POLÍTICA DE SEGURIDADE DA INFORMACIÓN E PROTECCIÓN DE DATOS PERSOAIS

Índice

1 Aprobación e Entrada en Vigor

Texto aprobado o día 27 de marzo de 2023 por Resolución de Presidencia, con modificación dun dos membros do Comité de Seguridade aprobada por Resolución da Presidencia de data 17 de outubro de 2023.

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

2 Introdución

A Deputación de Lugo (en adiante, "a Deputación") está sometida ó cumprimento do disposto no 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 derroga a Directiva 95/46/CE (en adiante, Regulamento Xeral de Protección de Datos ou RXPD) e á Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais (en adiante, LOPDGDD). Para a protección dos dereitos e liberdades das persoas físicas no que respecta ao tratamento dos datos persoais, é necesaria a adopción de medidas técnicas e organizativas. A Deputación, na súa condición de responsable do tratamento, debe adoptar políticas internas coa finalidade de garantir e poder demostrar que o tratamento dos datos se axusta á normativa vixente. A Deputación, firmemente comprometida coa garantía dos dereitos e liberdades dos seus empregados e da cidadanía en xeral, adopta esta política de seguridade e protección de datos, para unha maior seguridade xurídica e un mellor coñecemento da mesma.

A Deputación de Lugo depende dos sistemas TIC (Tecnoloxías de Información e Comunicacións) para alcanzar os seus obxectivos. Estes sistemas deben ser administrados con dilixencia, tomando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados que poidan afectar á dispoñibilidade, integridade ou confidencialidade da información tratada ou os servizos prestados.

O obxectivo da seguridade da información é garantir a calidade da información e a prestación continuada dos servizos, actuando preventivamente, supervisando a actividade diaria e reaccionando con presteza aos incidentes.

O obxectivo da protección de datos é garantir a protección dos dereitos e liberdades dos cidadáns con pleno respecto á normativa vixente.

Os sistemas TIC deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na confidencialidade, integridade, dispoñibilidade, uso previsto e valor da información e os servizos. Para defenderse destas ameazas, requírese unha estratexia que se adapte aos cambios nas condicións da contorna para garantir a prestación continua dos servizos.

Os sistemas TIC deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na confidencialidade, integridade, dispoñibilidade, uso previsto e valor da información e os servizos. Para defenderse destas ameazas, requírese unha estratexia que se adapte aos cambios nas condicións da contorna para garantir a prestación continua dos servizos.

Isto implica que A Deputación de Lugo e todo o seu persoal debe aplicar as medidas mínimas de seguridade esixidas polo Esquema Nacional de Seguridade, así como realizar un seguimento continuo dos niveis de prestación de servizos, seguir e analizar as vulnerabilidades reportadas, e preparar unha resposta efectiva aos incidentes para garantir a continuidade dos servizos prestados.

Para todo isto, a Organización adaptará as medidas de seguridade establecidas no Esquema Nacional de Seguridade (Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade, en adiante "ENS") e na normativa UNE-EN-ISO/IEC 27001, de seguridade da información. Pola súa banda, de acordo co establecido na LOPDGDD na súa Disposición Adicional Primeira, a Deputación establece as medidas de seguridade previstas no ENS no tratamento de datos persoais.

Para a aplicación das medidas do ENS considerarase a categorización dos sistemas de información. Para a realización da citada categorización seguiranse os criterios xerais sinalados no Anexo I do ENS e no artigo 40.

A Deputación de Lugo debe asegurarse de que a seguridade TIC é unha parte integral de cada etapa do ciclo de vida do sistema, desde a súa concepción ata a súa retirada de servizo, pasando polas decisións de desenvolvemento ou adquisición e as actividades de explotación. Os requisitos de seguridade e as necesidades de financiamento, deben ser identificados e incluídos na planificación, na solicitude de ofertas, e en pregos de licitación para proxectos de TIC.

A entidade debe estar preparada para previr, detectar, reaccionar, recuperarse de incidentes e conservar a información, de acordo ao Artigo 8 do ENS.

Así mesmo, no que respecta ao tratamento de datos persoais, aplicarase a normativa vixente en materia de protección de datos.

Con todo isto, esta Política ten como obxectivo establecer as pautas globais de seguridade e protección de datos para a Organización, así como protexer os activos de información, garantindo que:

- É axeitada ao propósito da Deputación.
- Proporcionar un marco de referencia para o establecemento dos obxectivos de seguridade da información de protección de datos persoais.
- Inclúe o compromiso de cumprir os requisitos aplicables á seguridade da información e protección de datos persoais.
- Inclúe o compromiso de mellora continua do sistema de xestión da seguridade da información.
- Inclúe o compromiso de mellorar a xestión das obrigas establecidas pola normativa de protección de datos.

2.1 Prevención

A Deputación de Lugo debe evitar, ou polo menos previr na medida do posible, que a información ou os servizos véxanse prexudicados por incidentes de seguridade. Para iso implantará as medidas mínimas de seguridade determinadas polo ENS, así como calquera control adicional identificado a través dunha avaliación de ameazas e riscos.

