POLÍTICA DE SEGURIDADE DA INFORMACIÓN E PROTECCIÓN DE DATOS
ANO 2024.

Concello da Coruña

Índice

1. Introdución

Neste apartado, contémplanse aspectos crave como a misión ou obxectivos da entidade, así como o alcance da Política.

1.1. Misión

A entidade integra o conxunto de EELL do Estado, encadrándose na Comunidade Autónoma de Galicia, e sendo a máxima competencia no ámbito municipal da Coruña .

Como calquera Concello, presta os servizos de administración que son da súa competencia en todo o territorio asignado. Neste sentido, cada vez atribúese máis importancia á prestación dos mesmos de forma electrónica, xurdindo a necesidade de cumprir cunhas normas de seguridade que ofreza confianza necesaria aos cidadáns no tratamento da súa información.

Por este motivo, xorde a presente Política e o resto das accións dirixidas a cumprir co Esquema Nacional de Seguridade (ENS) e a lexislación sobre protección de datos (RXPD e LOPDGDD).

1.2. Alcance

Esta Política aplícase a todos os sistemas TIC (Tecnoloxías da Información e Comunicacións) do Concello da Coruña e a todos os membros da organización, que dean servizo no ámbito electrónico da administración.

As directrices desta Política esténdense a todos os servizos prestados por parte da entidade aos cidadáns, sempre que estean baixo o ámbito do ENS, así como ás actividades de tratamento de datos persoais que se realicen.

Ademais dos servizos mencionados, inclúese no alcance desta Política todos os servizos internos da entidade, así como servizos prestados a outras entidades do Sector Público a través de medios electrónicos nalgunha das súas fases.

2. Xustificación da Política

2.1. Necesidade de Seguridade nos Sistemas

Para o cumprimento da súa Misión, a prestación dos servizos identificados e o cumprimento dos seus obxectivos, a entidade depende dos sistemas TIC.

Estes sistemas deben ser administrados con dilixencia, adoptando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados que poidan afectar á confidencialidade, integridade, dispoñibilidade, autenticidade e trazabilidade da información tratada ou dos 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, autenticidade, trazabilidade, 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.

É por iso que o Real Decreto que regula Esquema Nacional de Seguridade (ENS), no seu artigo 12.2, establece que *"Cada administración pública contará cunha política de*

seguridade formalmente aprobada polo órgano competente. Así mesmo, cada órgano ou entidade con personalidade xurídica propia comprendido no ámbito subxectivo do artigo 2 deberá contar cunha política de seguridade formalmente aprobada polo órgano competente".

A política de seguridade establecerase de acordo cos principios básicos sinalados no capítulo II e desenvolverase aplicando os seguintes requisitos mínimos:

- Organización e implantación do proceso de seguridade.
- Análise e xestión dos riscos.
- Xestión de persoal.
- Profesionalidade.
- Autorización e control dos accesos.
- Protección das instalacións.
- Adquisición de produtos de seguridade e contratación de servizos de seguridade.
- Mínimo privilexio.
- Integridade e actualización do sistema.
- Protección da información almacenada e en tránsito.
- Prevención ante outros sistemas de información interconectados.
- Rexistro da actividade e detección de código daniño.
- Incidentes de seguridade.
- Continuidade da actividade.
- Mellora continua do proceso de seguridade.

De forma adicional, e pola súa especial relación, esta necesidade esténdese á materia de protección de datos, por considerar á privacidade como unha parte inseparable da seguridade da información en xeral.

2.2. Requisitos de Seguridade nas Unidades Organizativas Municipais

En vista do alcance, todas as unidades organizativas municipais da entidade deben aplicar as medidas mínimas de seguridade esixidas polo ENS, 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.

As diferentes unidades organizativas municipais 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.

As unidades organizativas municipais deben estar preparados para previr, detectar, responder e recuperarse de incidentes, de acordo co Artigo 8 do Real Decreto que regula o Esquema Nacional de Seguridade (ENS).

3. Marco normativo

3.1. Responsabilidades derivadas da natureza legal

A entidade, en cumprimento das súas responsabilidades e en atención ás normas que regulan a actividade do Sector Público, deberá atender a diferentes regulacións, de entre as que destacamos, as seguintes:

No que se refire ao Procedemento Administrativo

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 203/2021, do 30 de marzo, polo que se aproba o Regulamento de actuación e funcionamento do sector público por medios electrónicos

Lei 7/1985, do 2 de abril, Reguladora das Bases do Réxime Local.

No que se refire á Protección de Datos

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.

Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e Garantía dos Dereitos Dixitais.

No que respecta ao Esquema Nacional de Seguridade e lexislación complementaria

O Real Decreto 311/2022, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade.

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 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno.

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.
Lei 9/2014, do 9 de maio, Xeneral 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.

Lei 6/2020, de 11 de novembro, reguladora de determinados aspectos dos servizos electrónicos de confianza.
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 9/2017, de 8 de novembro, de Contratos do Sector Público

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.

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

4. Organización da Seguridade

4.1. Definición de Roles

A Política de Seguridade, segundo require o artigo 13 e segundo detalla a sección 3.1 do Anexo II do ENS, debe identificar uns claros responsables para velar polo seu cumprimento e ser coñecida por todos os membros da entidade.

A responsabilidade da actividade dunha entidade do Sector Público sitúase, en última instancia, no seu Titular.

O Titular da entidade, rexedor/a municipal, é responsable de fixar os obxectivos estratéxicos, organizar adecuadamente os seus elementos constituíntes, as súas relacións internas e externas, e dirixir a súa actividade, incluíndo a aprobación da Política de Seguridade da Información e Protección de Datos do organismo, así como, no seu caso, a Política de Protección de Datos, facilitando os recursos adecuados para alcanzar os obxectivos propostos, velando polo seu cumprimento.

No caso de servizos externalizados, salvo por causa xustificada e documentada, a organización prestataria dos devanditos servizos deberá designar un POC (Punto ou Persoa de Contacto) para a seguridade da información tratada e o servizo prestado, que conte co apoio dos órganos de dirección, e que canalice e supervise, tanto o cumprimento dos requisitos de seguridade do servizo que presta ou solución que provea, como as comunicacións relativas á seguridade da información e a xestión dos incidentes para o ámbito do devandito servizo.

Devandito POC de seguridade será o propio Responsable de Seguridade da organización contratada, formará parte da súa área ou terá comunicación directa coa mesma.

Así pois, concretando os roles requiridos polo ENS, a figura da Dirección da entidade recaerá na Alcaldía e na Xunta de Goberno Local.

Da Dirección depende o compromiso da entidade coa seguridade e a súa adecuada implantación, xestión e mantemento. Tal como establece o Regulamento Orgánico Municipal, son órganos directivos da entidade:

- Coordinadores Xerais.
- Secretario Xeral do Pleno.
- Directores de Área ou asimilados.
- Oficial Maior.
- Director da Asesoría Xurídica.
- Interventor Xeral Municipal.
- Tesoureiro Xeral.
- Titular da área e Gabinete da Alcaldía.

