MIGUEL IGLESIAS MARTÍNEZ, secretario accidental da Deputación Provincial da Coruña.

CERTIFICA: Que o PLENO DA CORPORACIÓN da Deputación Provincial de A Coruña, na sesión ordinaria celebrada o 1 de abril de 2024, adoptou o seguinte acordo:

---

28. Aprobación da revisión da Política de Seguridade da Deputación da Coruña.

Aprobar a modificación da política de seguridade da información da Deputación Provincial da Coruña que é do seguinte tenor literal:

Introdución

Este documento constitúe a Política de Seguridade da Información da Deputación provincial da Coruña, en diante "A Deputación", en cumprimento do artigo 12 (Política de seguridade e requisitos mínimos de seguridade) do Real Decreto 311/2022 do 3 de maio, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica e da medida de seguridade org.1 contemplada no Anexo II deste Real Decreto. Neste sentido, o mencionado artigo 12 establece que "Cada administración pública contará cunha política de seguridade formalmente aprobada polo órgano competente".

A estrutura deste documento segue as pautas establecidas pola guía CCN-STIC-805 (publicada polo Centro Criptológico Nacional, ente adscrito ao Centro Nacional de Intelixencia) para a redacción da Política de Seguridade no ámbito do Esquema Nacional de Seguridade.

A Política de Seguridade da Información recolle a postura da Deputación en canto á seguridade da información e establece os criterios xerais que deben rexer a actividade do organismo en canto á seguridade.

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 de información deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na dispoñibilidade, integridade, confidencialidade, 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.

Esto implica que se deben aplicar as medidas de seguridade esixidas polo Esquema Nacional de Seguridade e a Lei Orgánica de Protección de Datos e garantía de dereitos dixitais (en diante LOPD-gdd), 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.

Así mesmo, as áreas deben estar preparadas para previr, detectar, reaccionar e recuperarse de incidentes, de acordo ao Artigo 8 do ENS.

Misión da Deputación da Coruña

A Deputación da Coruña é unha institución de goberno local que promove o desenvolvemento e o benestar da cidadanía nos municipios que compoñen a provincia da Coruña. Actúa prestando servizos directamente aos cidadáns e sobre todo en cooperación cos concellos. A Deputación ten como misión a asistencia técnica, económica e material aos concellos para que poidan prestar servizos locais de calidade de forma homoxénea en toda a provincia, coordinando servizos e organizando servizos públicos de carácter supramunicipal.

Marco Normativo da Deputación da Coruña

A normativa legal á que se atopa sometida a Deputación da Coruña, máis relacionada coa súa actividade, recóllese a continuación, en orde cronolóxica ascendente:

- Lei 7/85 Reguladora das Bases de Réxime Local.
- Real Decreto 2568/1986, do 28 de novembro, polo que se aproba o Regulamento de Organización, Funcionamento e Réxime Xurídico das Entidades Locais.
- Lei 5/1997, do 22 de xullo, de Administración Local de Galicia.
- Lei 33/2003, do 3 de novembro, do Patrimonio das Administracións Públicas.
- Lei 38/2003, do 17 de novembro, Xeneral de Subvencións.
- Lei 58/2003, do 17 de decembro, Xeral Tributaria.
- Real Decreto Lexislativo 2/2004, do 5 de marzo, polo que se aproba o texto refundido da Lei Reguladora das Facendas Locais.
- Lei 9/2007, do 13 de xuño, de subvencións de Galicia.
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica.
- Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno.
- Lei 27/2013 de Racionalización e Sustentabilidade da Administración Local.
- Orde HAP/2425/2013, do 23 de decembro, pola que se publican os límites dos distintos tipos de contratos a efectos da contratación do sector público a partir do 1 de xaneiro de 2014.