Estes controis, e os roles e responsabilidades de seguridade de todo o persoal, van estar claramente definidos e documentados.

Para garantir o cumprimento da política, a Deputación de Lugo debe:

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

2.2 Detección

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

A supervisión é especialmente relevante cando se establecen liñas de defensa de acordo co Artigo 9 do ENS. Estableceranse mecanismos de detección, análise e reporte que cheguen aos responsables regularmente e cando se produce unha desviación significativa dos parámetros preestablecidos como normais.

2.3 Resposta

A Deputación de Lugo:

- Establece mecanismos para responder eficazmente os incidentes de seguridade.
- Designa un punto de contacto para as comunicacións con respecto a incidentes detectados noutros departamentos ou noutros organismos.
- Establece protocolos para o intercambio de información relacionada co incidente. Isto inclúe comunicacións, en ambos os sentidos, cos Equipos de Resposta a Emerxencias (CERT).

2.4 Recuperación e conservación

Para garantir a dispoñibilidade dos servizos críticos, os departamentos da Deputación de Lugo deben desenvolver plans de continuidade dos sistemas TIC como parte do seu plan xeral de continuidade do servizo e actividades de recuperación para garantir a conservación dos datos e información en soporte electrónico.

3 Alcance

Esta política de seguridade é de aplicación e de obrigado cumprimento para todos os membros que, de forma permanente ou eventual, presten servizos á Deputación de Lugo, especialmente aos responsables dos Servizos de Explotación dos Sistemas de Información e aos propios usuarios, como actores ambos, incluíndo, se é o caso, o persoal de provedores externos, cando proceda e sexan usuarios dos sistemas de información.

No ámbito desta Política, enténdese por usuario todo empregado/empregada público pertencente ou alleo á Deputación de Lugo, así como persoal de organizacións privadas externas, entidades colaboradoras ou calquera outro tipo de relación coa Deputación e que utiliza ou ten acceso aos seus sistemas de información.

Os requisitos de seguridade e as necesidades de financiamento deberán identificarse e incluírse na planificación, na solicitude de ofertas e nos pregos de proxectos TIC.

4 Misión

A Deputación de Lugo constitúese como organismo democrático no ano 1979, dentro do proceso de Transición, cuxa estrutura e regulación son similares aos de hoxe en día.

A Deputación ten unha importante misión de organización do conxunto das administracións. Trátase dun organismo territorial operativo, eficaz para coñecer a realidade municipal de maneira inmediata, para comprender as relacións entre os municipios e para brindar solucións contra os desequilibrios existentes entre eles, próximos ou distantes, pero coa capacidade de complementarse.

O seu carácter de organismo intermedio outórgalle un papel moi importante como colaborador necesario das pequenas administracións municipais, coordinador de recursos e servizos compartidos, mediador entre os intereses opostos ou locais e a execución de reclamos comúns ou específicos ante outros organismos superiores, entre moitas outras facetas.

Coa elaboración do presente documento preténdese establecer as pautas que garantan a Dispoñibilidade, Integridade, Confidencialidade, Autenticidade e Trazabilidade da información na Deputación a un nivel axeitado segundo o risco dos activos, as necesidades e os recursos.

5 Marco normativo

O marco normativo en materia de seguridade da información no que a Deputación de Lugo desenvolve a súa actividade, esencialmente, é o seguinte:

- Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade.
- Lei 39/2015, do 1 de outubro, do Procedemento Administrativo Común das Administracións Públicas.
- Lei 40/2015, do 1 de outubro, de Réxime Xurídico do Sector Público.
- 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 derroga a Directiva 95/46/CE.
- Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e Garantía dos Dereitos Dixitais.
- Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de

Interoperabilidade no ámbito da Administración electrónica.

- Lei 34/2002, do 11 de xullo, de Servizos da Sociedade da Información e de comercio electrónico.
- Real Decreto Lexislativo 5/2015, do 30 de outubro, polo que se aproba o texto refundido da Lei do Estatuto Básico do Empregado Público.
- Real Decreto Lexislativo 1/1996, do 12 de abril, polo que se aproba o Texto Refundido da Lei de Propiedade Intelectual.
- Lei 2/2019, do 1 de marzo, pola que se modifica o texto refundido da Lei de Propiedade Intelectual.
- Real Decreto-lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información.
- Real Decreto 43/2021, do 26 de xaneiro, de Seguridade das Redes e Sistemas de Información.
- Lei 6/2020, do 11 de novembro, de regulación de determinados aspectos dos servizos electrónicos de confianza.

6 Organización da Seguridade

A implantación da Política de Seguridade na Deputación de Lugo require que todos os membros da organización entendan as súas obrigacións e responsabilidades en función do posto desempeñado. Como parte da Política de Seguridade da Información, cada rol especifico, personalizado en usuarios concretos, debe entender as implicacións das súas accións e as responsabilidades que ten atribuídas, quedando identificadas e detalladas nesta sección, e que se agrupan do modo seguinte:

a) Comité de Seguridade da Información

b) Responsable do Servizo

c) Responsable da Información

d) Responsable de Seguridade da Información

e) Responsable de Sistemas

Na definición de funcións, a función de Responsable da Información e do Responsable de Servizos poden coincidir na mesma persoa. Adicionalmente, na definición de funcións terase en conta segundo o ENS que o Responsable de Seguridade e o Responsable do Sistema non teñen unha dependencia xerárquica.

