Deputación DA CORUÑA

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

CERTIFICA: Que o PLENO DA CORPORACIÓN da Deputación Provincial de A Coruña, na sesión ordinaria celebrada o 27 de marzo de 2026, adoptou o seguinte acordo:

---

24. 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 cuxo texto definitivo é o seguinte:

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.
Isto 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

O marco normativo aplicable á seguridade da información da Deputación da Coruña identifícase e mantén no **"Rexistro de Normas que constitúen o Marco Legal e Regulatorio"**, o cal forma parte do sistema documental de seguridade da organización.

Este rexistro mantense actualizado e constitúe a referencia normativa para a aplicación, revisión e mellora continua da presente Política de Seguridade.
Adicionalmente, forman 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.

Principios da Política de Seguridade da Información

Toda a actividade relacionada co uso dos activos de información e o tratamento de datos persoais na Deputación rexerase polos seguintes principios:

- Alcance estratéxico: A Política de Seguridade da Información contará co compromiso de todos os niveis directivos de modo que a seguridade da información e a protección de datos estean integradas e coordinadas coas decisións estratéxicas da Deputación.

- Seguridade integral: A seguridade entenderase como un proceso integral e planificado, constituído por todos os elementos técnicos, humanos, materiais, procedementais e organizativos relacionados cos sistemas de información, evitando as actuacións puntuais ou tratamentos conxunturais.

- Xestión da seguridade baseada nos riscos: A análise e a xestión dos riscos serán parte esencial e permanente do proceso de seguridade. Mediante a análise de riscos detéctanse os problemas de seguridade e coa súa correcta xestión perséguese reducilos a un nivel aceptable mediante a selección e implantación de medidas de seguridade.

- Prevención, detección, resposta e conservación: A seguridade do sistema debe contemplar as accións relativas aos aspectos de prevención, detección, resposta e conservación, ao obxecto de minimizar as súas vulnerabilidades e lograr que as ameazas sobre o mesmo non se materialicen ou que, no caso de facelo, non afecten gravemente á información que manexa ou os servizos que aguzosa.

- Existencia de liñas de defensa: Os sistemas de información dispoñerán dunha estratexia de protección constituída por múltiples capas de seguridade disposta de forma que, cando unha das capas sexa comprometida, permita desenvolver unha reacción adecuada fronte aos incidentes que non puideron evitarse, reducindo a probabilidade de que o sistema sexa comprometido no seu conxunto e minimizar o impacto final sobre o mesmo.

- Vixilancia continua: A vixilancia continua permitirá a detección de actividades ou comportamentos anómalos e a súa oportuna resposta.

- Reevaluación periódica: A avaliación permanente do estado da seguridade dos activos permitirá medir a súa evolución, detectando vulnerabilidades e identificando deficiencias de configuración. As medidas de seguridade se reevaluarán e actualizarán periodicamente,

adecuando a súa eficacia á evolución dos riscos e os sistemas de protección, podendo chegar a unha reconsideración da seguridade, se fose necesario.

- Diferenciación de responsabilidades: Nos sistemas de información diferenciaranse o responsable da información, o responsable do servizo, o Responsable de Seguridade e o Responsable do Sistema. A responsabilidade da seguridade dos sistemas de información estará diferenciada da responsabilidade sobre a explotación dos sistemas de información concernidos.

- Ciclo completo e seguridade por defecto: Contemplaranse os aspectos de seguridade en todas as fases do ciclo de vida dos sistemas de información, garantindo a súa seguridade por defecto. A seguridade debe considerarse como parte da operativa habitual, estando presente e aplicándose desde o deseño inicial dos sistemas de información.

- Autorización para operar: Ningún sistema de información poderá entrar en operación sen que o seu Responsable do Sistema, o Responsable de Seguridade e, no seu caso, o Comité de Seguridade completasen o proceso de verificación de medidas, análises de riscos e aceptación formal do risco residual.