- Real Decreto-lei 8/2014, do 4 de xullo, de aprobación de medidas urxentes para o crecemento, a competitividade e a eficiencia.
- Lei 18/2014, do 15 de outubro, de aprobación de medidas urxentes para o crecemento, a competitividade e a eficiencia.
- Lei 2/2015, do 29 de abril, do emprego público de Galicia.
- Lei 39/2015, do 1 de outubro, de Procedemento Administrativo Común das Administracións Públicas.
- Lei 40/2015, do 1 de outubro de Réxime Xurídico do Sector Público.
- Real Decreto Lexislativo 5/2015, do 30 de outubro, polo que se aproba o texto refundido da Lei do Estatuto Básico do Empregado Público.
- REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEO E DO CONSELLO do 27 de abril de 2016 relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se deroga a Directiva 95/46/CE (Regulamento xeral de protección de datos)
- Lei 9/2017, do 8 de novembro, de Contratos do Sector Público, pola que se transpoñen ao ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23/UE e 2014/24/UE, do 26 de febreiro de 2014.
- Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.
- Lei 6/2020, do 11 de novembro, reguladora de determinados aspectos dos servizos electrónicos de confianza.
- Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade.

Forman tamén parte do marco normativo as restantes normas aplicables á administración electrónica da Deputación da Coruña derivadas das relacionadas anteriormente e publicadas nas sedes electrónicas comprendidas dentro do ámbito de aplicación desta Política.

Política Xeral de Seguridade

O obxecto da presente Política é establecer a postura da Deputación respecto á Seguridade que afecta os procesos relacionados co desempeño das súas funcións e, moi particularmente, cos relacionados coa administración electrónica, tanto desde o punto de vista dos usuarios dos servizos, como desde o punto de vista interno, para a xestión da propia Entidade.

A Diputación utiliza as Tecnoloxías da Información e as Comunicacións para prestar os seus servizos, polo que é consciente de que estes sistemas deben ser administrados con dilixencia, tomando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados.

Así mesmo, tamén é consciente de que os incidentes de seguridade poden estar provocados desde lugares remotos, a través das conexións a redes de comunicacións das que se dispón e, moi concretamente, a través das conexións á Internet (ciber-ataques).

O fin da política é contrarrestar as ameazas mencionadas anteriormente cos medios suficientes, dentro das posibilidades orzamentarias. Para este fin, establecerase unha estrutura de seguridade, xunto cos mecanismos apropiados para a súa xestión, e un conxunto de instrumentos de apoio de forma que se garanta:

- O cumprimento dos obxectivos da misión da Deputación e de prestación dos seus servizos
- O cumprimento da lexislación e normativa aplicables.

Como norma xeral, terase un enfoque de orientación ao risco á hora de deseñar as medidas de seguridade necesarias, poñendo máis foco e esforzo na mitigación do que supoña un maior risco.

As distintas unidades baixo cuxa responsabilidade se atopan os servizos prestados deberán contemplar a seguridade desde o mesmo momento en que se concibe un novo sistema ou servizo, aplicando para estes e para os xa existentes, as medidas de seguridade prescritas polo Esquema Nacional de Seguridade para garantir a dispoñibilidade, confidencialidade, integridade, autenticidade e trazabilidade dos servizos e da información.

Os requisitos de seguridade dos sistemas, as necesidades e requisitos de formación dos usuarios, e as necesidades de financiamento deben ser identificados e incluídos na planificación dos sistemas e nos pregos de prescricións utilizados para a realización de proxectos que involucren ás Tecnoloxías da Información e Comunicacións (TIC).

Articularanse mecanismos de prevención, detección, resposta e conservación con obxecto de minimizar o impacto dos incidentes de seguridade.

En canto á prevención, débese evitar que os servizos e a información resulten afectados por un incidente de seguridade. Para iso, a Deputación implementará as medidas de seguridade establecidas no Anexo II do ENS, así como medidas adicionais que puidesen ser identificadas no proceso de análise de riscos e, en xeral, medidas que disuadan a posibles atacantes e que reduzan a superficie de exposición para minimizar a probabilidade de que as ameazas cheguen a materializarse.

En canto á detección, implementaranse as medidas adecuadas para descubrir a presenza dun incidente na fase máis temperá posible, con obxecto de contelo e minimizar o seu impacto. Sempre que sexa posible, detectaranse de forma automática os incidentes de seguridade, utilizando elementos de monitoraxe dos servizos ou de detección de anomalías. Para os incidentes detectados polos usuarios, xa sexan internos ou externos, estableceranse os pertinentes canles de comunicación de incidentes.