Nos seguintes apartados especifícanse as funcións atribuídas a cada un destes roles.

6.1 Comité de seguridade da información

O Comité de Seguridade da Información coordina a seguridade da información na Deputación

de Lugo.

O Comité de Seguridade da Información estará formado polos seguintes membros en función das súas funcións actuais:

a) Presidente: Responsable da Información e do Servizo ou persoa en quen delegue.

b) Secretaría: Responsable de Seguridade da Información.

c) Vogais:

   a. Responsables das unidades organizativas serán convocados polo presidente en función das cuestións a tratar (se afectan á súa área).

   b. DPD (pode ser membro sen dereito a voto)

O Comité de Seguridade deberá reunirse con carácter ordinario polo menos unha vez ao ano e con carácter extraordinario por razóns de urxencia e causa xustificada ou cando así o decida a súa Presidencia.

O resto de persoas con responsabilidades nas funcións do ENS ou do RXPD serán convocadas, segundo as necesidades do Comité de Seguridade da Información.

O Comité de Seguridade da Información reportará á Presidencia da Deputación de Lugo e terá as seguintes funcións:

- Atender as inquedanzas da Presidencia e dos diferentes departamentos.
- Informar regularmente o estado da seguridade da información á Presidencia.
- Promover a mellora continua do sistema de xestión da seguridade da información.
- Elaborar a estratexia de evolución da Deputación de Lugo no que respecta a seguridade da información.
- Coordinar os esforzos das diferentes áreas en materia de seguridade da información, para asegurar que os esforzos son consistentes, aliñados coa estratexia decidida na materia, e evitar duplicidades.
- Elaborar (e revisar regularmente) a Política de Seguridade da información para que sexa aprobada pola Presidencia.
- Aprobar a normativa de seguridade da información.
- Elaborar e aprobar os requisitos de formación e cualificación de administradores, operadores e usuarios desde o punto de vista de seguridade da información.
- Realizar un seguimento dos principais riscos residuais asumidos pola Deputación de Lugo e recomendar posibles actuacións respecto de eles.
- Supervisar o desempeño dos procesos de xestión de incidentes de seguridade e recomendar posibles actuacións respecto de eles. En particular, velar pola coordinación das diferentes áreas de seguridade na xestión de incidentes de seguridade da información.

- Promover a realización das auditorías periódicas que permitan verificar o cumprimento das obrigacións do organismo en materia de seguridade.

- Aprobar plans de mellora da seguridade da información da Deputación de Lugo. En particular velará pola coordinación de diferentes plans que poidan realizarse en diferentes áreas.

- Priorizar as actuacións en materia de seguridade cando os recursos sexan limitados.

- Garantir que se teña en conta a seguridade da información en todos os proxectos TIC dende a súa especificación inicial ata a súa posta en macha. En particular deberá garantir a creación e utilización de servizos horizontais que reduzan duplicidades e apoien un funcionamento homoxéneo de todos os sistemas TIC.

- Resolver os conflitos de responsabilidade que poidan aparecer entre os diferentes responsables, elevando aqueles casos nos que non teña suficiente autoridade para decidir.

- Impulsar o cumprimento e difusión da Política de Seguridade da Información e Protección de Datos, promovendo as actividades de sensibilización en materia de seguridade para o persoal da Deputación.

- Recompilará regularmente do persoal técnico propio ou externo a información pertinente para a toma de decisións.

- Será asesorado sobre as cuestións que teña que decidir ou emitir unha opinión. Este consello determinarase en cada caso, podendo materializarse de diferentes xeitos e modos:

    - Grupos de traballo especializados internos, externos ou mixtos.

    - Asesoramento interno e/ou externo.

    - Asistencia a cursos ou outro tipo de contornos formativos ou de intercambio de experiencias.

No caso de incidentes de seguridade da información:

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

O Secretario do Comité de Seguridade da Información será o Responsable de Seguridade e terá como funcións:

- Convocar as reunións do Comité de Seguridade da Información.

- Prepara os temas para tratar nas reunións do Comité, achegando información puntual para a toma de decisións.

- Elabora a acta das reunións.

- É responsable da execución directa ou delegada das decisións do Comité.

6.2 Responsable da Información

Serán persoas cun alto cargo na dirección da organización e pertencentes ao Comité directivo da mesma.