- Proporcionalidade: O establecemento de medidas de protección, detección e recuperación será proporcional, nos seus custos económicos e operativos, aos potenciais riscos e á criticidad e valor da información e dos servizos afectados.

- Responsabilidade proactiva: O responsable do tratamento deberá aplicar as medidas técnicas e organizativas apropiadas a fin de garantir e poder demostrar que o tratamento da información se fai conforme a normativa española e europea na materia.

- Lexitimación no tratamento de datos persoais: Só se tratarán os datos de carácter persoal cando este tratamento estea lexitimado nalgunha das causas previstas no Regulamento (UE) 2016/679.

- Licitud, lealdade e transparencia: Os datos de carácter persoal serán tratados de maneira lícita, leal e transparente en relación co interesado.

- Limitación da finalidade: Os datos persoais deben ser recollidos con fins determinados, explícitos e lexítimos, e non serán tratados ulteriormente de maneira incompatible co devanditos fin.

- Minimización de datos: Os datos tratados serán adecuados, pertinentes e limitados ao necesario en relación cos fins para os que sexan tratados.

- Integridade e calidade: Garantirase o mantemento da integridade e calidade da información, así como dos procesos de tratamento da mesma, establecéndose os mecanismos para asegurar que os procesos de creación, tratamento, almacenamento e distribución da información contribúen a preservar a súa exactitude e, no seu caso, actualización.

- Limitación do prazo de conservación: Os datos conservaranse durante o tempo necesario para cumprir coa finalidade para a que solicitáronse e para determinar as posibles

responsabilidades que puidesen derivarse do seu tratamento. Os datos poderán conservarse durante períodos máis longos cando sexan tratados exclusivamente con fins de arquivo en interese público, fins de investigación científica e histórica ou fins estatísticos consonte o establecido no Regulamento (UE) 2016/679. O tratamento para estes fins realizarase coas medidas técnicas e organizativas adecuadas, respectando particularmente o principio de minimización dos datos persoais, así como, cando sexa posible, o seu anonimización. Nesta modalidade de tratamento será á súa vez de aplicación o disposto na normativa sobre arquivos e documentación.

- Confidencialidade: Quen interveña no tratamento estarán obrigados a gardar o deber de segredo, mesmo despois de finalizar o proceso de tratamento.

- Profesionalidade: A seguridade dos sistemas de información estará implantada, atendida, revisada e auditada por persoal cualificado e formado, que participará en todas as fases do ciclo de vida dos sistemas.

- Prevención, dispoñibilidade e recuperación: Desenvolveranse plans de acción e liñas de traballo específicas orientadas a previr fraudes, incumprimentos ou incidentes relacionados coa seguridade. Asegurarase o nivel de dispoñibilidade requirido para os activos e recuperación ante calquera continxencia.

Obxectivos de Seguridade da Información

A Política de Seguridade da Información establece como obxectivos xerais garantir un nivel adecuado de protección dos sistemas de información, os servizos e os datos xestionados pola Deputación.
En particular, son obxectivos de seguridade da información:

- Garantir a confidencialidade, integridade, dispoñibilidade, autenticidade e trazabilidade da información tratada pola Deputación.

- Asegurar a continuidade e calidade dos servizos, minimizando o impacto de incidentes de seguridade sobre a prestación dos mesmos.

- Protexer os sistemas de información fronte a ameazas internas e externas, reducindo o nivel de risco a valores aceptables.

- Detectar, xestionar e responder de forma eficaz aos incidentes de seguridade da información.

- Garantir o cumprimento do Esquema Nacional de Seguridade, da normativa de protección de datos persoais e do resto de normativa aplicable.

O grao de cumprimento destes obxectivos será obxecto de seguimento periódico mediante indicadores e métricas, que permitirán avaliar a eficacia das medidas implantadas e apoiar a toma de decisións en materia de seguridade da información.