En canto á resposta, poñeranse en marcha mecanismos, asociados aos procedementos de xestión de incidentes e de continuidade das operacións, para a restauración da información e os servizos que puidesen haberse se afectados por un incidente de seguridade.

En canto á conservación, despregaranse medidas que garantan a conservación da información en soporte electrónico.

Alcance

Esta Política de Seguridade é de aplicación a todos os servizos prestados pola Deputación, así como a todo o persoal, sen excepcións.

Organización da Seguridade

A seguridade na Deputación está soportada sobre as estruturas e roles que se describen a continuación:

- Estrutura de especificación, que é a que se encarga de establecer os requisitos de seguridade asociados aos servizos prestados.
- Estrutura de supervisión, que é a que se encarga de verificar o cumprimento dos requisitos de seguridade e o aliñamento continuo cos obxectivos da organización.
- Estrutura de operación, que se encarga de implantar as medidas de seguridade identificadas.

Estrutura de especificación

Esta estrutura é a encargada de determinar os requisitos de seguridade que serán de aplicación aos servizos prestados pola Deputación e a garantir o cumprimento normativo asociado que lle é de aplicación, en concreto o Real Decreto 311/2022 do 3 de maio polo que se regula o Esquema Nacional de Seguridade.

Descríbense a continuación as funcións e responsabilidades dos roles asociados á especificación.

Responsable da Información

É o responsable último da protección da información, garantindo a súa dispoñibilidade, confidencialidade e integridade.

Ten a potestade de establecer os requisitos de seguridade da información, no sentido de asignarlle á mesma unha valoración que determinará o nivel de protección que requira. O establecemento de requisitos poderá realizarse a proposta do Responsable de Seguridade da Información e contando coa opinión do Responsable do Sistema.

O Responsable da Información ten, de forma exclusiva, a potestade de modificar no tempo a valoración mencionada anteriormente, se así fose necesario.

Este rol poderá recaer nunha ou varias persoas, e mesmo nun órgano colexiado, podendo coincidir co Responsable do Servizo.

Responsable do Servizo

Este rol é o responsable de establecer os niveis de seguridade (ou requisitos de seguridade) que requiran os servizos prestados, que determinarán as medidas de protección necesarias, así como a súa intensidade.

O establecemento de requisitos poderá realizarse a proposta do Responsable de Seguridade da Información e contando coa opinión do Responsable do Sistema. Os requisitos do servizo deben ter en conta os requisitos da información que manexen.

Este rol poderá recaer nunha ou varias persoas, e mesmo nun órgano colexiado, podendo coincidir co Responsable da Información.

Responsable do Tratamento

O Responsable do Tratamento é a persoa física ou xurídica sobre a que recaen as funcións xenéricas recolleitas na normativa de protección de datos aplicable e vixente en canto a responsabilidade última dos tratamentos de datos persoais que se leven a cabo.

En xeral, esta figura determina os fins e os medios relacionados co tratamento dos datos persoais.

As súas funcións son as seguintes:

- Garantir o cumprimento de principios relativos ao tratamento recolleitos na normativa vixente en materia de protección de datos persoais.
- Garantir o cumprimento das normativas existentes na Deputación da Coruña en materia de protección de datos persoais.
- Garantir o mantemento adecuado, e conforme á lexislación vixente, do Rexistro de Actividades de Tratamento.
- Garantir o cumprimento do deber de información ao interesado recolleito na normativa vixente en materia de protección de datos persoais.
- Establecer os mecanismos necesarios para recibir, xestionar e resolver solicitudes de exercicio de dereitos por parte dos interesados.
- Avaliar o risco para os dereitos e liberdades dos afectados nas brechas de seguridade e a posible notificación ás autoridades de control e aos afectados.
- Determinar as medidas técnicas e organizativas apropiadas que se deben aplicar a fin de garantir e acreditar que o tratamento é conforme coa normativa vixente de protección de datos persoais.
- Actuar como punto de contacto coas autoridades de control, conxuntamente co Delegado de Protección de Datos.
- Implantar e seguir os programas de formación e sensibilización do persoal da Deputación da Coruña en materia de protección de datos persoais.