As funcións do Responsable da Información son as seguintes:

- Ten a potestade de establecer os requisitos, en materia de seguridade, da información xestionada. Se esta información inclúe datos de carácter persoal, ademais deberán terse en conta os requisitos derivados da lexislación correspondente sobre protección de datos.
- Ten a responsabilidade última do uso que se faga de determinada información e, por tanto, da súa protección.
- O Responsable da Información é o responsable último de calquera erro ou neglixencia que leve a un incidente de confidencialidade ou de integridade.
- Determina os niveis de seguridade da información en cada dimensión dentro do marco establecido no Anexo I do Esquema Nacional de Seguridade.
- Aínda que a aprobación formal dos niveis corresponda ao Responsable da Información, poderá solicitar unha proposta ao Responsable de Seguridade e convén que escoite a opinión do Responsable do Sistema.

6.2.1 Compatibilidade con outras funcións

Este rol pode coincidir co Responsable do Servizo.

Este rol non poderá coincidir co de Responsable de Seguridade da Información, salvo en pequenas organizacións que funcionen de forma autónoma.

Este rol non pode coincidir co de Responsable do Sistema, nin sequera no caso de pequenas organizacións de reducidas dimensións que funcionen de forma autónoma.

6.3 Responsable do Servizo

O Responsable do servizo pode acordar a suspensión do tratamento de determinada información ou a prestación dun determinado servizo, se é informado de graves deficiencias de seguridade que poidan afectar ao cumprimento dos requisitos establecidos. Esta decisión deberá ser acordada cos Responsables da Información, Responsable de Seguridade da Información e Responsable do Sistema, antes de ser executada.

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

A persoa ou órgano que o asuma deberá identificarse para cada servizo que preste a organización.

Son funcións do Responsable do Servizo:

- No relativo ao RXPD, por delegación do Responsable do Tratamento, encárgase ao Responsable do Servizo o desenvolvemento das tarefas relacionadas coa xestión dos tratamentos dos datos persoais realizados no seu ámbito específico.

- Ten a facultade de establecer os requisitos, en materia de seguridade, dos servizos prestados.

- Ten a responsabilidade última do uso que se faga de determinados servizos e, polo tanto, da súa protección.

- O Responsable do Servizo é o responsable último de calquera erro ou neglixencia que leve a un incidente de dispoñibilidade dos servizos.

- Determinará a dispoñibilidade do servizo dentro do marco establecido no Anexo I do Esquema Nacional de Seguridade.

- Aínda que a aprobación formal dos niveles corresponda ao Responsable do Servizo, poderá solicitar unha proposta ao Responsable de Seguridade e convén que escoite a opinión do Responsable do Sistema.

6.3.1 Compatibilidade con outras funcións

As funcións de Responsable da Información e Responsable do Servizo poderán coincidir nunha mesma persoa ou organismo, aínda que, en xeral, non coincidirán cando:

- O servizo xestione información de distintas fontes, non necesariamente do mesmo departamento que presta o servizo.

- A prestación do servizo non dependa da unidade á que pertence o Responsable da Información.

- Este rol non poderá coincidir co de Responsable de Seguridade, salvo en organizacións de reducida dimensión que funcionen de forma autónoma.

6.4 Responsable de Seguridade

Responsable da definición, coordinación e verificación de cumprimento dos requisitos de seguridade da información definidos de acordo aos obxectivos estratéxicos.

As funcións do Responsable de Seguridade da Información son as seguintes:

- Convocar e dirixir as reunións do Comité de Seguridade, informando, propoñendo e coordinando as súas actividades e decisións. Actuará como Secretario do Comité de Seguridade da Información.

- Coordinará e controlará as medidas definidas no Rexistro de actividades de tratamento e, en xeral, encargarase do cumprimento das medidas de seguridade que se detallan no informe de avaliación de impacto da protección de datos da Deputación.

- Recompilará os requisitos de seguridade do Responsable de Información e Servizo e determinará a categoría do Sistema.

- Promoveras actividades de sensibilización e formación en materia de seguridade da información no seu ámbito de responsabilidade.

- Participará na elaboración, no marco do Comité de Seguridade da Información, da Política de Seguridade da Información e Protección de Datos, para a súa aprobación

pola Dirección.

- Participará na elaboración e aprobación, no marco do Comité de Seguridade da Información, da normativa de Seguridade da Información.
- Elaborará os Plans de Formación e Sensibilización do persoal en Seguridade da Información, que deberán ser aprobados polo Comité de Seguridade da Información.
- Validará os Plans de Continuidade de Sistemas elaborados polo Responsable do Sistema, que deberán ser aprobados polo Comité de Seguridade da Información e probados periodicamente polo Responsable do Sistema.
- Supervisar a implantación, manter, controlar e verificar o cumprimento de:
    - A estratexia de seguridade da información definida polo Comité de Seguridade.
    - As normas e procedementos contidos na Política de Seguridade da Información da Deputación de Lugo e normativa de desenvolvemento.
- Supervisar os incidentes de seguridade producidos na Deputación de Lugo.
- Difundir na Deputación de Lugo as normas e procedementos contidos na Política de Seguridade da Información e Protección de Datos e normativa de desenvolvemento, así como as funcións e obrigacións en materia de seguridade da información.
- Supervisar e colaborar nas auditorías internas ou externas necesarias para verificar o grao de cumprimento da Política de Seguridade e Protección de Datos, normativa de desenvolvemento e leis aplicables en materia de protección de datos persoais e de seguridade da información.
- Asesorar en materia de seguridade da información ás diferentes áreas operativas da Deputación de Lugo.
- Realizar, coa colaboración do Responsable do Sistema, a Análise de Riscos.
- Elaborar unha Declaración de Aplicabilidade a partir das medidas de seguridade esixidas conforme ao Anexo II do ENS e do resultado da Análise de Riscos.
- Facilitar ao Responsable da Información e do Servizo información sobre o nivel de risco residual previsto despois de implantar as opcións de tratamento seleccionadas na análise de riscos e as medidas de seguridade requiridas polo ENS.

