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

A BAÑA

Aprobación da política de seguridade do Concello da Baña - ENS

Aprobación da política de seguridade do Concello da Baña.

Expte. TEDEC: 2023/X999/000028.

O Pleno do Concello da Baña, na sesión do día 7 de febreiro de 2024, acordou aprobar a política de seguridade nos termos que a continuación se recollen:

Dáse conta do ditame da Comisión Informativa Única Asuntos do Pleno con data do 2 de febreiro de 2024 que deseguido se transcribe:

"DITAME DA COMISIÓN DE ASUNTOS DO PLENO RELATIVO Á APROBACIÓN DA POLÍTICA DE SEGURIDADE DO CONCELLO DA BAÑA.

Expte. TEDEC: 2023/X999/000028 (Ciberseguridade).
Expte. TEDEC: 2024/G006/000016 (Proposta)
Expte. TEDEC: 2024/G012/000004 (Comisión Informativa).
Expte. TEDEC: 2024/G010/000002 (Pleno).

Vista a resolución de Alcaldía de data 28/03/023, con número de Decreto 174/2023, mediante a que se acorda a adhesión do Concello da Baña á Oficina Técnica de Ciberseguridade Provincial da Deputación da Coruña e a realización de todos aqueles trámites oportunos para establecer a relación de colaboración entre as dúas Administracións a través do acto ou documento correspondente.

Visto que en dito Decreto exponse que a través desta oficina a Deputación da Coruña ofrecerá asesoramento especializado na adecuación á normativa de seguridade da información e de protección de datos, na xestión e mellora continua do modelo de gobernanza da ciberseguridade e no apoio na xestión das cibercrises. Trátase de asegurar o cumprimento normativo no ámbito da seguridade da información e a protección de datos: fundamentalmente o Esquema Nacional de Seguridade (en diante ENS), o Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello do 27 de abril de Protección de Datos de Carácter Persoal (RGPD) e a Lei Orgánica de Protección de Datos Persoais e Garantía dos Dereitos Dixitais (LOPDGDD) xunto coa adopción das medidas técnicas, organizativas e normativas necesarias para minimizar o risco.

Visto que o cronograma deste proxecto de adhesión é o seguinte:

- Confirmación do interese do concello en participar na iniciativa; a través do representante da entidade local, mediante a adhesión á Oficina Técnica Provincial de Ciberseguridade. [Solicitude dispoñible en SUBTEL: OTS-Adhesión].
- Diagnose inicial de cumprimento.
- Aprobación da Política de Seguridade e elaboración do Plan de adecuación.
- Implantación de seguridade.
- Proceso de verificación da conformidade.
- Auditoría e certificación.
- Ciclo de mellora continua.

Visto que o Concello da Baña ven de aprobar con carácter definitivo a ordenanza de Administración electrónica no pleno ordinario celebrado o 27 de setembro de 2023 (BOP A Coruña núm.: 189, de 03/10/2023), ó abeiro da realización inicial do cumprimento a través da solución INES (Centro Criptolóxico Nacional).

Visto que ó abeiro e dita diagnose tamén se debe proceder á aprobación da política de seguridade, empregando o modelo fornecido polo Centro Criptolóxico Nacional e a Oficina de Ciberseguridade da Deputación Provincial da Coruña, o cal se anexa ó presente acordo.

Número de anuncio 2024/1055

Visto que consta toda a documentación precisa para a súa aprobación no expediente, incluíndo decretos de designación de roles e de adhesión á política de sinatura electrónica da Administración Xeral do Estado.

Vistas as intervencións dos membros da Comisión de Asuntos do Pleno, as cales se recollen a continuación:

· O Alcalde, don Jose Antonio Pereira Gil, introduce brevemente a proposta de ditame e dálle paso ó Secretario – Interventor, don Ricardo Garrido Caneda, para que detalle máis polo miúdo dita proposta.

· Non se realizan máis intervencións de consideración.

En virtude do disposto nos artigos 123 e ss. do Real Decreto 2568/1986, de 28 de novembro, mediante o que se aproba o Regulamento de organización e, funcionamento e réxime xurídico das Entidades Locais, esta comisión informativa ditamina, por unanimidade dos presentes, o seguinte:

PRIMEIRO. Aprobar a política de seguridade do Concello da Baña, a cal se anexa ó presente acordo. Esta Política de Seguridade ten sido desenvolta tendo en conta os principios básicos i en base ós requisitos mínimos de seguridade establecidos pola normativa do Esquema Nacional de Seguridade e conforme ó esixido no Anexo II do Real Decreto 311/2022, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade.

SEGUNDO. Publicar a política de seguridade do Concello da Baña no Boletín Oficial da Provincia da Coruña, así como na Sede Electrónica municipal.