Estrutura de supervisión

A estrutura de supervisión da seguridade encárgase de verificar a correcta implantación e operación dos requisitos de seguridade que se estableceron, para manter a aliñación cos obxectivos e de cumprir coas normas e lexislación aplicable.

Na supervisión global de todas as actividades relativas á seguridade da información atópase o Responsable de Seguridade da Información.

Na supervisión global das actividades relativas á seguridade física atópase o Responsable de Seguridade Física.

Para a coordinación global e integral da seguridade atópase o Comité de Seguridade da Información.

As funcións e responsabilidades de cada unha das figuras descríbense a continuación:

Responsable de Seguridade da Información

É responsable da determinación das decisións para satisfacer os requisitos de seguridade da información e dos servizos na Deputación.

Este Responsable forma parte do Comité de Seguridade da Información, sendo o encargado de elevar ao devandito Comité os asuntos de interese relacionados coa seguridade da información.

As súas responsabilidades comprenden:

- Manter a seguridade da información manexada e dos servizos prestados polos sistemas de información da Deputación.
- Promover e coordinar a realización de programas de formación e sensibilización en materia de seguridade da información.
- Levar a cabo a realización de análise de riscos de seguridade da información, así como os plans para mitigalos, de forma periódica, elevando as conclusións ao Comité de Seguridade da Información para a súa aprobación.
- Elaborar a normativa de seguridade derivada da Política de Seguridade.
- Aprobar os procedementos operativos para a realización das actividades que se atopen reguladas pola normativa interna de seguridade.
- Manter actualizada a documentación asociada á xestión da seguridade da información: normativas, procedementos e rexistros.
- Supervisar a implantación, manter, controlar e verificar o cumprimento das normas e procedementos establecidos.
- Coordinar e controlar as medidas de seguridade da información e de protección de datos da Deputación.
- Conseguir que se elabore o orzamento anual de seguridade de tecnoloxías da información e as comunicacións (TIC) da Deputación.

- Supervisar as situacións excepcionais (ou incidentes) de ciberseguridade producidas na Deputación.
- Analizar os indicadores de seguridade para medir a eficacia e eficiencia das medidas implantadas.
- Analizar os incidentes de seguridade da información reflectidos nos rexistros destes e verificar que se estableceron os plans para a súa resolución.
- Velar pola inclusión de cláusulas de seguridade nos contratos con terceiras partes e polo seu cumprimento.
- Autorizar por escrito a execución de procedementos de recuperación de datos nos casos en que se requira.
- Elaborar o documento de Declaración de Aplicabilidade de medidas de seguridade.
- Establecer a categoría dos sistemas de información da Deputación.
- Colaborar coas auditorías externas/internas en materia de seguridade da información, revisalas e encargar aos responsables dos sistemas a implantación das correccións que se deriven.
- Notificar ao CCN-CERT os incidentes de seguridade que se deban comunicar, en base á lexislación vixente.
- Constituírse en punto de contacto do CCN-CERT en materia de seguridade da información.
- Recibir, interpretar e aplicar as instrucións e guías emanadas do CCN-CERT para a súa aplicación no ámbito da Deputación.

Delegado de Protección de Datos

O Delegado de Protección de Datos é a figura que actúa como asesor, supervisor e interlocutor do Responsable do Tratamento no ámbito das competencias marcadas pola normativa en materia de protección de datos vixente.

As súas funcións son:

- Informar e asesorar á Deputación da Coruña, e a todo o persoal que se ocupe do tratamento de datos persoais, das obrigacións que se deriven do Regulamento Xeral de Protección de Datos e doutras disposicións relacionadas coa protección de datos.
- Supervisar o cumprimento do Regulamento Xeral de Protección de Datos na Deputación da Coruña.
- Asesorar acerca da avaliación de impacto relativa á protección de datos e supervisar a súa aplicación.
- Cooperar coa Autoridade de Control.