Requisitos mínimos e Directrices

Adoptaranse as medidas técnicas, organizativas e procedementais necesarias para o cumprimento da normativa legal vixente en materia de seguridade da información. A Política de Seguridade da Información establecerase consonte os principios básicos sinalados e desenvolverase aplicando os seguintes requisitos mínimos e directrices:

- Protección das instalacións: Os activos de información emprazaranse en áreas seguras, protexidas por controis de acceso físico adecuados ao seu nivel de criticidad. Os sistemas e

os activos de información situados nas devanditas áreas estarán suficientemente protexidos fronte a ameazas físicas ou ambientais.

- Autorizacións e controis de acceso: O acceso á información estará debidamente controlado e limitado as persoas usuarias, procesos, dispositivos ou outros sistemas de información autorizados, e exclusivamente ás funcións permitidas. A tal fin implementarnse os mecanismos de identificación e autenticación adecuadas para cada activo.

- Xestión de activos de información: Os activos de información inventariaranse e categorizarán. Os soportes de información etiquetaranse de forma que, sen revelar o seu contido, indíquese o nivel de seguridade da información contida de maior cualificación.

- Autorización de sistemas e solucións: Deberase autorizar os sistemas e solucións antes de entrar en operación. Controlarase e limitará os accesos aos sistemas de información. Configurarase e deseñará os sistemas de información de forma que se garanta a seguridade e protección de datos por defecto

- Seguridade ligada ás persoas: Implementaranse os mecanismos necesarios para que calquera persoa que, debidamente autorizada, acceda aos activos de información coñeza as súas responsabilidades e deste xeito redúzase o risco derivado dun uso indebido dos devanditos activos.

- Protección de datos de carácter persoal: Adoptaranse as medidas técnicas e organizativas que corresponda implementar para atender os riscos xerados polo tratamento de acordo ao esixido polo Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016.

- Rexistro de actividade: A actividade realizada polas persoas usuarias de sistemas de información deberá ser rexistrada o obxecto de verificar e auditar o bo uso da información, sempre con plenas garantías á intimidade e dignidade persoal, e consonte a normativa sobre protección de datos persoais, de función pública ou laboral, e demais disposicións que resulten de aplicación. A monitoraxe deberá realizarse motivando a súa necesidade e aplicando o principio de proporcionalidade, elixindo a medida menos invasiva. Para corrixir ou, no seu caso, esixir responsabilidades, cada usuario que acceda ao sistema de información deberá estar identificado de forma única, de modo que se saiba, en todo momento, quen recibe dereitos de acceso, de que tipo son estes, e quen realizou unha determinada actividade.

- Xestión de incidentes de seguridade: Os procedementos de xestión permitirán identificar, rexistrar e dar unha efectiva e pronta resposta aos incidentes de seguridade, comunicando os procedentes á Plataforma Nacional de Notificación e Seguimento de Ciberincidentes.

- Protección das comunicacións: A información que se transmita a través de redes de comunicacións deberá ser adecuadamente protexida, sen prexuízo das actuacións realizadas con fins de rexistro de actividade.

- Especificacións de seguridade: O desenvolvemento e mantemento dos sistemas de información irán acompañados das especificacións de seguridade e dos correspondentes procedementos de control.

- Adquisición de produtos de seguridade e contratación de servizos de seguridade: Optarase, de forma proporcionada á categoría do sistema e nivel de seguridade determinados, por aqueles que teñan certificada a funcionalidade de seguridade relacionada co obxecto da súa adquisición.

- Monitoraxe continua: desenvolveranse servizos horizontais de seguridade que aumenten a capacidade de vixilancia e detección de ameazas na operación diaria dos sistemas de información e comunicacións da Deputación integrados na Rede Nacional de Centros de Operacións de Ciberseguridad.

- Prevención ante outros sistemas de información interconectados: Protexerase o perímetro de sistemas de información, en particular, se se conecta a redes públicas e reforzaranse as tarefas de prevención, detección e resposta a incidentes de seguridade.