TERCEIRO. Facultar ó Sr. Alcalde-Presidente para subscribir e asinar toda clase de documentos relacionados con este asunto.

CUARTO. Dar traslado do presente acordo ós servizos municipais responsables da súa tramitación, así como a notificación ós terceiros interesados no expediente."

En virtude do disposto nos artigos 123 e ss. do Real Decreto 2568/1986, de 28 de novembro, mediante o que se aproba o Regulamento de organización e, funcionamento e réxime xurídico das Entidades Locais, o Pleno da Corporación acorda, por unanimidade:

PRIMEIRO. Aprobar a política de seguridade do Concello da Baña, a cal se anexa ó presente acordo. Esta Política de Seguridade ten sido desenvolta tendo en conta os principios básicos i en base ós requisitos mínimos de seguridade establecidos pola normativa do Esquema Nacional de Seguridade e conforme ó esixido no Anexo II do Real Decreto 311/2022, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade.

SEGUNDO. Publicar a política de seguridade do Concello da Baña no Boletín Oficial da Provincia da Coruña, así como na Sede Electrónica municipal.

TERCEIRO. Facultar ó Sr. Alcalde-Presidente para subscribir e asinar toda clase de documentos relacionados con este asunto.

CUARTO. Dar traslado do presente acordo ós servizos municipais responsables da súa tramitación, así como a notificación ós terceiros interesados no expediente.

Número de anuncio 2024/1055

ANEXO - POLÍTICA DE SEGURIDADE

ÍNDICE

1. APROBACIÓN I ENTRADA EN VIGOR

Texto aprobado o día 31 de xaneiro de 2024 por acordo Plenario do Concello da Baña.

Esta "Política de Seguridade da Información", en diante Política, será efectiva dende dita data e ata que sexa reemplazada por unha nova Política.

2.- INTRODUCIÓN

O Concello da Baña, 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 axeitadas para protexe-los 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 e a prestación continuada dos servizos, actuando preventivamente, supervisando a actividade diaria e reaccionando con presteza ós 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 dunha estratexia que se adapte ós cambios nas condicións do entorno para garantir a prestación continua dos servizos. Isto implica que os departamentos deben aplica-las medidas mínimas de seguridade esixidas polo Esquema Nacional de Seguridade, así como realizar un seguimento continuo dos niveis de prestación de servizos, seguir e analiza-las vulnerabilidades reportadas, e preparar unha resposta efectiva ós 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, dende 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 nos pregos de licitación para proxectos de TIC.

3.- MISIÓN DO CONCELLO DA BAÑA

O Concello da Baña, para a xestión dos seus intereses e das funcións e competencias que ten asignadas en diferentes normas ou convenios, promove actividades e presta servizos públicos que contribúen a satisfacer as necesidades e aspiracións da poboación. Para isto pon a disposición desta a realización de trámites online 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 i eficiencia da acción pública.

Deséxase potenciar por outro lado 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 precisa entre cidadán e Concello nesta relación.

Número de anuncio 2024/1055

4.- ALCANCE

Esta Política aplicarase ós sistemas de información do Concello da Baña, que están relacionados co exercicio de dereitos por medios electrónicos, co cumprimento de deberes por medios electrónicos ou co acceso á información ou ó procedemento administrativo e que se atopan dentro do ámbito de aplicación do Esquema Nacional de Seguridade (ENS).

5.- MARCO NORMATIVO

A base normativa que afecta ó desenvolvemento das actividades e competencias do Concello da Baña, no que a 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, de 1 de outubro, do Procedemento Administrativo Común das Administracións Públicas.
- Lei 40/2015, de 1 de outubro, de Réxime Xurídico do Sector Público.
- Real Decreto 311/2022, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade.
- Real Decreto 4/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Resolución de 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 de 7 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade do Informe do Estado da Seguridade.
- Resolución de 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 de 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, de 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.
- Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, de 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ó tratamento de datos persoais e a la libre circulación destes datos e polo que se deroga a Directiva 95/46/CE (Regulamento xeral de protección de datos, RGPD).
- Lei 36/2015, de 28 de setembro, de Seguridade Nacional.
- Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos servizos electrónicos de confianza.
- O Regulamento (UE) Nº 910/2014 do Parlamento Europeo e do Consello, de 23 de xullo de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo á identificación electrónica e os 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, de 23 de outubro, polo que se declara ó Laboratorio do Real Instituto e Observatorio da Armada, como Laboratorio depositario do patrón nacional de Tempo e Laboratorio asociado ó Centro Español de Metroloxía.
- Lei 34/2002, de 11 de xullo, de servizos da sociedade da información e do comercio electrónico.
- Lei 37/2007, de 16 de novembro, sobre reutilización da información do sector público.
- Lei 34/2002, de 11 de xullo, de servizos da sociedade da información do comercio electrónico.
- Real Decreto 1553/2005, de 23 de decembro, polo que se regula o documento nacional de identidade e os seus certificados de sinatura electrónica.
- Lei 25/2007, de 18 de outubro, de conservación de datos relativos ás comunicacións electrónicas e ás redes públicas de comunicacións.
- Lei 56/2007, de 28 de decembro, de Medidas de Impulso da sociedade da Información.
- Real Decreto 1494/2007, de 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, de 24 de outubro, polo que se desenvolve a Lei 37/2007, de 16 de novembro, sobre reutilización da información do sector público, para o ámbito do sector público estatal.
- Lei 19/2013, de 9 de decembro, de transparencia, acceso á información pública e bo goberno.
- Lei 25/2013, de 27 de decembro, de Impulso da factura electrónica e creación do Rexistro electrónico de facturas no sector público.
- Lei 7/1985, de 2 de abril, Reguladora das Bases do Réxime Local, modificada pola lei 11/1999, de 21 de abril.
- Lei 16/1985, de 25 de xuño, do Patrimonio Histórico Español (arquivo).