Establécense os seguintes roles na organización relacionados coa Seguridade da Información.

4.1.1. Responsable da Información

Corresponde ao nivel de goberno da entidade, constituído pola Alta Dirección (Alcaldía ou Xunta de Goberno Local), que entende a misión da organización, determina os obxectivos que se propón alcanzar e responde de que se alcancen.

As súas funcións poderán ser asignadas a persoas individuais, ou ben ser asumidas polo Comité de Seguridade da Información.

A persoa ou órgano que o asuma deberá ser identificada para cada Información que trate o Concello, salvo que exista só un rol con carácter xeral.

O **Responsable da Información** na entidade será o Comité de Seguridade da Información.

Funcións asociadas

As súas funcións serán as seguintes:

- Ten a responsabilidade última do uso que se faga dunha certa información e, por tanto, da súa protección.
- Responsable da Información é o responsable último de calquera erro ou neglixencia que leve a un incidente de confidencialidade de integridade.
- Establece os requisitos da información en materia de seguridade. No marco do ENS, equivale á potestade de determinar os niveis de seguridade da información.
- Determinará os niveis de seguridade en cada dimensión dentro do marco establecido no Anexo I do ENS.
- Aínda que a aprobación formal dos niveis corresponda ao Responsable da Información, poderá solicitar unha proposta ao Responsable da Seguridade e convén que escoite a opinión do Responsable do Sistema.

Compatibilidade con outros roles

Este rol poderá coincidir co do Responsable do Servizo.

Este rol non poderá coincidir co de Responsable de Seguridade da Información.

Este rol non poderá coincidir co de Responsable de Sistema nin co de Administrador da Seguridade do Sistema.

4.1.2. Responsable do Servizo

Cando sexa distinto do Responsable da Información, pode corresponder ao nivel de goberno da entidade, do mesmo xeito que o Responsable da Información, ou ben ao dunha Dirección Executiva ou Xerencia, que entende que fai cada departamento, e como as unidades organizativas municipais coordínanse entre si para alcanzar os obxectivos marcados pola Dirección.

As súas funcións poderán ser asignadas a persoas individuais, ou ben ser asumidas polo Comité de Seguridade da Información.

A persoa ou órgano que o asuma deberá ser identificada para cada Servizo que preste a organización, salvo que exista só un rol con carácter xeral.

O **Responsable do Servizo** da entidade será o Comité de Seguridade da Información.

Funcións asociadas

As súas funcións serán as seguintes:

- En canto ao RXPD, por delegación do Responsable do Tratamento encoméndase ao Responsable do Servizo o desenvolvemento das tarefas

relacionadas coa xestión dos tratamentos de datos persoais que se realizan na súa área en concreto.

- Establece os requisitos dos servizos en materia de seguridade. No marco do ENS, equivale á potestade de determinar os niveis de seguridade da información.
- Ten a responsabilidade última do uso que se faga de determinados servizos e, por tanto, da súa protección.
- O Responsable do Servizo é o responsable último de calquera erro ou neglixencia que leve a un incidente de dispoñibilidade dos servizos.
- Determinará os niveis de seguridade en cada dimensión do servizo dentro do marco establecido no Anexo I do ENS.
- Aínda que a aprobación formal dos niveis corresponda ao Responsable do Servizo, poderá solicitar unha proposta ao Responsable da Seguridade e convén que escoite a opinión do Responsable do Sistema.
- A prestación dun servizo sempre debe atender aos requisitos de seguridade da información que manexa, de forma que poden herdarse os requisitos de seguridade da mesma, engadindo requisitos de dispoñibilidade, así como outros como accesibilidade, interoperabilidade, etc.

Compatibilidade con outros roles

Poderá coincidir na mesma persoa ou órgano o rol de Responsable da Información e do Responsable do Servizo.

Este rol non poderá coincidir co de Responsable de Seguridade.

Este rol non poderá coincidir co de Responsable de Sistema nin co de Administrador da Seguridade do Sistema, nin sequera cando se trate de organizacións de reducida dimensión que funcionen de forma autónoma.

4.1.3. Responsable de Seguridade da Información

Nomearase formalmente como tal a unha única persoa na organización. O rol non poderá ser desenvolto por un órgano colexiado, nin poderá haber máis dunha persoa asumindo o rol na organización, aínda que poida delegar parte das súas funcións noutras persoas.

Desígnase como **Responsable da Seguridade da Información** o titular da Xefatura do Servizo de Innovación Tecnolóxica ou no seu defecto o titular da Xefatura do Departamento de Innovación Tecnolóxica.

Desígnase como Responsable de Seguridade Delegado ao funcionario de carreira da Escala de Administración Especial, subescala técnica, clase técnicos superiores, subgrupo A1 co nº de posto na RPT 2097.

Funcións asociadas

As súas funcións serán as seguintes:

- Reportará directamente ao Comité de Seguridade da Información.
- Actuará como Secretario do Comité de Seguridade da Información.
- Convocará ao Comité de Seguridade da Información, recompilando a información pertinente.
- Manterá a seguridade da información manexada e dos servizos prestados polos sistemas de información no seu ámbito de responsabilidade, de acordo ao establecido na Política de Seguridade da Organización.

- Promoverá a formación e concienciación en materia de seguridade da información dentro do seu ámbito de responsabilidade.
- Recompilará os requisitos de seguridade dos Responsables de Información e Servizo e determinará a categoría do Sistema.
- Realizará a Análise de Riscos.
- Elaborará unha Declaración de Aplicabilidade a partir das medidas de seguridade requiridas conforme ao Anexo II do ENS e do resultado da Análise de Riscos.
- Facilitará aos Responsable de Información e aos Responsables de Servizo información sobre o nivel de risco residual esperado tras implementar as opcións de tratamento seleccionadas na análise de riscos e as medidas de seguridade requiridas polo ENS.
- Participará na elaboración, no marco do Comité de Seguridade da Información, a Política de Seguridade da Información e Protección de Datos, para a súa aprobación por Dirección.
- Participará na elaboración e aprobación, no marco do Comité de Seguridade da Información, da normativa de Seguridade da Información.
- Elaborará e aprobará os Procedementos Operativos de Seguridade da Información.
- Facilitará periodicamente ao Comité de Seguridade da Información un resumo de actuacións en materia de seguridade, de incidentes relativos a seguridade da información e do estado da seguridade do sistema (en particular do nivel de risco residual ao que está exposto o sistema).
- Elaborará, xunto aos Responsables de Sistemas, Plans de Mellora da Seguridade, para a súa aprobación polo Comité de Seguridade da Información.
- Validará os Plans de Continuidade de Sistemas que elabore o Responsable de Sistemas, que deberán ser aprobados polo Comité de Seguridade da Información e probados periodicamente polo Responsable de Sistemas.
- Aprobará as directrices propostas polos Responsables de Sistemas para considerar a Seguridade da Información durante todo o ciclo de vida dos activos e procesos: especificación, arquitectura, desenvolvemento, operación e cambios.
- Elaborar e propoñer para aprobación pola organización as políticas de seguridade, que incluirán as medidas técnicas e organizativas, adecuadas e proporcionadas, para xestionar os riscos que se expoñan para a seguridade das redes e sistemas de información utilizados e para previr e reducir ao mínimo os efectos dos ciberincidentes que afecten á organización e os servizos.
- Desenvolver as políticas de seguridade, normativas e procedementos derivados da organización, supervisar a súa efectividade e levar a cabo auditorías periódicas de seguridade.
- Actuar como capacitador de boas prácticas en seguridade das redes e sistemas de información, tanto en aspectos físicos como lóxicos.
- Constituírse como punto de contacto coa autoridade competente en materia de seguridade das redes e sistemas de información e responsable ante aquela de o cumprimento das obrigacións que se derivan do Real Decreto-lei 12/2018, de seguridade das redes e sistemas de información.
- Constituír o punto de contacto especializado para a coordinación co CSIRT de referencia.
- Notificar á autoridade competente, a través do CSIRT de referencia e sen dilación indebida, os incidentes que teñan efectos perturbadores na prestación dos servizos.
- Recibir, interpretar e aplicar as instrucións e guías emanadas da Autoridade Competente, tanto para a operativa habitual como para a corrección das deficiencias observadas.