- Actuar como punto de contacto da Autoridade de Control conxuntamente co Responsable do Tratamento.

Ademais, asesorará ao Responsable do Tratamento ou, en xeral, a aquela figura que o necesite, nas seguintes áreas:

- Cumprimento de principios relativos ao tratamento, como os de limitación na finalidade, minimización ou exactitude dos datos.
- Identificación das bases xurídicas dos tratamentos.
- Valoración da compatibilidade de finalidades distintas das que orixinaron a recollida inicial dos datos.
- Existencia de normativa sectorial que poida determinar condicións de tratamento específicas 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 de solicitudes de exercicio de dereitos por parte dos interesados.
- Valoración das solicitudes de exercicio de dereitos por parte dos interesados.
- Mantemento de rexistro de encargados de tratamento
- Asesoramento a Contratación en relación cos encargados de tratamento en canto ao contido dos contratos ou actos xurídicos que regulen a relación entre a Deputación da Coruña e os encargados do tratamento.

Responsable de Seguridade Física

É responsable da definición, coordinación, difusión e verificación dos requisitos de seguridade física das instalacións onde se aloxen os sistemas de información

Este Responsable forma parte do Comité de Seguridade da Información, sendo o encargado de elevar ao devandito Comité os asuntos de interese relacionados coa seguridade física dos locais e as infraestruturas.

As súas responsabilidades comprenden:

- Identificación de necesidades de seguridade física.
- Conseguir a elaboración dun orzamento anual de investimentos e actuacións en seguridade física.
- Supervisar a instalación e o mantemento posterior dos elementos e servizos destinados á seguridade física.
- Analizar os incidentes de seguridade física que se poidan producir e establecer actuacións para dar resposta aos mesmos.

- Manter actualizada a documentación asociada á xestión da física: normativas, procedementos e rexistros.

Comité de Seguridade da Información

A misión do Comité de Seguridade é a coordinación xeral das actividades que teñen relación coa seguridade integral.

Un obxectivo fundamental do Comité de Seguridade é a posta en común de aspectos importantes da seguridade entre todos os responsables. Con iso evitarase que actividades referentes á seguridade, que poidan afectar a varias ou todas as unidades da organización, queden sen o suficiente coñecemento por parte dos seus responsables, ou sen o suficiente apoio ou compromiso, prexudicando a eficacia.

As funcións do Comité de Seguridade son:

- Establecer uns obxectivos de seguridade da información corporativos aliñados cos obxectivos de prestación de servizos e xestión da Deputación.
- Informar regularmente o estado da seguridade á Presidencia.
- Elaborar a estratexia de evolución da organización no que respecta a seguridade da información.
- Elaborar e revisar regularmente a Política de Seguridade e propoñer cambios, se procede, para a súa aprobación polo Pleno da Deputación.
- Revisar as normativas internas de seguridade que se poidan derivar da Política de Seguridade, a proposta do Responsable de Seguridade da Información, e aprobalas, no seu caso.
- Elaborar e propoñer os requisitos de formación para a persoal clave que manexe información, sistemas e infraestruturas físicas.
- Asumir o papel de dono dos riscos de seguridade da información (quen ten a potestade para aceptar os riscos residuais sobre os activos), tendo en conta os requisitos de seguridade establecidos para os diferentes activos por parte dos seus responsables correspondentes, aprobando as apreciacións de riscos realizadas e aceptando o risco residual resultante, no seu caso.
- Aprobar os plans de tratamento de riscos e mellora da seguridade que xurdan a raíz das apreciacións de riscos realizadas e velar pola coordinación da súa execución nas distintas unidades.
- Seguir o desenvolvemento dos plans de acción aprobados.
- Coordinar as actuacións en materia de seguridade que se poidan estar a realizar en diferentes unidades da Deputación, con obxecto de evitar esforzos duplicados ou desalineados coa Política de Seguridade