Número de anuncio 2024/1055

- Real Decreto Lexislativo 1/1996, de 12 de abril, polo que se aproba o Texto Refundido da Lei de Propiedade Intelectual.
- Real Decreto Lexislativo 5/2015, de 30 de outubro, polo que se aproba o texto refundido da Lei do Estatuto Básico do Empregado Público.
- Lei 9/2017, de 8 de novembro, de Contratos do Sector Público, pola que se traspoñen ó ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23/UE e 2014/24/UE, de 26 de febreiro de 2014.
- Lei 9/2014, de 9 de maio, Xeral de Telecomunicacións (Vixente nos apartados sinalados na Disposición Derogatoria Única da Lei 11/2022, de 28 de xuño).
- Real Decreto 203/2021, de 30 de marzo, polo que se aproba o Regulamento de actuación e funcionamento do sector público por medios electrónicos.
- Lei 11/2022, de 28 de xuño, Xeral de Telecomunicacións (segundo prazos entrada en vigor de Disposición desta Lei).
- Política de sinatura electrónica do Concello da Baña, adherido á política da Administración Xeral do Estado.
- Regulamento polo que se establece a Sede Electrónica do Concello da Baña, Ordenanza de Administración Electrónica municipal.

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

O mantemento do marco normativo será responsabilidade do Concello da Baña, e manterase nun Anexo a este documento. Incluído 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 Criptolóxico Nacional (CCN) tal e como se establece no Real Decreto.

Así mesmo, o Concello da Baña, 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.

6.- CUMPRIMENTO DOS REQUISITOS MÍNIMOS DE SEGURIDADE

O Concello da Baña, para lograr o cumprimento do Real Decreto 311/2022, de 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 os 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 da Baña, 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 desenvoltas 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 será 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.

Número de anuncio 2024/1055

Vixilancia continua, reavaliación periódica e Integridade, actualización do sistema e mellora continua do proceso de seguridade.

A vixilancia continua por parte do Concello da Baña 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 reavaliaranse e actualizaranse 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 a persoa, propio ou alleo relacionado cos sistemas de información do Concello da Baña, 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 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 proporcionen 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 ó que estean expostos.

Esta xestión realizarase por medio da análise e tratamento dos riscos aos que está exposto o sistema. 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 da Baña, 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 das vías de comunicación ás partes interesadas.

A seguridade do sistema contemplará as accións relativas ós aspectos de prevención, detección e resposta, ó 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 ós 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 os servizos que puidesen verse afectados por un incidente de seguridade.

Número de anuncio 2024/1055

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

De igual xeito, 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 da Baña, despregа 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 fora comprometida permita desenvolver unha reacción adecuada fronte ós 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 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 da Baña, organiza a súa seguridade comprometendo a tódolos 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 da Baña, despregou mecanismos de control de acceso ó sistema de información, limitándoo ós usuarios, procesos, dispositivos e outros sistemas de información, debidamente autorizados, e exclusivamente ás funcións permitidas.

Protección das instalacións

O Concello da Baña, despregou mecanismos de control de acceso físico, previndo os accesos físicos non autorizados, así como os danos á información e ós 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 da Baña, 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 ó sinalado en canto á profesionalidade.

Protección da información almacenada e en tránsito e continuidade da actividade

O Concello da Baña, 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 (ENS), 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 (ENS), 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.

Rexistro de actividade e detección de código daniño

O Concello da Baña, co propósito de satisfacer o obxecto deste real decreto (ENS), 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.