- Recompilar, preparar e fornecer información ou documentación á autoridade competente ou o CSIRT de referencia, á súa solicitude ou por propia iniciativa.

En caso de ocorrencia de incidentes de seguridade da información:

- Analizará e propoñerá salvagardas que preveñan incidentes similares nun futuro.

Compatibilidade con outros Roles

Este rol non poderá coincidir co de Responsable do Sistema e o de Administrador de Seguridade do Sistema, aínda que se trate de organizacións de reducidas dimensións que teñan unha estrutura autónoma de funcionamento.

Delegación de Funcións

Para determinados Sistemas de Información que, pola súa complexidade, distribución, separación física dos seus elementos ou número de usuarios necesítese de persoal adicional para levar a cabo as funcións de Responsable da Seguridade da Información, poderanse designar os Responsables de Seguridade Delegados que se consideren necesarios.

A designación corresponde ao Responsable da Seguridade. Por medio da designación de delegados, deléganse funcións. A responsabilidade final seguirá recaendo sobre o Responsable da Seguridade.

Os Responsables de Seguridade Delegados faranse cargo, no seu ámbito, de todas aquelas accións que delegue o Responsable da Seguridade, podendo ser, por exemplo, a seguridade de sistemas de información concretos ou de sistemas de información horizontais.

Cada Responsable de Seguridade Delegado terá unha dependencia funcional directa do Responsable de Seguridade, que é a quen reporta.

4.1.4. Responsable do Sistema

Nomearase formalmente como tal a unha única persoa para o Sistema de Información Municipal. O rol non poderá ser desenvolto por un órgano colexiado, aínda que poida delegar parte das súas funcións noutras persoas.

Desígnase como **Responsable do Sistema** á Xefatura de Servizo de Informática ou no seu defecto á Xefatura do Departamento de Informática.

Desígnase como Responsable do Sistema Delegado ao Xefe de Sección de Innovación y Desarrollo Tecnológico.

Funcións asociadas

As súas funcións serán as seguintes:

- Coordinar o desenvolvemento, operación e mantemento do Sistema de Información durante todo o seu ciclo de vida, das súas especificacións, instalación e verificación do seu correcto funcionamento.
- Definir a topoloxía e sistema de 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.
- O Responsable do Sistema pode acordar a suspensión do manexo dunha certa información ou a prestación dun certo servizo se é informado de deficiencias graves de seguridade que puidesen afectar á satisfacción dos requisitos establecidos. Esta decisión debe ser acordada cos Responsables da Información afectada, do Servizo afectado e co Responsable da Seguridade antes de ser executada.
- Verificar a aplicación dos procedementos operativos de seguridade elaborados e aprobados polo Responsable de Seguridade.
- Monitorar o estado da seguridade do Sistema de Información e reportalo periodicamente ou ante incidentes de seguridade relevantes ao Responsable de Seguridade da Información, de acordo aos informes remitidos polos administradores de seguridade.
- Elaborar os Plans de Continuidade do Sistema para que sexan validados polo Responsable de Seguridade da Información, e coordinados e aprobados polo Comité de Seguridade da Información.
- Coordinar a realización de exercicios e probas periódicas dos Plans de Continuidade do Sistema para mantelos actualizados e verificar que son efectivos.
- Elaborará as directrices para considerar a Seguridade da Información durante todo o ciclo de vida dos activos e procesos (especificación, arquitectura, desenvolvemento, operación e cambios) e facilitaraas ao Responsable de Seguridade da Información para a súa aprobación.

En caso de ocorrencia de incidentes de seguridade da información:

- Planificará a implantación de salvagárdalas no sistema.
- Executará o plan de seguridade aprobado.

Compatibilidade con outros roles

Este rol non poderá coincidir co de Responsable da Información, co de Responsable do Servizo nin co de Responsable de Seguridade da Información.

Este rol poderá coincidir co de Administrador de Seguridade do Sistema en organizacións dunha dimensión reducida ou intermedia que teñan unha estrutura autónoma de funcionamento.

En grandes organizacións non debería coincidir co de Administrador da Seguridade do Sistema, independentemente do tamaño do Sistema.

Delegación de Funcións

En determinados Sistemas de Información que, pola súa complexidade, distribución, separación física dos seus elementos ou número de usuarios necesítese de persoal adicional para levar a cabo as súas funcións, poderanse designar Responsables do Sistema Delegados.

Os Responsables do Sistema Delegados serán responsables, no seu ámbito, daquelas accións que delegue o Responsable do Sistema relacionadas coa implantación, xestión e mantemento das medidas de seguridade aplicables ao sistema de información.

O Responsable do Sistema Delegado será designado a solicitude do Responsable do Sistema, do que dependerá funcionalmente.

4.1.5. Administrador da Seguridade do Sistema

Corresponde ao nivel dun empregado cualificado en seguridade informática de sistemas.

Poderá nomearse formalmente como tal a varias persoas para cada Sistema. O rol non poderá ser desenvolto por un órgano colexiado, nin poderá delegar parte das súas funcións noutras persoas. No seu caso, nomearíanse novos Administradores da Seguridade do Sistema.

Será proposto polo Responsable do Sistema, a quen reportará en todo o relacionado con seguridade da información.