- Priorizar as actuacións en materia de seguridade cando os recursos sexan limitados.
- Velar por que a seguridade da información téñase en conta en todos os proxectos de 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.
- Supervisar e participar na resolución dos incidentes de seguridade que se poidan producir e expor as estratexias e salvagardas ante os mesmos, velando pola adecuada coordinación dos diferentes actores involucrados na xestión destes incidentes.
- Impulsar a realización das auditorías ordinarias regulares, polo menos cada dous anos, que permitan verificar o cumprimento das obrigacións da Deputación en materia de seguridade.
- Analizar información de indicadores de seguridade que puidese haber definidos. Tomar decisións en caso de desviación respecto aos limiares establecidos.
- Resolver os conflitos de responsabilidade que poidan aparecer entre os diferentes responsables e/ou entre diferentes áreas da Deputación, elevando aqueles casos nos que non teña suficiente autoridade para decidir.
- Promover a mellora continua da seguridade da información.

O Comité de Seguridade da Información terá unha composición de membros fixos e outros que participarán en función dos temas para tratar.

Serán membros fixos do Comité de Seguridade:

- O Presidente da Deputación
- O Responsable de Seguridade da Información
- O Responsable do Sistema
- O Responsable de Seguridade Física
- Os responsables dos diferentes Servizos da Deputación, ou o deputado que os represente.

Adicionalmente, poderán asistir ao Comité de Seguridade os responsables das materias específicas a tratar nas reunións, que poderán ser convidados en función do contido da axenda.

Cando os asuntos para tratar incidan ou poidan incidir en tratamentos de datos persoais, deberase convocar ao Delegado de Protección de Datos.

Frecuencia de reunións do Comité de Seguridade da Información

O Comité de Seguridade da Información reunirase con carácter ordinario, como mínimo, unha vez cada seis meses e, extraordinariamente, por convocatoria dalgún dos seus membros fixos.

Convocatorias do Comité de Seguridade

As convocatorias do Comité de Seguridade serán realizadas polo Secretario do Comité, quen elaborará unha acta recollendo os asuntos tratados e as decisións tomadas.

O Secretario do Comité preparará a axenda de temas a tratar, achegando a información necesaria para a toma de decisións e será o responsable de que as accións acordadas lévense a cabo, xa sexa por execución directa ou por delegación.

Estrutura de Operación

A estrutura de operación da seguridade debe asumir a administración operativa da seguridade dos sistemas de información, implantando nos devanditos sistemas as medidas necesarias para satisfacer os requisitos de seguridade establecidos pola estrutura de especificación.

Descríbense a continuación as funcións e responsabilidades das figuras asociadas á estrutura de operación.

Responsable dos Sistemas de Información

As súas funcións e responsabilidades son:

- Desenvolver, operar e manter o sistema de información durante todo o seu ciclo de vida, incluíndo as súas especificacións, instalación e verificación do seu correcto funcionamento.
- Definir a topoloxía e a xestión do sistema de información, establecendo os criterios de uso e os servizos dispoñibles no mesmo.
- Confirmarse de que as medidas de seguridade intégrense adecuadamente no marco xeral de seguridade.
- Definir, en coordinación co Responsable de Seguridade da Información, as especificacións funcionais de seguridade dos Sistemas de Información da Deputación.
- Garantir que no deseño de sistemas de información e redes de comunicacións contémplense desde o principio os aspectos necesarios de seguridade da información en canto a dispoñibilidade, integridade, confidencialidade, autenticación, control de acceso, auditoría e rexistro.
- Revisar que a configuración de seguridade tras a instalación dun sistema novo é a adecuada.
- Revisar que a configuración de seguridade tras os cambios nun sistema segue sendo a adecuada.
- Verificar o funcionamento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos ou recursos con dereitos distintos dos autorizados, sen que en ningún caso póidanse desactivar.
- Seguir os foros de vulnerabilidades e elaboración do calendario de aplicación de parches para os sistemas de información, en función dos que xurdan e o impacto que teñan na seguridade (os parches mesmos aplicaranos os administradores de sistemas).
- Implantar as medidas de seguridade que resulten dos plans de tratamento de riscos ou plans de accións correctivas a raíz das auditorías de seguridade da información.
- Proporcionar datos para a alimentación de indicadores de seguridade da información.