6.4.1 Compatibilidade con outras funcións

Este rol só poderá coincidir co de Responsable da Información e Responsable do Servizo en organizacións de reducidas dimensións que teñan unha estrutura operativa autónoma.

Este ron non poderá coincidir co de Responsable do Sistema, aínda que sexan pequenas organizacións que teñan unha estrutura operativa autónoma.

6.4.2 Delegación de funcións

Para determinados Sistemas de Información que, pola súa complexidade, distribución, separación física dos seus elementos e número de usuarios necesiten de persoal adicional

para o desempeño das funcións de Responsable de Seguridade da Información, poderán designarse Responsables de Seguridade da Información Delegados se se considera necesario.

A designación corresponde ao Responsable de Seguridade da Información. Mediante o nomeamento de delegados, deléganse as funcións. A responsabilidade final seguirá recaendo sobre o Responsable de Seguridade da Información.

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

Cada Responsable de Seguridade da Información Delegado terá unha dependencia funcional directa do Responsable de Seguridade da Información, que é a persoa a quen reportan.

6.5 Responsable do Sistema

É responsable de asegurar a execución de medidas para asegurar os activos e servizos dos sistemas de información, que soportan a actividade da Deputación de Lugo, de acordo aos obxectivos da organización.

As funcións do Responsable de Sistemas da Información son as seguintes:

- Desenvolver, operar e manter o Sistema de Información durante todo o seu ciclo de vida, das súas especificacións, instalación e verificación do seu correcto funcionamento.
- Elaborar os procedementos operativos necesarios e realizar exercicios e probas sobre os mesmos.
- Elaborar Plans de Continuidade do Sistema para que sexan validados polo Responsable de Seguridade da Información, e coordinados e aprobados polo Comité de Seguridade da Información.
- Realizar exercicios e probas periódicas dos Plans de Continuidade do Sistema para mantelos actualizados e verificar a súa efectividade.
- Definir a topoloxía e sistema de xestión do Sistema de Información establecendo os criterios de uso e os servizos dispoñibles no mesmo.
- Asegurarse de que as medidas específicas de seguridade intégrense adecuadamente dentro do marco xeral de seguridade.
- Seleccionar e establecer as funcións e obrigacións aos Responsables Técnicos Informáticos encargados de personificar unha xestión da seguridade dos activos da Deputación de Lugo, conforme á estratexia de seguridade definida.
- Garantir que a implantación de novos sistemas e dos cambios nos existentes cumpre cos requirimentos de seguridade establecidos na Deputación de Lugo.
- Establecer e supervisar os procesos e controis de monitoraxe do estado da seguridade que permitan detectar as incidencias producidas e coordinar a súa investigación e resolución.
- O Responsable do Sistema pode acordar a suspensión do manexo dunha certa

información ou a prestación dun certo servizo se é informado de deficiencias graves de seguridade que puidesen afectar á satisfacción dos requisitos establecidos. Esta decisión debe ser acordada cos responsables da información afectada, do servizo afectado e o Responsable da Seguridade, antes de ser executada.

- Realizar, coa colaboración do Responsable de Seguridade, a perceptiva análise de riscos, de seleccionar as salvagardas a implantar e de revisar o proceso de xestión de riscos.

6.5.1 Compatibilidade con outras funcións

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

6.6 Xerarquía no proceso de decisións e mecanismos de coordinación

As distintas funcións de seguridade da información (autoridade principal e posibles delegadas) limítanse a unha xerarquía sinxela: o Comité de Seguridade da Información da instrucións ao Responsable de Seguridade da Información que se encarga de cumprir, supervisando que os administradores e operadores implantan as medidas de seguridade segundo o establecido na Política de Seguridade e Protección de Datos aprobada pola Deputación.

O Administrador da Seguridade do Sistema reporta ao Responsable do Sistema:

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

O Responsable do Sistema informa ao Responsable da Información das incidencias funcionais relacionadas coa información que lle incumbe.

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

O Responsable do Sistema reporta ao Responsable da Seguridade:

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

O Responsable de Seguridade informa ao Responsable da Información das decisións e incidentes de seguridade que afecten á información da que é responsable, en particular da estimación do risco residual e das desviacións de risco significativas en relación aos marxes aprobados.

O Responsable de Seguridade informa ao Responsable do Servizo das decisións e incidentes de seguridade que afecten ao servizo do que é responsable, en particular da estimación de risco residual e das desviacións significativas de risco respecto dos marxes aprobados.