Funcións asociadas

As súas funcións serán as seguintes:

- A implementación, xestión e mantemento das medidas de seguridade aplicables ao Sistema de Información.
- Asegurar que os controis de seguridade establecidos son cumpridos estritamente.
- Asegurar que a trazabilidade, pistas de auditoría e outros rexistros de seguridade requiridos atópense habilitados e rexistren coa frecuencia desexada, de acordo coa política de seguridade establecida pola Organización.
- Aplicar aos Sistemas, usuarios e outros activos e recursos relacionados co mesmo, tanto internos como externos, os Procedementos Operativos de Seguridade e os mecanismos e servizos de seguridade requiridos.
- Asegurar que son aplicados os procedementos aprobados para manexar o Sistema de información e os mecanismos e servizos de seguridade requiridos.
- A xestión, configuración e actualización, no seu caso, do hardware e software nos que se basean os mecanismos e servizos de seguridade do Sistema de Información.
- Supervisar as instalacións de hardware e software, as súas modificacións e melloras para asegurar que a seguridade non está comprometida.
- Aprobar os cambios na configuración vixente do Sistema de Información, garantindo que sigan operativos os mecanismos e servizos de seguridade habilitados.
- Informar os Responsables da Seguridade e do Sistema de calquera anomalía, compromiso ou vulnerabilidade relacionada coa seguridade.
- Monitorar o estado da seguridade do sistema.

En caso de ocorrencia de incidentes de seguridade da información:

- Levar a cabo o rexistro, contabilidade e xestión dos incidentes de seguridade nos Sistemas baixo a súa responsabilidade.
- Executar o plan de seguridade aprobado.
- Illar o incidente para evitar a propagación a elementos alleos á situación de risco.
- Tomar decisións a curto prazo se a información viuse comprometida de tal forma que puidese ter consecuencias graves (estas actuacións deberían estar procedimentadas para reducir a marxe de discrecionalidade do Administrador de Seguridade do Sistema ao mínimo número de casos).
- Asegurar a integridade dos elementos críticos do Sistema se se viu afectada a dispoñibilidade dos mesmos (estas actuacións deberían

estar procedimentadas para reducir a marxe de discrecionalidade do Administrador de Seguridade do Sistema ao mínimo número de casos).
- Manter e recuperar a información almacenada polo Sistema e os seus servizos asociados.
- Investigar o incidente: Determinar o modo, os medios, os motivos e a orixe do incidente.

Compatibilidade con outros roles

Este rol non poderá coincidir co de Responsable de a Información, co de Responsable do Servizo nin co de Responsable de Seguridade da Información.

Este rol poderá coincidir co de Responsable do Sistema en organizacións dunha dimensión reducida ou intermedia que teñan unha estrutura autónoma de funcionamento.

En grandes organizacións non debería coincidir co de Responsable do Sistema, independentemente do tamaño do Sistema.

Delegación de Funcións

En determinados Sistemas de Información que, pola súa complexidade, distribución, separación física dos seus elementos ou número de usuarios necesítese de persoal adicional para levar a cabo as súas funcións, poderanse designar Administradores de Seguridade do Sistema Delegados.

Os Administradores de Seguridade do Sistema Delegados serán responsables, no seu ámbito, daquelas accións que delegue o Administrador de Seguridade do Sistema relacionadas coa implantación, xestión e mantemento das medidas de seguridade aplicables ao sistema de información.

O Administrador de Seguridade do Sistema Delegado será designado a solicitude do Administrador de Seguridade do Sistema, do que dependerá funcionalmente.

A súa identidade aparecerá reflectida na documentación de seguridade do sistema de información.

4.1.6. O Centro de Seguridade da Información e Privacidade

A Concellería de Economía e Planificación Urbana, como concellería titular da área con competencias sobre a materia, establece o Centro de Seguridade da Información e Privacidade como instrumento de apoio no goberno e xestión da seguridade da información, e aos roles e órganos definidos na presente política. Estará dispoñible en csi@coruna.gal

4.1.7. Definición de Comités: O Comité de Seguridade da Información

É o órgano que coordina a Seguridade da Información a nivel de organización, e actuará como Responsable do Servizo e Responsable da Información.
Estará constituído por:

- Presidente: o concelleiro titular da área de Economía e Planificación Urbana (actualmente Concelleiro delegado responsable do Área de Economía e Planificación Urbana), ou director de área en quen delegue.
- Secretario/a: Responsable de Seguridade da Información ENS.
- Vogais:

- Secretario Xeral.
- Oficial Maior.
- Responsable do sistema.
- O titular da dirección da área responsable do Servizo de Informática (actualmente o Director de Economía, Facenda e Réximen Interior).
- O Titular da dirección do Área responsable do Servizo de Innovación Tecnolóxica (actualmente Director da Área de Infraestruturas, Mobilidade e Innovación Tecnolóxica.
- Os responsables das unidades organizativas municipais serán convocados pola presidencia en función dos asuntos para tratar.
- Vogal sen dereito a voto: o Delegado de Protección de Datos da entidade.

Sempre que sexa posible, deberá asumir as seguintes funcións:

- Atender as inquietudes da Alta Dirección (Alcaldía ou Xunta de Goberno Local) e das diferentes unidades organizativas.
- Informar regularmente o estado da seguridade da información á Alta Dirección, o que poderá facerse simultaneamente se esta forma parte do mesmo.
- Promover a mellora continua do Sistema de Xestión da Seguridade da Información.
- Elaborar a estratexia de evolución da Organización no que respecta a seguridade da información.
- Coordinar os esforzos das diferentes áreas en materia de seguridade da información, para asegurar que os esforzos son consistentes, aliñados coa estratexia decidida na materia, e evitar duplicidades.
- Elaborar (e revisar regularmente) a Política de Seguridade da Información e Protección de Datos para que sexa aprobada pola Dirección (Alcaldía ou Xunta de Goberno Local).
- Aprobar a normativa de seguridade da información.
- Elaborar e aprobar os requisitos de formación e cualificación de administradores, operadores e usuarios desde o punto de vista de seguridade da información.
- Monitorear os principais riscos residuais asumidos pola organización e recomendar posibles actuacións respecto de eles.
- Monitorear o desempeño dos procesos de xestión de incidentes de seguridade e recomendar posibles actuacións respecto de eles. En particular, velar pola coordinación das diferentes áreas de seguridade na xestión de incidentes de seguridade da información.
- Promover a realización das auditorías periódicas que permitan verificar o cumprimento das obrigacións da organización en materia de seguridade.
- Aprobar plans de mellora da seguridade da información da Organización. En particular, velará pola coordinación de diferentes plans que poidan realizarse en diferentes áreas.
- Velar porque a seguridade da información téñase en conta en todos os proxectos TIC 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.
- Resolver os conflitos de responsabilidade que poidan aparecer entre os diferentes responsables e/ou entre diferentes áreas da organización, elevando aqueles casos nos que non teña suficiente autoridade para decidir.

En caso de ocorrencia de incidentes de seguridade da información:

- Aprobará o Plan de Mellora da Seguridade, coa súa dotación orzamentaria correspondente.