- Mínimo privilexio: os sistemas de información deben deseñarse e configurarse outorgando os mínimos privilexios necesarios e a funcionalidade imprescindible para que a organización alcance os seus obxectivos.

- Xestión da continuidade: implementaranse os mecanismos apropiados para asegurar a dispoñibilidade dos sistemas de información e manter a continuidade dos seus procesos de negocio, de acordo ás necesidades de nivel de servizo dos seus usuarios.

- Cumprimento: Adoptaranse as medidas técnicas, organizativas e procedementais necesarias para o cumprimento da normativa legal vixente en materia de seguridade da información.

- Avaliación de sistemas de intelixencia artificial: Os sistemas de información que incorporen capacidades de intelixencia artificial serán avaliados conforme o Regulamento (UE) 2024/1689, garantindo a identificación de riscos asociados e a implementación de medidas de mitigación antes da súa posta en produción.

- Asignación de responsabilidades segundo RACI: A Deputación adoptará a matriz RACI definida pola guía CCN-STIC 801 para clarificar funcións en cada actividade do ENS, garantindo a correcta segregación e ausencia de conflitos de interese.

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 Deputación 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 (ciberataques).
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, co 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 verse 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 goberno, 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 goberno

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.
Así mesmo, participará na determinación da categoría do sistema, colaborando na valoración do impacto asociado á información tratada. Valorará a análise de riscos relativo á información, podendo formular requisitos adicionais cando cumpra, e aceptará formalmente o risco residual que afecte á información baixo a súa responsabilidade, consonte o proceso de autorización para operar.
O Responsable da Información ten, de forma exclusiva, a potestade de modificar no tempo a valoración mencionada anteriormente, se así fose necesario, podendo solicitar un Plan de Mellora da Seguridade cando o risco residual non resulte aceptable.
Este rol poderá recaer nunha ou varias persoas, e mesmo nun órgano colexiado, podendo coincidir co Responsable do Servizo e coordinarase co Delegado de Protección de Datos cando a información tratada inclúa datos persoais.

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 e o impacto que unha interrupción poida ter na súa prestación.
Así mesmo, participará na determinación da categoría do sistema e na análise de riscos, identificando aqueles que afecten á continuidade, dispoñibilidade e calidade do servizo. No marco do proceso de autorización para operar establecido no ENS, aceptará formalmente o risco residual que afecte o servizo baixo a súa responsabilidade, podendo solicitar un Plan de Mellora da Seguridade cando este risco non sexa aceptable ou as medidas propostas resulten insuficientes.
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 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. A implantación de todas as actividades relativas á seguridade da información, de acordo ás directrices do Responsable de Seguridade da Información, corresponde ao Administrador 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 as análises de riscos de seguridade da información dos sistemas da Deputación, integrando, cando se traten datos persoais, as medidas derivadas das análises de riscos e das avaliacións de impacto en protección de datos, en coordinación co Delegado de Protección de Datos, e elevando as conclusións e o risco residual ao Comité de Seguridade da Información para a súa aprobación.
- Participar na elaboración e na proposta da Política de Seguridade da Información e os procedementos, normativas e instrucións en aplicación do ENS.
- 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, **determinando, en coordinación cos Responsables da Información e do Servizo, as medidas aplicables a cada sistema de información en función das análises de riscos e dos niveis de seguridade establecidos.**
- 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.
- Definir e propoñer indicadores de risco e indicadores de seguridade, analizar periodicamente a súa evolución e monitorizar que os sistemas se manteñen dentro das marxes de risco aceptados, informando das desviacións significativas ao Comité de Seguridade da Información, aos Responsables da Información e do Servizo e, cando cumpra, ao Titular da entidade.
- Analizar os incidentes de seguridade da información reflectidos nos rexistros destes e verificar que se estableceron os plans para a súa resolución.
- Analizar os riscos antes do despregamento dos sistemas de intelixencia artificial, atendendo as valoracións do Responsable da Información e do Servizo e, no seu caso, do Delegado de Protección de Datos e supervisar o seu despregamento.
- 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 e aprobar a Declaración de Aplicabilidade, atendendo os requirimentos do Responsable da Información e do Servizo.
- 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.