Cando existe un Comité de Seguridade da Información, o Responsable de Seguridade reporta

ao comité como secretario:

- Resumo consolidado das actuacións de seguridade.
- Resumo consolidado dos incidentes de seguridade da información.
- Estado da seguridade do sistema, en particular do risco residual ao que está exposto o sistema.

O Responsable de Seguridade informa á Dirección da Deputación, segundo o acordado no Comité de Seguridade da Información.

Cano non existe un Comité de Seguridade da Información, o Responsable de Seguridade reporta directamente á Dirección da Deputación.

- Resumo consolidado das actuacións de seguridade.
- Resumo consolidado dos incidentes de seguridade da información.
- Estado da seguridade do sistema, en particular do risco residual ao que está exposto o sistema.

6.7 Procedemento de designación de persoas

O nomeamento e designación dos seguintes cargos estará aprobado pola Presidencia da Deputación:

- Responsable da Información; pode ser un posto unipersoal ou un órgano colexiado (normalmente, o Comité de Seguridade da Información)
- Responsable do Servizo; pode ser o mesmo que o Responsable da Información, pode ser un posto unipersoal ou un órgano colexiado.
    - Responsable da Información e Responsable do Servizo: Presidente da Deputación de Lugo.
- Responsable de seguridade, que debe reportar directamente á Dirección ou, cando exista, ao Comité de Seguridade da Información.
    - Enxeñeiro Técnico de Telecomunicación do Servizo de Comunicación e Tics (Sección de Novas Tecnoloxías).
- Responsable do Sistema, que debe reportar directamente á Dirección ou, cando exista, ao Comité de Seguridade da Información.
    - O Adxunto á Xefa do Servizo de Comunicación e Tics (Sección de Novas Tecnoloxías).

A Dirección da Organización designa á persoa Responsable do Sistema:

- Por proposta do Responsable da Información tratada, cando o sistema de información trate unha única información.
- A proposta do Responsable do Servizo prestado, cando o sistema de información preste

un único servizo.

- Directamente cando o sistema de información trata diferentes informacións ou presta diferentes servizos, oídos dos responsables das informacións e os servizos afectados.

A Dirección da Deputación designa ao Administrador de Seguridade do Sistema a proposta do Responsable do Sistema ou do Responsable de Seguridade da Información.

Os nomeamentos revisaranse cada 2 anos ou cando algún dos postos quede vacante.

O Responsable de Seguridade da Información será designado por resolución de Presidencia a proposta do Comité de Seguridade da Información.

7 Organización de Protección de Datos

Para a prestación dos servizos previstos deben tratarse datos persoais. No Rexistro de Actividades de Tratamento detállanse os tratamentos afectados e os responsables correspondentes, así como as medidas adoptadas derivadas das avaliacións de impacto realizadas sobre os tratamentos. Todos os sistemas de información cumprirán cos niveis de seguridade requiridos pola normativa pola natureza e finalidade dos datos persoais recollidos no citado Rexistro de Actividades de Tratamento.

O Rexistro de Actividades de Tratamento da Deputación de Lugo atópase publicado no portal web corporativo, que se pode consultar na seguinte ligazón:

https://www.deputacionlugo.gal/rexistro_actividades_tratamento

De conformidade co disposto nos artigos 37 e seguintes do Regulamento Xeral de Protección de Datos e nos artigos 34 e seguintes da LOPDGDD, a Deputación de Lugo conta cun Delegado de Protección de Datos. A continuación, establécense as funcións e responsabilidades nesta materia.

7.1 Delegado de Protección de Datos

As funcións encomendadas ao Delegado de Protección de Datos son:

- Informar e asesorar ao responsable ou ao encargado do tratamento e aos empregados que se ocupen do tratamento das obrigacións que lles incumben en virtude do RGPD e doutras disposicións de protección de datos da Unión ou dos Estados membros (LOPDGDD).

- Supervisar o cumprimento do disposto no RGPD e na LOPDGDD, doutras disposicións de protección de datos da Unión ou dos Estados membros e das políticas do responsable ou do encargado do tratamento en materia de protección de datos persoais, incluída a asignación de responsabilidades, a concienciación e formación do persoal que participa nas operacións de tratamento, e as auditorías correspondentes.

- Ofrecer o asesoramento que se lle solicite acerca da avaliación de impacto relativa á protección de datos e supervisar a súa aplicación.

- Cooperar coa autoridade de control.

- Actuar como punto de contacto da autoridade de control para cuestións relativas ao tratamento, e realizar consultas, no seu caso, sobre calquera outro asunto.

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

    - Reunir información para determinar as actividades de tratamento.

    - Analizar e verificar a conformidade das actividades de tratamento.

    - Informar, asesorar e emitir recomendacións ao responsable ou encargado do tratamento.

    - Recoller información para supervisar o rexistro das operacións de tratamento.

    - Asesorar na aplicación do principio de protección de datos dende o deseño e por defecto.