O Comité de Seguridade da Información non é un comité técnico, pero solicitará regularmente do persoal técnico propio ou externo, a información pertinente para tomar decisións. O Comité de Seguridade da Información asesorarase dos temas sobre os que teña que decidir ou emitir unha opinión. Este asesoramento determinarase en cada caso, podendo materializarse de diferentes formas e maneiras:

- Grupos de traballo especializados internos, externos ou mixtos.
- Asesoría externa.
- Asistencia a cursos ou outro tipo de contornas formativas ou de intercambio de experiencias.

O Responsable da Seguridade da Información é o secretario do Comité de Seguridade da Información e como tal:

- Convoca as reunións do Comité de Seguridade da Información.
- Prepara os temas para tratar nas reunións do Comité, achegando información puntual para a toma de decisións.
- Elabora a acta das reunións.
- É responsable da execución directa ou delegada das decisións do Comité.

Xerarquía no proceso de decisións e mecanismos de coordinación

Os diferentes roles de seguridade da información limítanse a unha xerarquía simple: o Comité de Seguridade da Información dá instrucións ao Responsable da Seguridade da Información, que se encarga de supervisar que administradores e operadores implementan as medidas de seguridade segundo o establecido na política de seguridade aprobada para a organización.

O Administrador de Seguridade reporta ao Responsable do Sistema:

- Incidentes relativos á seguridade do sistema
- Accións de configuración, actualización ou corrección

O Responsable do Sistema informa ao Responsable da Información das incidencias funcionais relativas á información que lle compete.

O Responsable do Sistema informa ao Responsable do Servizo das incidencias funcionais relativas ao servizo que lle compete.

O Responsable do Sistema reporta ao Responsable da Seguridade:

- Actuacións en materia de seguridade, en particular no relativo a decisións de arquitectura do sistema
- Resumo consolidado dos incidentes de seguridade
- Medidas da eficacia das medidas de protección que se deben implantar

O Responsable da Seguridade informa ao Responsable da Información das decisións e incidentes en materia de seguridade que afecten á información que lle compete, en particular da estimación de risco residual e das desviacións significativas de risco respecto de as marxes aprobadas.

O Responsable da Seguridade informa ao Responsable do Servizo das decisións e incidentes en materia de seguridade que afecten o servizo que lle compete, en particular da estimación de risco residual e das desviacións significativas de risco respecto de as marxes aprobadas.

Sempre que exista e estea vixente un Comité de Seguridade da Información, o Responsable da Seguridade reporta ao devandito comité como secretario:

- Resumo consolidado de actuacións en materia de seguridade
- Resumo consolidado de incidentes relativos á seguridade da información
- Estado da seguridade do sistema, en particular do risco residual ao que o sistema está exposto

Procedementos de designación de persoas

A Dirección da organización (Alcaldía ou Xunta de Goberno Local) nomeará formalmente, tanto na súa designación inicial como nas súas renovacións:

- Ao Responsable da Información; pode ser un cargo unipersoal ou un órgano colexiado.
- Ao Responsable do Servizo; pode ser o mesmo que o Responsable da Información; pode ser un cargo unipersoal ou un órgano colexiado.
- Ao Responsable da Seguridade, que debe reportar directamente á Dirección ou, cando existan, aos comités de seguridade da información e seguridade corporativa.
- Ao Responsable do Sistema, que debe reportar directamente á Dirección ou, cando existan, aos comités de seguridade da información e seguridade corporativa.

A Dirección da organización designa á persoa Responsable do Sistema:

- A proposta do Responsable da Información tratada, cando o Sistema de información trate unha única información.
- A proposta do Responsable do Servizo prestado, cando o Sistema de información preste un único servizo.
- Directamente cando o Sistema de Información trata diferentes informacións ou presta diferentes servizos, oídos os responsables das informacións e os servizos afectados.

A Dirección da organización designa ao Administrador de Seguridade do Sistema a proposta do Responsable do Sistema.

Procedemento para resolución de conflitos

En caso de conflito, prevalecerán as decisións do nivel superior xerárquico, que atenden á orde exposta no apartado anterior relativo á xerarquía.

Para a coordinación e implantación dá Política de Seguridade, o Comité de Seguridade da Información será o órgano competente onde deberán resolverse todas as cuestións de coordinación e resolución de conflitos que xurdan en materia de Seguridade da Información.

Relación coa Protección de Datos Persoais

Para a prestación dos servizos previstos deben ser tratados datos de carácter persoal. O Rexistro de Tratamento detallará os ficheiros afectados e os responsables correspondentes, así como as medidas adoptadas neste marco.

Todos os sistemas de información axustaranse aos niveis de seguridade requiridos pola normativa para a natureza e finalidade dos datos de carácter persoal recollidos no mencionado Rexistro de Actividades.

Nesta materia xorden varias responsabilidades a nivel legal ou organizativo. Por unha banda, o **responsable do tratamento ou responsable**, que é a persoa física ou xurídica, autoridade pública, servizo ou outro organismo que, só ou xunto con outros, determine os fins e medios do tratamento.

Por outro, o **encargado** é a persoa física ou xurídica, autoridade pública, servizo ou outro organismo que trate datos por conta do responsable do tratamento. A relación entre responsable e encargado deberá estar regulada nun contrato ou instrumento xurídico.

En definitiva, unha vez considerada a Seguridade da Información como un concepto amplo, que podería abarcar ao de Privacidade, faise necesario que o cumprimento da entidade nesta materia relaciónese co daquela, sendo interoperables as medidas de seguridade que se definan en ambos os marcos normativos.

5. Datos de Carácter Persoal

Para a prestación dos servizos previstos deben ser tratados datos de carácter persoal. O Rexistro de Actividades do Tratamento detalla os tratamentos afectados e os responsables correspondentes, así como as medidas adoptadas derivadas das avaliacións de impacto realizadas sobre os tratamentos.

Todos os sistemas de información axustaranse aos niveis de seguridade requiridos pola normativa para a natureza e finalidade dos datos de carácter persoal recollidos no mencionado Rexistro de Actividades do Tratamento.

En todo caso, deberase atender aos principios regulados no artigo 5 do RXPD, que se considerar auténticas obrigacións para esta entidade.

5.1. Figuras vinculadas á protección de datos de carácter persoal

5.1.1. Responsable do Tratamento

O Responsable do tratamento é a persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo, que decide sobre a finalidade, contido e uso do tratamento.

A eses efectos atribuíuse a condición de Responsable de Tratamento á persoa xurídico-pública, é dicir, ao propio Concello da Coruña. De maneira que, entendeuse que o Concello é Responsable do Tratamento dos datos de carácter persoal que obran nos seus sistemas de información, e que derivan da prestación dos servizos públicos atribuídos a nivel de competencias.