- Supervisar os procedementos de copia de seguridade.
- Realizar auditorías técnicas periódicas da infraestrutura de tecnoloxías da información, sistemas e aplicacións.

O Responsable do Sistema ten a potestade para propoñer a suspensión do tratamento dunha certa información ou a prestación dun determinado servizo se apreciase deficiencias graves de seguridade que puidesen afectar á satisfacción dos requisitos establecidos. A proposta debe ser acordada cos responsables da información e os servizos afectados e o Responsable da Seguridade e elevada ao Presidente da Deputación para a súa decisión final.

Designación de roles das estruturas de seguridade

O Pleno da Deputación da Coruña designará, inicialmente, e ratificará nas sucesivas revisións desta Política de Seguridade, os roles de goberno da seguridade recollidos na presente Política, que exercerán as súas funcións de forma horizontal para toda a información e servizos prestados pola Deputación da Coruña.

Establécese que o Comité de Seguridade é o órgano con potestade para modificar a designación de roles establecida anteriormente. En caso de modificación, recollerase a mesma na acta da sesión correspondente, que constituirá o documento xustificativo en tanto non se realice unha revisión do presente documento de Política de Seguridade, momento no que se ratificarán os novos nomeamentos polo Pleno.

Os roles de goberno da seguridade quedan establecidos como segue:

ROL	EXERCIDO POR
Responsable da Información	O Comité de Seguridade da Información. O Comité de Seguridade delega nos responsables das diferentes áreas organizativas da Deputación para a operativa do día a día coa información propia de cada área (autorizacións, cualificación de información e outras actividades atribuíbles ao responsable da información)
Responsable do Servizo	O Comité de Seguridade da Información. O Comité de Seguridade delega nos responsables das diferentes áreas organizativas da Deputación para a operativa do día a día cos servizos ofrecidos por cada área para as actividades atribuíbles ao responsable do servizo.
Responsable de Seguridade da Información	Titular da Xefatura do Servizo de Informática e Administración Electrónica.
Responsable de Seguridade Física	Titular da Xefatura do Servizo de Sistemas e Soporte
Responsable dos Sistemas de Información	Titular da Xefatura do Servizo de Sistemas e Soporte

Presidente do Comité de Seguridade	Titular da Presidencia da Deputación
Secretario do Comité de Seguridade	Responsable de Seguridade da Información
Responsable do Tratamento	Deputación da Coruña
Delegado de Protección de Datos	Titular da Oficialía Mayor

Os roles de seguridade quedan asignados aos postos organizativos recolleitos no cadro anterior, quedando automaticamente designados os seus titulares en cada momento.

Mecanismos de coordinación e de resolución de conflitos

A coordinación entre os diferentes roles participantes das actividades de seguridade así como a resolución de conflitos que puidesen xurdir entre eles levarase a cabo no seo do Comité de Seguridade da Información.

Funcións e obrigacións

Á marxe das funcións e atribucións que incumben ao persoal que integra o esquema organizativo responsable da seguridade, establécense a continuación as obrigacións do persoal da Deputación así como daqueles terceiros que teñan acceso aos seus sistemas de información.

Funcións e obrigacións do persoal

Todo o persoal da Deputación ten a obrigación de coñecer a Política de Seguridade e cumprila. O Comité de Seguridade da Información dispoñerá os medios para que esta Política chegue aos afectados.

Así mesmo, o persoal deberá asistir ás sesións de concienciación e formación en materia de seguridade para as que sexa designado como asistente.

Funcións e obrigacións de terceiras partes

As terceiras partes (entidades externas á Deputación) que estean relacionadas coa xestión, mantemento ou explotación dos servizos prestados pola Deputación serán feitas partícipes desta Política. As terceiras partes quedarán obrigadas ao cumprimento desta Política e ás normativas que se poidan derivar dela.

As terceiras partes poderán desenvolver os seus propios procedementos operativos para satisfacer a Política.

Deberanse establecer procedementos específicos de comunicación de incidencias para que os terceiros afectados poidan reportalas.