    - Asesorar sobre:

        - Realizar ou non unha avaliación de impacto da protección de datos.

        - Se a avaliación do impacto da protección de datos debe realizarse con recursos propios ou con contratación externa.

        - Que salvagardas (incluídas medidas técnicas e organizativas) aplicar para mitigar calquera risco para os dereitos dos intereses dos afectados.

        - Se a avaliación do impacto da protección de datos se realizou ou non correctamente.

        - Se as súas conclusións (se procede ou non coa tramitación e que garantías aplicar) son conformes ao Regulamento.

    - Priorizar as súas actividades e centrar os seus esforzos naquelas cuestións que presentan os maiores riscos relacionados coa protección de datos.

    - Informar ao responsable do tratamento sobre:

        - Que metodoloxía se debe seguir á hora de realizar unha avaliación de impacto da protección de datos.

        - Que áreas deben ser obxecto de auditoría de protección de datos interna ou externa.

        - Que actividades de formación interna impartir ao persoal ou aos directores responsables das actividades de tratamento de datos e a que operacións de tratamento dedicar máis tempo e recursos.

O delegado de protección de datos é formalmente designado e comunicado á Axencia Española de Protección de Datos.

7.2 Responsable de xestión de protección de datos

As funcións encomendadas ao Responsable de Xestión son:

- Executar as directrices que poida emitir a Dirección ou o Delegado de Protección de Datos.
- Actuar como punto de contacto entre o Delegado de Protección de Datos e os diferentes interesados e organismos da Deputación.
- Atender aos exercicios de dereito e á caixa de correo de protección de datos.
- Actuar como punto de contacto con auditores externos, entidades de formación, etc.
- Establecer os controis e medidas que se programen.
- Actualización do rexistro de actividades de tratamento e análise de riscos.

7.3 Comité de Protección de Datos

Existe un Comité de Protección de Datos que estará integrado polos seguintes membros:

PRESIDENTE: Responsable de Xestión de Protección de datos.

SECRETARIO: o Enxeñeiro Técnico de Telecomunicacións do Servizo de Comunicación e TICs (Sección de Novas Tecnoloxías).

VOGAIS: Delegado de Protección de Datos.

Poderán asistir, por petición do Comité, aqueles outros responsables cuxa intervención sexa necesaria por estar afectados pola normativa vixente. O Comité reunirase a proposta dun dos seus membros, e polo menos unha vez ao ano.

Son funcións do Comité de Protección de Datos as seguintes:

- Atender as inquedanzas da Alta Dirección e dos diferentes departamentos.
- Informar regularmente as obrigas de protección de datos á Alta Dirección.
- Promover a mellora continua no cumprimento das obrigas de protección de datos.
- Coordinar as actuacións programadas para o cumprimento das obrigas de protección de datos.
- Elaborar (e revisar periodicamente) a Política de Seguridade da Información e Protección de Datos, en materia de protección de datos, para que sexa aprobada pola Presidencia.
- Aprobar os procedementos e a normativa interna de protección de datos.
- Aprobar o Rexistro de Actividades de Tratamento, avaliacións de impacto e análise de riscos.
- Preparar e aprobar os requisitos de formación e concienciación en materia de protección de datos.

- Monitorar os principais riscos en materia de protección de datos.
- Promover auditorías periódicas para verificar o cumprimento das obrigas de seguridade da organización.
- Resolver os conflitos de responsabilidade que poidan xurdir entre os distintos responsables e/ou entre as distintas áreas da Organización, elevando aqueles supostos nos que esta non teña autoridade suficiente para decidir.
- Recompilará regularmente do persoal técnico propio ou externo a información pertinente para tomar decisións.
- Será asesorado sobre as cuestións que teña que decidir ou emitir unha opinión. Este consello determinarase en cada caso, podendo materializarse de diferentes xeitos e modos:
    - Grupos de traballo especializados internos, externos ou mixtos.
    - Asesoramento interno e/ou externo.
    - Asistencia a cursos ou outro tipo de contornos formativos ou de intercambio de experiencias.

7.4 Procedementos de designación de persoas

O nomeamento e a designación das seguintes funcións serán aprobados pola Presidencia da Deputación:

- Ao Delegado de Protección de Datos; pode ser un cargo unipersoal ou un órgano colexiado. O DPD deberá reunir coñecementos especializados do Dereito e a práctica de protección de datos. En consecuencia, identificáronse os coñecementos, habilidades ou destrezas necesarias que deba coñecer ou posuír o Delegado de Protección de Datos para levar a cabo unha das funcións propias do seu posto.
    - Xefe da Sección de Innovación e Participación Cidadá.
- E os Responsables de Xestión de Protección de Datos, que deberán reportar directamente á Dirección ou ao Comité de Protección de Datos.