As funcións do Responsable do Tratamento son, principalmente:

- Adoptar as medidas de índole técnica e organizativas necesarias que garantan a seguridade dos datos de carácter persoal e eviten a súa alteración, perda, tratamento ou acceso non autorizado.
- Deberá informar os titulares dos datos os dereitos que lles asisten e nos termos nos que poden exercelos.
- Deberá excluír do tratamento os datos relativos ao afectado que se opoña ao tratamento dos mesmos.
- Deberá cesar na utilización ou cesión ilícita dos datos cando así o requira o interesado.

- Obrigación de facer efectivo o dereito de rectificación ou supresión do interesado no prazo máximo de 1 mes.
- Notificar as rectificacións ou cancelacións efectuadas nos datos persoais a quen se haxa comunicado devanditos datos, no caso de que se manteña o tratamento por este último, que deberá tamén proceder á cancelación.

5.1.2. Delegado de Protección de datos

O Delegado de Protección de Datos (DPD) pode ser interno ou externo á organización, podendo revestir así mesmo a forma dun órgano colexiado (Comité Delegado de Protección de Datos), velando sempre por evitar conflito de intereses en calquera dos seus membros. Ademais diso, poderá designarse un único DPD para varias autoridades ou organismos públicos, tendo en consideración a súa estrutura e tamaño.

O **Delegado de Protección de Datos** na entidade será unha figura que poderá recaer na persoa ou servizo da entidade que mellor se adapte en cada momento ás características propias do rol, sendo designado formalmente e estando comunicado á Autoridade de Control competente. Estará dispoñible para a cidadanía na dirección delegadodeprotecciondedatos@coruna.gal

As funcións asociadas son:

- Informar e asesorar ao responsable ou ao encargado do tratamento e aos empregados que se ocupen do tratamento das obrigacións que lles incumben en virtude do presente Regulamento e doutras disposicións de protección de datos da Unión ou dos Estados membros;
- Supervisar o cumprimento do disposto no presente Regulamento, doutras disposicións de protección de datos da Unión ou dos Estados membros e das políticas do responsable ou do encargado do tratamento en materia de protección de datos persoais, incluída a asignación de responsabilidades, a concienciación e formación do persoal que participa nas operacións de tratamento, e as auditorías correspondentes;
- Ofrecer o asesoramento que se lle solicite acerca da avaliación de impacto relativa á protección de datos e supervisar a súa aplicación de conformidade co artigo 35;
- Cooperar coa autoridade de control;
- Actuar como punto de contacto da autoridade de control para cuestións relativas ao tratamento, incluída a consulta previa a que se refire o artigo 36, e realizar consultas, no seu caso, sobre calquera outro asunto.

O delegado de protección de datos desempeñará as súas funcións prestando a debida atención aos riscos asociados ás operacións de tratamento, tendo en conta a natureza, o alcance, o contexto e fins do tratamento. Para iso **deberá ser capaz** de:

- Solicitar información para determinar as actividades de tratamento.
- Analizar e comprobar a conformidade das actividades de tratamento.
- Informar, asesorar e emitir recomendacións ao responsable ou o encargado do tratamento.
- Solicitar información para supervisar o rexistro das operacións de tratamento.
- Asesorar na aplicación do principio da protección de datos por deseño e por defecto.
- Asesorar sobre:
  - Se se debe levar a cabo ou non unha avaliación de impacto da protección de datos

  - Que metodoloxía debe seguirse ao efectuar unha avaliación de impacto da protección de datos.
  - Se se debe levar a cabo a avaliación de impacto da protección de datos con recursos propios ou con contratación externa.
  - Que salvagardas (incluídas medidas técnicas e organizativas) aplicar para mitigar calquera risco para os dereitos de intereses dos afectados.
  - Se se levou a cabo correctamente ou non a avaliación de impacto da protección de datos.
  - Se as súas conclusións (se seguir adiante ou non co tratamento e que salvagardas aplicar) son conformes ao Regulamento.
- Priorizar as súas actividades e centrar os seus esforzos naquelas cuestións que presenten maiores riscos relacionados coa protección de datos.
- Asesorar ao responsable do tratamento sobre:

  - Que metodoloxía empregar ao levar a cabo unha avaliación de impacto da protección de datos.
  - Que áreas deben someterse a auditoría de protección de datos interna ou externa.
  - Que actividades de formación internas proporcionar ao persoal ou aos directores responsables das actividades de tratamento de datos e a que operacións de tratamento dedicar máis tempo e recursos.

O DPD deberá reunir coñecementos especializados do Dereito e a práctica en materia de protección de datos. Identificáronse, en consecuencia, aqueles coñecementos, **habilidades ou destrezas** necesarias que ten que saber ou posuír o Delegado de Protección de Datos para levar a cabo una das funcións propias do seu posto.

Estas funcións xenéricas do DPD pódense concretar en tarefas de asesoramento e supervisión, entre outras, nas seguintes áreas:

- Cumprimento de principios relativos ao tratamento, como os de limitación de finalidade, minimización ou exactitude dos datos.
- Identificación das bases xurídicas dos tratamentos.
- Valoración de compatibilidade de finalidades distintas das que orixinaron a recollida inicial dos datos.
- Determinación da existencia de normativa sectorial que poida determinar condicións de tratamentos específicos distintas das establecidas pola normativa xeral de protección de datos.
- Deseño e implantación de medidas de información aos afectados polos tratamentos de datos.
- Establecemento de mecanismos de recepción e xestión das solicitudes de exercicio de dereitos por parte dos interesados.
- Valoración das solicitudes de exercicio de dereitos por parte dos interesados.
- Contratación de encargados de tratamento, incluído o contido dos contratos ou actos xurídicos que regulen a relación responsable-encargado.
- Identificación dos instrumentos de transferencia internacional de datos adecuados ás necesidades e características da organización e das razóns que xustifiquen a transferencia.
- Deseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecemento e xestión dos rexistros de actividades de tratamento.

- Análise de riscos dos tratamentos realizados.
- Implantación das medidas de protección de datos desde o deseño e protección de datos por defecto adecuadas aos riscos e natureza dos tratamentos.
- Implantación das medidas de seguridade adecuadas aos riscos e natureza dos tratamentos.
- Establecemento de procedementos de xestión de violacións de seguridade dos datos, incluída a avaliación do risco para os dereitos e liberdades dos afectados e os procedementos de notificación ás autoridades de supervisión e aos afectados.
- Determinación da necesidade de realización de avaliacións de impacto sobre a protección de datos.
- Realización de avaliacións de impacto sobre a protección de datos
- Relacións coas autoridades de supervisión.
- Implantación de programas de formación e sensibilización do persoal en materia de protección de datos.

5.1.3. Funcións e obrigacións de Usuarios con acceso a datos

Todos os empregados da entidade están suxeitos a funcións e obrigacións que se definan neste sentido.