Número de anuncio 2024/1055

Ó 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 ós 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 da Baña, terá en conta que a utilización de infraestruturas e servizos comúns das Administracións Públicas, incluídos os compartidos ou transversais, facilitará o cumprimento do disposto neste real decreto (ENS).

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

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

7.- 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, proponse unha designación de roles por bloques de responsabilidade: Goberno, Supervisión e Operación.

De acordo con esta estrutura, asignáronse 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:
  - o Comité de Seguridade da Información.
  - o Responsable da Información.
  - o Responsable do Servizo.
- A Alcaldía-Presidencia pode delegar estos roles e/ou funcións nun Concelleiro/a ou Concelleiros/as.

Bloque Executivo/Supervisión:

- **Responsable de Supervisión**, cuxas funcións exercita a Secretaría-Intervención do Concello, e que integra o seguinte rol ENS:
  - o Responsable da Seguridade.
- **Delegado Protección de Datos (DPD)**, cuxas funcións exercita a empresa contratada atal efecto, apoiando ó Responsable de Supervisión, con funcións de asesoramento e supervisión en materia de protección de datos.

Bloque de Operación:

- **Responsable de Operación**, cuxas competencias exercita un empregado municipal que ocupa o posto como Persoal Técnico Informático ou, no seu caso, empresa contratada a tal efecto, e que integra o seguinte rol ENS:
  - o Responsable do Sistema.

7.1.- Responsabilidades asociadas ó Esquema Nacional de Seguridade

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

1.- Funcións do Responsable da Información e dos Servizos:

- Establecer e aprobar os requisitos de seguridade aplicables ó 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 ó Servizo e á Información.

2.- 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.

Número de anuncio 2024/1055

- 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.

3.- Funcións do Responsable do Sistema:

- Paralizar ou dar suspensión ó acceso á 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 ó 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 ós 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 axústanse ás autorizacións pertinentes.
- Monitorizar o estado de seguridade proporcionado polas ferramentas de xestión de eventos de seguridade e mecanismos de auditoría técnica.

7.2.- 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 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:
  a) 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.
  b) 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.
  c) Velar porque a Seguridade da Información se teña en conta en tódolos 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.

Número de anuncio 2024/1055

d) Realizar un seguimento dos principais riscos residuais asumidos pola Administración e recomendar posibles actuacións respecto deles.

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

f) Elaborar e revisar regularmente a Política de Seguridade da Información para a súa aprobación polo órgano competente.

g) Elaborar a normativa de Seguridade da Información para a súa aprobación en coordinación coa Dirección Xeral.

h) Verificar os procedementos de seguridade da información e demais documentación para a súa aprobación.

i) Elaborar programas de formación destinados a formar e sensibilizar ó persoal en materia de Seguridade da Información e en particular en materia de protección de datos de carácter persoal.

j) Elaborar e aprobar os requisitos de formación e cualificación de administradores, operadores e usuarios desde o punto de vista de Seguridade da Información.

k) 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.

7.3.- Procedementos de designación

A designación dos Responsables identificados nesta Política realízase pola Alcaldía-Presidencia do Concello da Baña mediante Decreto o mesmo día da aprobación desta política, e comunicada ás partes afectadas con anterioridade.

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.

Resolución de conflitos

Si se presentase un conflito entre os Responsables, será resolto polo Comité de Seguridade da Información.

8.- DATOS DE CARÁCTER PERSOAL

O Concello da Baña, no tratamento dos datos persoais, cumpre cos principios e obrigacións 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 ó 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-) 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, a intimidade e o resto dos dereitos fundamentais recoñecidos tanto na lexislación e tratados internacionais como na Constitución vixente.

En desenvolvemento dos principios da vixente normativa de protección de datos, entre outros, os de minimización, confidencialidade ou proactividade, este Concello define un marco de actuación na Política de Protección de Datos, que se debe aprobar por Decreto de Alcaldía.

9.- 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 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.

10.- TERCEIRAS PARTES

Cando se preste servizos a outros organismos, ou manexe información doutros organismos, faráselles partícipe desta Política de Seguridade da Información. O Concello da Baña, 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 da Baña, utilice servizos de terceiros ou ceda información a terceiros, faráselles partícipe desta Política de Seguridade e da Normativa de Seguridade existente que incumba ós devanditos servizos ou información. Dita terceira parte quedará suxeita ás obrigas establecidas na mencionada normativa, podendo desenvolver os seus propios procedementos operativos para satisface-la. Estableceranse procedementos específicos de comunicación e resolución de incidencias.

Número de anuncio 2024/1055

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 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 oferten solucións ás entidades públicas, ós 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.

A Baña, a 13 de febreiro de 2024.

Asdo. O alcalde,

José Antonio Pereira Gil.

2024/1055