O persoal das Terceiras Partes deberá recibir sesións de concienciación, tal como se esixe para o persoal propio.

Cando algún aspecto desta Política non poida ser satisfeito por unha terceira parte, o Responsable de Seguridade da Información deberá realizar un informe do risco en que se incorre. Ese risco deberá ser aceptado polo Comité de Seguridade da Información.

Formación e concienciación

De maneira sistemática realizaranse accións de formación e concienciación en materia de seguridade da información.

O obxectivo da acción formativa e de concienciación é dobre:

- Manter informado o persoal máis directamente relacionado co manexo de información e os sistemas que a tratan sobre os procedementos existentes de seguridade, configuración segura de equipos, desenvolvemento seguro, xestión de incidentes de seguridade, riscos, etc.
- Concienciar ao persoal, en xeral, da importancia da seguridade e dos procedementos básicos de manexo e intercambio de información.

Todo o persoal deberá asistir a unha sesión de concienciación en materia de seguridade da información coa periodicidade que se determine por parte do Comité de Seguridade da Información.

As persoas con responsabilidade no uso, a xestión, mantemento ou explotación dos servizos soportados nas 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.

Xestión de riscos

Todos os sistemas, servizos e infraestruturas suxeitos á presente Política deberán ser obxecto dunha análise de riscos que avalíe as ameazas e os riscos aos que están expostos.

A análise repetirase regularmente, polo menos unha vez ao ano, elevándose as conclusións ao Comité de Seguridade da Información.

Realizarase unha análise de riscos dos sistemas de información en períodos inferiores a un ano cando:

- haxa cambios nos servizos esenciais prestados ou cambios significativos nas infraestruturas que os soportan.
- ocorra un incidente de seguridade grave.
- identifíquense ameazas severas que non fosen tidas en conta ou vulnerabilidades graves que non estivesen contrarrestadas polas medidas de protección implantadas.

O Comité de Seguridade da Información establecerá os niveis aceptables de risco e aprobará as actuacións para levar a cabo no caso de que se incorra en niveis de risco non aceptables.

Datos de carácter persoal

A Diputación só recollerá datos de carácter persoal cando sexan adecuados, pertinentes e non excesivos, con fins determinados, explícitos e lexítimos, e non serán tratados ulteriormente de

maneira incompatible co devanditos fin. De igual modo, a Deputación adoptará as medidas técnicas e organizativas necesarias para o cumprimento da lexislación vixente en materia de protección de datos.

Desenvolvemento da Política de Seguridade e Estruturación da Documentación de Seguridade

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

A aprobación, revisión e nivel de acceso dos documentos anteriormente apuntados farase conforme ao seguinte:

- Política de Seguridade da Información:
    - Será aprobada polo Pleno da Deputación da Coruña, sendo responsabilidade do Comité de Seguridade da Información a súa revisión para elevar unha proposta de modificación cando sexa necesario.
    - Será un documento de público acceso.
- Normativa Interna de seguridade da información:
    - Será aprobada polo Comité de Seguridade da Información, sendo o Responsable de Seguridade da Información o responsable da súa elaboración e actualización.
    - A normativa de seguridade estará ao dispor de todo o persoal da Deputación.
- Procedementos operativos de seguridade da información:
    - Serán aprobados polo Responsable de Seguridade, sendo o Responsable do Sistema ou o responsable do servizo competente na materia do procedemento, o responsable da súa elaboración e actualización.
    - Os procedementos operativos estarán ao dispor de todo o persoal da Deputación que os requira levar a cabo para a súa actividade.

Revisión da Política de Seguridade

A presente política de seguridade será revisada con carácter anual polo Comité de Seguridade da Información, que poderá modificala e elevala para a súa aprobación.

E para que conste e sen prexuízo dos termos da aprobación da acta, segundo o disposto no artigo

206 do Regulamento de organización, funcionamento e réxime xurídico das Corporacións locais, expido a presente de orde e co visto e prace do Sr. Presidente na Coruña.

O secretario accidental: Miguel Iglesias Martínez (asinado dixitalmente)

O presidente: Valentín González Formoso (asinado dixitalmente)