Todo o persoal da entidade que dispoña de acceso aos datos de carácter persoal debe cumprir coas seguintes obrigacións xerais:

- Non se permite a difusión de datos de carácter persoal nin confidencial pertencente á entidade, estando obrigado a gardar secreto da información mesmo terminada a relación laboral.
- O usuario responsabilizarase de notificar toda incidencia segundo o procedemento de xestión de incidencias. Non notificar unha incidencia será considerada unha omisión do deber do traballador.
- O usuario responsabilizarase de todos os accesos que se realicen baixo o seu identificador e contrasinal, por tanto, non deberá revelar o contrasinal.
- Non se permite a copia de datos de carácter persoal, en soportes, sen a autorización expresa do delegado de protección de datos.

De calquera forma, conforme referido, cada usuario dos sistemas de información da entidade deberá respectar as normativas que estean vixentes e aprobadas en cada momento.

5.1.4. Funcións e obrigacións do Encargado do Tratamento

O **apartado 8 do artigo 4 do RXPD** define ao Encargado de Tratamento como <<*a persoa física ou xurídica, autoridade pública, servizo ou outro organismo que trate datos persoais por conta do responsable do tratamento*>>.

O Encargado do Tratamento deberá aplicar as medidas de índole técnica e organizativas necesarias que garantan a seguridade dos datos de carácter persoal e eviten a súa alteración, perda, tratamento ou acceso non autorizado.

Igualmente deberá implementar as medidas de seguridade a que se refire o parágrafo anterior e que aparecerán estipuladas no contrato co Responsable do Tratamento.

En concreto, as súas funcións son as de:

- Tratar os datos do tratamento.
- Realizar o control de tratamento, calidade e seguridade dos datos.

- Controlar a forma e requisitos para proceder ás adicións e cancelacións.
- Controlar os soportes de seguridade.
- Control e acceso de contrasinais.
- Mantemento do rexistro de incidencias.
- Crear unha lista para as situacións na que un afectado non desexe que os seus datos persoais almacénense no tratamento.
- Dar traslado ao responsable do tratamento daquelas solicitudes de exercicio de dereito que se reciban por parte dos interesados.

En consecuencia, o Concello da Coruña deberá levar a cabo un documento actualizado onde se identificarán os Encargados de Tratamento que están a prestar servizos na entidade, así como a indicación da formalización do pertinente contrato con estes prestadores de servizos con acceso a datos.

6. Xestión de Riscos

6.1. Xustificación

Todos os sistemas suxeitos a esta Política deberán realizar unha análise de riscos, avaliando as ameazas e os riscos aos que están expostos.

A análise de riscos será a base para determinar as medidas de seguridade que se deben adoptar, ademais dos mínimos establecidos polo ENS, segundo o previsto no seu Artigo 7, e polo RXPD, no seu artigo 32.

6.2. Criterios de avaliación de riscos

Para a harmonización das análises de riscos, o Comité de Seguridade da Información establecerá unha valoración de referencia para os diferentes tipos de información manexados e os diferentes servizos prestados.

Os criterios de avaliación de riscos detallados especificaranse na metodoloxía de avaliación de riscos que elaborará a organización, baseándose en estándares e boas prácticas recoñecidas.

Deberán tratarse, como mínimo, todos os riscos que poidan impedir a prestación dos servizos ou o cumprimento da misión da organización de forma grave.

6.3. Directrices de tratamento

O Comité de Seguridade da Información dinamizará a dispoñibilidade de recursos para atender ás necesidades de seguridade dos diferentes sistemas, promovendo investimentos de carácter horizontal.

6.4. Proceso de aceptación do risco residual

Os riscos residuais serán determinados polo Responsable de Seguridade da Información, incluíndo os riscos relacionados coa privacidade.

Os niveis de risco residuais esperados sobre cada Información tras a implementación das opcións de tratamento previstas (incluída a implantación das medidas de seguridade previstas no Anexo II do ENS) deberán ser aceptados previamente polo seu Responsable desa Información.

Os niveis de risco residuais esperados sobre cada Servizo tras a implementación das opcións de tratamento previstas (incluída a implantación das medidas de seguridade previstas no Anexo II do ENS) deberán ser aceptados previamente polo seu Responsable dese Servizo.

Os niveis de risco residuais serán presentados polo Responsable de Seguridade da Información ao Comité de Seguridade da Información , para que este proceda, no seu caso, a avaliar, aprobar ou rectificar as opcións de tratamento propostas.

6.5. Necesidade de realizar ou actualizar as avaliacións de riscos

A análise dos riscos e o seu tratamento deben ser unha actividade repetida regularmente, segundo o establecido no Artigo 10, Artigo 11 do ENS e na lexislación sobre protección de datos persoais. Esta análise repetirase:

- Regularmente, polo menos unha vez ao ano.
- Cando se produzan cambios significativos na información manexada.
- Cando se produzan cambios significativos nos servizos prestados.
- Cando se produzan cambios significativos nos sistemas que tratan a información e interveñen na prestación dos servizos.
- Cando ocorra un incidente grave de seguridade.
- Cando se reporten vulnerabilidades graves.

7. Xestión de Incidentes de Seguridade

7.1. Prevención de Incidentes

As distintas unidades organizativas municipais deben evitar, ou polo menos previr na medida do posible, que a información ou os servizos véxanse prexudicados por incidentes de seguridade. Para iso, as unidades organizativas municipais deben implementar as medidas mínimas de seguridade determinadas polo ENS, así como calquera control adicional identificado a través dunha avaliación de ameazas e riscos. Estes controis, e os roles e responsabilidades de seguridade de todo o persoal, deben estar claramente definidos e documentados.

Para garantir o cumprimento da política, todas as unidades organizativas municipais deben:

- Autorizar os sistemas antes de entrar en operación.
- Avaliar regularmente a seguridade, incluíndo avaliacións dos cambios de configuración realizados de forma rutineira.
- Solicitar a revisión periódica por parte de terceiros co fin de obter unha avaliación independente.

7.2. Monitoraxe e Detección de Incidentes

Dado que os servizos pódense degradar rapidamente debido a incidentes, que van desde unha diminución ata o cesamento do nivel de prestación, os servizos deben monitorear a operación de maneira continua para detectar anomalías nos niveis de prestación dos servizos e actuar en consecuencia, segundo o establecido no Artigo 10 do ENS.

A monitoraxe é especialmente relevante cando se establecen liñas de defensa de acordo co Artigo 9 do ENS. Estableceranse mecanismos de detección, análise e reporte que poidan informar os responsables, tanto regularmente como cando se produza unha desviación significativa dos parámetros que se haxan preestablecido como normais.

7.3. Resposta ante Incidentes

As distintas unidades organizativas municipais deben:

- Establecer mecanismos para responder eficazmente os incidentes de seguridade.
- Designar puntos de contacto para as comunicacións con respecto a incidente detectados noutras unidades organizativas municipais ou noutros organismos.

- Establecer protocolos para o intercambio de información relacionada co incidente. Isto inclúe comunicacións, en ambos os sentidos, cos Equipos de Resposta a Emerxencias (CERT).

