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.

• Confirmarse de que as medidas específicas de seguridade intégrense 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 monitoraxe 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 axústanse ás autorizacións pertinentes.

• Monitorar o estado de seguridade proporcionado polas ferramentas de xestión de eventos de seguridade e mecanismos de auditoría técnica.

Funcións particulares do Responsable de Gobierno e Supervisión

O Responsable de Gobierno e Supervisión asumirá as funcións propias dun Comité de Seguridade:

Atender as solicitudes, en materia de Seguridade da Información, da Administración e dos diferentes roles de seguridade e/ou áreas informando regularmente o 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 das 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 sexan limitados.

Velar porque a Seguridade da Información se teña 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 apoien un funcionamento homoxéneo de todos os sistemas TIC.

Realizar un seguimento dos principais riscos residuais asumidos pola Administración e recomendar posibles actuacións respecto de eles.

Número de anuncio 2024/5806

Realizar un seguimento da xestión dos incidentes de seguridade e recomendar posibles actuacións respecto de eles.

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 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 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 obrigacións da Administración en materia de seguridade da Información.

Procedementos de designación:

Os roles de seguridade quedan asignados aos postos organizativos sinalados nesta política e en decreto do Alcalde de Carral notificado ás partes quedando automaticamente designados os seus titulares en cada momento.

Establécese que polo Alcalde é o órgano con potestade para modificar os roles establecidos, incoando ante a modificación expediente de revisión do presente documento de Política de Seguridade así como a tramitación de expedientes administrativos (modificación RPT , etc..) necesarios para a materialización das devanditas modificacións de roles.

Os roles de seguridade serán revisados cada [catro anos] ou con ocasión de vacante neste caso deberá ser cuberta no prazo dun mes seguindo o mesmo procedemento.

Reportes

O responsable de Operación reportará ao Responsable de Gobierno e Supervisión, as actuacións en materia de seguridade que puidesen executarse e especificamente, as actividades desenvolvidas na arquitectura e infraestrutura tecnolóxica do Concello.

O responsable de Operación reportará ao Responsable de Gobierno e Supervisión reportará de maneira inmediata calquera incidente de seguridade que puidese detectarse, e elevará ao mesmo en todo caso, informes consolidados dos incidentes de seguridade, cambios no sistema de información e adquisicións de produtos ou servizos de seguridade.

O Responsable de Gobierno e Supervisión reportará directamente ao Pleno , todos os asuntos relacionados coa seguridade do Concello. Anualmente elevará un resumo consolidado de todas as actuacións en materia de seguridade e dos incidentes de seguridade que sucedesen no Concello. No devandito resumo informarase á corporación do estado de seguridade desta, e do risco residual presentado.

Resolución de conflitos

Se houbese conflito entre os Responsables, será resolto polo Alcalde ou no órgano no que delegue.

7.-DATOS DE CARÁCTER PERSOAL

O Concello de Carral só recollerá datos de carácter persoal cando sexan adecuados, pertinentes e non excesivos e estes atópense en relación co ámbito e as finalidades para os que se obtiveron. De igual modo, adoptará as medidas de índole técnica e organizativas necesarias para o cumprimento da normativa de Protección de Datos vixente en cada caso.

Á vista da entrada en aplicación, o día 25 de maio de 2018, do 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 deroga a Directiva 95/46/CE (Regulamento xeral de protección de datos) e a súa translación á lexislación española coa Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais, adoptaranse as medidas oportunas talles como, a análise de lexitimidade xurídica de cada un dos datos tratamentos de datos que leven a cabo, a análise de riscos, a avaliación de impacto se o risco é alto, o rexistro de actividades e o nomeamento de quen vaia a desempeñar as funcións de Delegado de Protección de Datos.

En desenvolvemento dos principios da citada normativa d eprotección de datos en tre outros os de minimización, confidencialidade ou proactividad, o Concello de Carral definirá un marco de actuación na política de protección de datos mediante o establecemento dunha Política de privacidade que estará dispoñible na sede electrónica e a seb municipal, e o rexistro de actividades de tratameinto de datos persoais do Concello de Carral a crear por decreto do Alcalde que estará dispoñible na sede electrónica e no Portal de transparencia municipal.

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.

Número de anuncio 2024/5806

Para a súa organización definirase 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 Gobierno e Supervisión, propoñendo no caso de que sexa necesario melloras da mesma, para a súa aprobación por parte do mesmo órgano que a aprobou inicialmente.

Esta Política de Seguridade desenvolverase mediante a elaboración doutras políticas ou normativas de seguridade que aborden aspectos específicos. A raíz das devanditas políticas e normativas poderanse desenvolver procedementos que describan a forma de levalas a cabo.

A aprobación e revisión dos documentos anteriormente apuntados farase conforme ao seguinte:

.- Política de Seguridade da Información: será aprobada polo Pleno do Concello de Carral sendo responsabilidade do Responsable de goberno e supervisión a súa revisión para elevar unha proposta de modificación cando sexa necesario.

.- Normativa Interna de seguridade da información: será aprobada polo Responsable de goberno e supervisión (Alcalde ou Junta de goberno local) actuando como Comité de Seguridade da Información, sendo o Responsable de Seguridade da Información o responsable da súa elaboración e actualización.

Procedementos operativos de seguridade da información: será aprobada polo Responsable de goberno e supervisión (Alcalde ou Junta de goberno local) actuando como Comité de Seguridade , sendo o Responsable de Seguridade da Información o responsable da súa elaboración e actualización.

A documentación de políticas e normativas de seguridade, así como esta Política de Seguridade atoparase ao dispor de todo o persoal da organización que necesite coñecela e, en particular, o persoal que utilice, operar ou administre os sistemas de información e comunicacións ou a información mesma albergada nos devanditos sistemas ou os servizos prestados polo Concello de Carral .

9.-TERCEIRAS PARTES

Cando o preste servizos a outros organismos, ou manexar información doutros organismos, faráselles partícipe desta Política de Seguridade da Información. O Concello de Carral 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 Carral utilice servizos de terceiros ou ceder 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 obrigacións 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 obrigación de cumprir co disposto nas Instrucións Técnicas de Seguridade recollida na Disposición adicional segunda (Desenvolvemento do Esquema Nacional de Seguridade) do Real Decreto Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade, e en consideración á 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, onde se establece que os operadores do sector privado que presten servizos ou prover 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 requírese nos parágrafos anteriores, requirirase un informe do Responsable de Seguridade da información que precise os riscos en que se incorre e a forma de tratalos. Requirirase a aprobación deste informe polos responsables da información e os servizos afectados con carácter previo ao comezo da relación coa terceira parte

APROBACIÓN E ENTRADA EN VIGOR

Texto aprobado o día _____ de _____ de_____ por acordo en sesión_____ plenaria do Concello de Carral

Esta "Política de Seguridade da Información", en diante Política, será efectiva desde a devandita data e ata que sexa substituída por unha nova Política.

Número de anuncio 2024/5806

SEGUNDO.- Que esta Política de seguridade da información do Concello de Carral sexa publicada no BOP así como no taboleiro de anuncios da sede electrónica municipal comunicando a mesma a todo o persoal e contratistas o Concello de Carral e iníciese a tramitación de procedementos de contratación necesarios para garantir o cumprimento da mesma así como modificacións na Relación de postos de traballo e adaptación de acordos organizativos que permitan e garantan a súa plena aplicación

Concello de Carral, 13 de agosto de 2024

O Alcalde

Francisco Javier Gestal Pose

2024/5806