Administrador de Seguridade da Información

É responsable da posta en marcha da implementación, xestión e mantemento das medidas de seguridade que sexan de aplicación aos sistemas de información de acordo ás directrices do Responsable de Seguridade da Información.

As súas funcións son as seguintes:

- Monitorizar o estado da seguridade do sistema.

- Aplicar os procedementos operativos de seguridade da información aprobados e informar o Responsable de Seguridade da Información de calquera anomalía, compromiso ou vulnerabilidade relacionada coa seguridade.
- Elaborar procedementos operativos de seguridade da información e asegurar que a trazabilidade, pistas de auditoría e outros rexistros de seguridade requiridos atópense habilitados e rexístrense coa frecuencia desexada, consonte esta Política e normativa derivada.
- Colaborar na elaboración de catálogos de activos e servizos, análises de riscos, avaliacións de impacto, na relación de auditorías, accións de asesoramento e en calquera outra actividade relacionada coa Seguridade da Información en que sexa necesaria a súa participación.
- Coordinar o proceso de resposta ante incidentes de seguridade no sistema baixo a supervisión do Responsable de Seguridade da Información e o Responsable dos Sistemas de Información.
- Implementar, xestionar e manter as medidas de seguridade aplicables ao sistema.
- Xestionar a configuración e actualización do hardware e software nos que se basean os mecanismos e servizos de seguridade do sistema.

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 polo normativa xeneral 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.
- Ser informado da análise de riscos de seguridade da información, realizado conforme o Esquema Nacional de Seguridade, e aprobar o limiar do risco residual aceptable, así como o plan de xestión do risco proposto, tendo en conta os requisitos de seguridade establecidos para os diferentes activos por parte dos seus responsables correspondentes.
- 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 desaliñados coa Política de Seguridade
- Priorizar as actuacións en materia de seguridade cando os recursos sexan limitados.
- Velar por que a seguridade da información se teña 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 Secretario Xeral da Deputación.
- O Responsable de Seguridade da Información.
- A Administradora de Seguridade da Información.
- O Delegado de Protección de Datos.
- 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.

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 leven 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 goberno.

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

Responsable do Sistema

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.

- Participar no proceso de autorización para operar previa á entrada en produción do sistema, achegando información técnica sobre o estado do sistema, o grao de implantación das medidas de seguridade e os riscos técnicos existentes.

- Definir a topoloxía e a xestión do sistema de información, establecendo os criterios de uso e os servizos dispoñibles no mesmo.

- Participar na determinación da categoría do sistema, achegando a información técnica necesaria sobre arquitectura, dependencias, configuracións e operación do sistema.

- 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 se poidan 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.
- Participar en auditorías técnicas periódicas da infraestrutura de tecnoloxías da información, sistemas e aplicacións, e adoptar as medidas correctoras derivadas das súas conclusións.

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.

ROL	EXERCIDO POR
Responsable de Seguridade da Información	Titular da Xefatura do Servizo de Informática e Administración Electrónica.
Administrador de Seguridade da Información	Titular da Xefatura de Sección de Seguridade da Información.
Responsable de Seguridade Física	Titular da Xefatura do Servizo de Sistemas e Soporte.
Responsable do Sistema	Titular da Xefatura do Servizo de Sistemas e Soporte.
Presidente do Comité de Seguridade	Titular da Presidencia da Deputación.
Secretario do Comité de Seguridade	Secretario Xeral da Deputación.
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

En caso de producirse conflitos ou discrepancias entre os diferentes responsables que integran a estrutura organizativa da Política de Seguridade da Información, a cuestión elevarase ao Comité de Seguridade da Información (CSI) para a súa avaliación e resolución definitiva. O CSI actuará como órgano independente, garantindo a adecuada diferenciación de responsabilidades e a adopción de decisións obxectivas, aliñadas cos intereses da organización e cos principios de protección e salvagarda 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