7.4. Recuperación ante Incidentes e Plans de Continuidade

Para garantir a dispoñibilidade dos servizos críticos, as distintas unidades organizativas municipais deben desenvolver plans de continuidade dos sistemas TIC como parte do seu plan xeral de continuidade de negocio e actividades de recuperación.

En caso necesario, os mesmos será comunicados ás entidades competentes.

8. Obrigacións do persoal

Todos os membros da organización teñen a obrigación de coñecer e cumprir esta Política de Seguridade da Información e Protección de Datos, así como a Normativa de Seguridade que se defina na entidade, sendo responsabilidade do Comité de Seguridade da Información dispoñer os medios necesarios para que a información chegue aos afectados.

Todos os membros da organización atenderán a unha sesión de concienciación en materia de seguridade TIC, polo menos, unha vez cada dous anos. Establecerase un programa de concienciación continua para atender a todos os membros da organización, en particular aos de nova incorporación.

As persoas con responsabilidade no uso, operación ou administración de sistemas TIC recibirán formación para o manexo seguro dos sistemas na medida en que a necesiten para realizar o seu traballo. A formación será obrigatoria antes de asumir unha responsabilidade, tanto se é a súa primeira asignación ou se se trata dun cambio de posto de traballo ou de responsabilidades no mesmo.

O cumprimento da presente Política de Seguridade é obrigatorio por parte de todo o persoal interno ou externo que interveña nos procesos a organización, constituíndo o seu incumprimento infracción grave a efectos laborais ou aos efectos previstos nos pregos das contratacións de servizos externos.

9. Terceiras Partes

Cando se presten servizos ou se xestione información doutras organizacións, faráselles partícipes desta Política de Seguridade e da Normativa de Seguridade que incumba aos devanditos servizos ou información, estableceranse canles para reporte e coordinación dos respectivos Comités de Seguridade da Información e estableceranse procedementos de actuación para a reacción ante incidentes de seguridade.

Dita terceira parte quedará suxeita ás obrigacións establecidas nos devanditos documentos, podendo desenvolver os seus propios procedementos operativos para satisfacela.

Estableceranse procedementos específicos de reporte e resolución de incidencias. Garantirase que o persoal de terceiros está adecuadamente concienciado en materia de seguridade, polo menos ao mesmo nivel que o establecido nesta Política, podendo requirir certificado neste sentido.

Cando algún aspecto da Política 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 antes de seguir adiante.

10. Documentación complementaria

A Política de Seguridade da Información e Protección de Datos cubrirase con documentos máis precisos que axudan a levar a cabo o proposto. Para iso utilizaranse:

- Normas de seguridade *(security standards)*
- Guías de seguridade *(security guides)*
- Procedementos de seguridade *(security procedures)*

As **normas** poñen de común o uso de aspectos concretos do sistema. Indican o uso correcto e as responsabilidades dos usuarios. Son de carácter obrigatorio.

As **guías** teñen un carácter formativo e buscan axudar aos usuarios para aplicar correctamente as medidas de seguridade proporcionando razoamentos onde non existen procedementos precisos. Por exemplo, adoita haber unha guía sobre como escribir procedementos de seguridade.

As guías axudan a previr que se pasen por alto aspectos importantes de seguridade que poden materializarse de varias formas.

Os **procedementos** [operativos] de seguridade afrontan tarefas concretas, indicando o que hai que facer, paso a paso. Son útiles en tarefas repetitivas.

Toda esta documental conformará, principalmente, a documentación de seguridade, á cal poderán vir integrar outro tipo de documentos.

A xestión e o acceso á devandita documentación quedará regulado a través do correspondente documento, onde se poderá atopar o detalle oportuno.

11. Revisión e aprobación da Política de Seguridade

A Política de Seguridade da Información e Protección de Datos será revisada polo Comité de Seguridade da Información a intervalos planificados, que non poderán exceder o ano de duración, ou sempre que se produzan cambios significativos, a fin de asegurar que se manteña a súa idoneidade, adecuación e eficacia.

Os cambios sobre esta Política deberán ser aprobados polo órgano superior competente que corresponda.

Calquera cambio sobre a mesma deberá ser difundido a todas as partes afectadas.

12. Aprobación e entrada en vigor

Texto aprobado o día 28 de xuño de 2024 pola Xunta de Goberno Local do Concello da Coruña.

Esta Política de Seguridade da Información e Protección de Datos é efectiva desde a devandita data e ata que sexa substituída por unha nova Política.

ANEXO A. GLOSARIO DE TERMOS E ABREVIATURAS

Análise de riscos
Utilización sistemática da información dispoñible para identificar perigos e estimar os riscos.

Datos de carácter persoal
Calquera información concernente a persoas físicas identificadas ou identificables.

Xestión de incidentes
Plan de acción para atender ás incidencias que se dean. Ademais de resolvelas debe incorporar medidas de desempeño que permitan coñecer a calidade do sistema de protección e detectar tendencias antes de que se convertan en grandes problemas. ENS.

Xestión de riscos
Actividades coordinadas para dirixir e controlar unha organización con respecto aos riscos. ENS.

Incidente de seguridade
Suceso inesperado ou non desexado con consecuencias en detrimento de a seguridade do sistema de información. ENS.

Información
Caso concreto dun certo tipo de información.

Política de seguridade
Conxunto de directrices plasmadas en documento escrito, que rexen a forma en que unha organización xestiona e protexe a información e os servizos que consideran críticos. ENS.

Principios básicos de seguridade
Fundamentos que deben rexer toda acción orientada a asegurar a información e os servizos. ENS.

Responsable da información
Persoa que ten a potestade de establecer os requisitos dunha información en materia de seguridade.

Responsable da seguridade
O responsable de seguridade determinará as decisións para satisfacer os requisitos de seguridade da información e dos servizos.

Responsable do servizo
Persoa que ten a potestade de establecer os requisitos dun servizo en materia de seguridade.

Responsable do sistema
Persoa que se encarga da explotación do sistema de información.

Servizo
Función ou prestación desempeñada por algunha entidade oficial destinada a coidar intereses ou satisfacer necesidades dos cidadáns.

Sistema de información
Conxunto organizado de recursos para que a información póidase recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, poñer a disposición, presentar ou transmitir. ENS.

ANEXO B. ABREVIATURAS

ENS Esquema Nacional de Seguridade

LOPDGDD Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.

RXPD 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.

TIC Tecnoloxías da Información e as Comunicacións

POC (Punto ou persoa de contacto)

ANEXO C. REFERENCIAS

CCN-STIC-402
Organización e Xestión para a Seguridade dos Sistemas TIC. Decembro 2006.

CCN-STIC-801
ENS - Responsables e Funcións. 2019.

RD 311/2022
Real Decreto 311/2022, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade. BOE/BOE do 4 de maio de 2022.