A Deputación xestionará os riscos que afecten os seus sistemas de información, servizos e datos, mediante un proceso sistemático, continuo e documentado, aliñado co Esquema Nacional de Seguridade.
O proceso de xestión de riscos comprenderá as seguintes actividades:

1. Determinación da categoría do sistema

O Responsable de Seguridade, coa participación do Responsable da Información, do Responsable do Servizo e do Responsable do Sistema, determinará e documentará a categoría do sistema conforme o Anexo I do ENS.

A categoría será revisada cando se produzan cambios significativos que poidan afectar o nivel de seguridade requirido.

2. Selección de medidas de seguridade

O Responsable de Seguridade elaborará e aprobará a Declaración de Aplicabilidade (DoA), identificando:

- as medidas do Anexo II do ENS aplicables segundo a categoría do sistema,

- as medidas adicionais derivadas das análises de riscos, e

- as medidas compensatorias que se requiran, debidamente xustificadas.

A selección de medidas terá en conta os riscos derivados do tratamento de datos persoais e as recomendacións do Delegado de Protección de Datos.

3. Implementación de medidas de seguridade

O Responsable do Sistema implantará as medidas recollidas na Declaración de Aplicabilidade e nos plans de tratamento de riscos, baixo a supervisión do Responsable de Seguridade.

Os terceiros que presten servizos á Deputación deberán implantar e acreditar as medidas de seguridade aplicables, incluíndo as relativas a servizos na nube, conforme os requisitos do ENS e ao establecido nos contratos.

4. Avaliación da eficacia das medidas

Verificarase que as medidas implantadas son eficaces mediante revisións periódicas, controis de seguridade, auditorías internas ou externas e outras actividades definidas polo Responsable de Seguridade.

O Responsable de Seguridade consolidará os resultados destas verificacións e elevaraos ao Comité de Seguridade da Información para a súa valoración e seguimento.

5. Autorización para operar (ATO)

O proceso de xestión de riscos culmina coa autorización para operar do sistema, que se articula mediante a aceptación do risco residual por parte dos responsables competentes.

Para iso, seguirase o seguinte procedemento:

a) O Comité de Seguridade da Información será informado da análise de riscos e aprobará o limiar do risco residual e o plan de xestión do risco proposto.
b) O Responsable da Información aceptará o risco residual que afecte á información baixo a súa responsabilidade.
c) O Responsable do Servizo aceptará o risco residual que afecte á prestación do servizo baixo a súa responsabilidade.
d) Cando existan riscos que non sexan aceptables ou cuxo tratamento resulte insuficiente, establecerase un Plan de Mellora da Seguridade, debendo regresar ao proceso de selección e axuste de medidas para a súa revisión.

A autorización para operar queda formalmente outorgada cando os responsables aceptasen o risco residual conforme este proceso.

6. Revisión continua e actualización do risco

A xestión de riscos repetirase:

- periodicamente, polo menos unha vez ao ano,
- cando se produzan cambios significativos nos sistemas, servizos ou estruturas organizativas,
- cando se identifiquen novas ameazas ou vulnerabilidades relevantes, ou
- tras a ocorrencia de incidentes de seguridade significativos.

O Responsable de Seguridade monitorizará a evolución do risco mediante indicadores e métricas definidos, e informará periodicamente o Comité de Seguridade da Información.

7. Integración con protección de datos

Os riscos relacionados con datos persoais serán avaliados coordinadamente co Delegado de Protección de Datos, incluíndo:

- identificación conxunta de riscos,
- determinación de medidas adicionais, e
- realización de Avaliacións de Impacto cando cumpra.

Datos de carácter persoal

A Deputación 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 xeral: Miguel Iglesias Martínez (asinado dixitalmente)

O presidente: Valentín González Formoso (asinado dixitalmente)