7.5 Funcións e obrigas dos usuarios con acceso a datos

Todos os empregados da entidade están suxeitos a funcións e obrigas. Todo o persoal da empresa que teña acceso aos datos persoais debe cumprir coas seguintes obrigas:

- Non está permitida a difusión de datos persoais ou confidenciais pertencentes á entidade, estando obrigado a gardar en segredo a información aínda despois de finalizada a relación laboral.
- O usuario será o responsable de comunicar calquera incidente de seguridade segundo o procedemento de incidentes; a non notificación dun incidente de seguridade considerarase unha omisión do deber do traballador.
- O usuario será o responsable de todos os accesos que se realicen baixo o seu

identificador e contrasinal e, polo tanto, non deberá revelar o contrasinal.

- O usuario será responsable sempre que abandone o posto de traballo de pechar a súa sesión ou bloquear o equipo con contrasinal.
- Non se poderán instalar aplicacións nos sistemas da entidade sen o consentemento do Responsable de Seguridade da Información.
- Non se permite a copia de datos persoais en soportes, sen a autorización expresa do delegado de protección de datos.
- O usuario será o responsable de conservar copias de todos os correos electrónicos que inclúan anexos con datos persoais vinculados á entidade.

8 Revisión da Política de Seguridade da Información

Será misión do Comité de Seguridade a revisión anual desta Política de Seguridade da Información e a proposta de modificación ou mantemento da mesma. A Política será aprobada por resolución da Presidencia da Deputación e difundida para que a coñezan todas as partes afectadas.

Xestión de Riscos

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

- regularmente, polo menos unha vez ao ano.
- cando cambie a información manexada
- cando cambien os servizos prestados
- cando ocorra un incidente grave de seguridade.
- cando se reporten vulnerabilidades graves

A xestión de riscos debe realizarse de forma continuada nos sistemas de información, de acordo cos principios de xestión da seguridade baseada no risco e reavaliación periódica

O Responsable de Seguridade da Información, xunto co Responsable de Sistemas, son os encargados de realizar a preceptiva análise de riscos, e de seleccionar as salvagardas a implantar.

O Responsable da Información e do Servizo é o responsable dos riscos sobre a información e o servizo, e polo tano, de aceptar os riscos residuais calculados na análise de riscos, e do seu seguimento e control sen prexuízo da posibilidade de delegar esta tarefa.

Para a harmonización das análises de riscos, o Comité de Seguridade establecerá unha valoración de referencia para os diferentes tipos de información manexados e os diferentes servizos prestados. O Comité de Seguridade dinamizará a dispoñibilidade de recursos para atender ás necesidades de seguridade dos diferentes sistemas, promovendo investimentos de

carácter horizontal.

O proceso de xestión de riscos, que inclúe as fases de categorización dos sistemas, análise de riscos e selección das medidas de seguridade a aplicar, que deberán ser proporcionais aos riscos e estar xustificadas, deberá revisarse cada ano por parte do Responsable de Seguridade da Información e coa colaboración do Responsable do Sistema, que elevarán un informe ao Comité de Seguridade da Información.

A xestión de riscos quedará documentada no Informe de Análise e Xestión de Riscos.

9 Documentación do Sistema de Xestión

A Política de Seguridade da Información e de Protección de Datos completarase con documentos máis precisos que axuden a levar a cabo o que se propón.

Esta Política desenvolverase mediante unha normativa de seguridade que aborde aspectos concretos. Esta normativa de seguridade estará a disposición de todos os membros da organización que necesiten coñecela, especialmente para aqueles que utilicen, operen ou xestionen os sistemas de información e de comunicación.

A normativa de seguridade estará dispoñible na intranet do organismo.

A documentación normativa sobre seguridade da información e protección de datos será obrigatorio e desenvolverase en catro niveis segundo o ámbito de aplicación e nivel de detalle técnico, de xeito que cada norma de un determinado nivel de desenvolvemento fundaméntase nas normas do nivel superior. Estes niveis de desenvolvemento normativo son os seguintes:

- Primeiro nivel normativo: Política de Seguridade da Información e Protección de Datos da Deputación de Lugo. Documento obrigatorio para todo o persoal, interno e externo, da Deputación Provincial de Lugo, recollido neste documento e aprobado por resolución da Presidencia da Deputación.

- Segundo nivel normativo: Políticas Específicas de Seguridade da Información e Estándares de Seguridade TIC (Normas STIC) que desenvolven o PSI con maior detalle dentro dun ámbito determinado. As Normas dan resposta, sen entrar en detalles de implantación nin tecnolóxicos, ao que se pode e non se pode facer en relación a unha determinada cuestión dende o punto de vista da seguridade: o que se considera un uso axeitado ou inadecuado, as consecuencias derivadas do incumprimento, entre outros aspectos.

  Tamén pertencen a este nivel a documentación de Procedementos Xerais do Sistema de Xestión de Seguridade da Información que establecen a forma na que a Deputación establece, implanta, mantén e mellora de maneira continua o Sistema de Xestión. Os documentos relacionados con este segundo nivel normativo serán aprobados polo Comité de Seguridade da Información por proposta do Responsable de Seguridade da Información.

- Terceiro nivel normativo: Procedementos Operativos STIC e Instrucións técnicas STIC. Son documentos que responden, incluíndo detalles de implantación e tecnolóxicos, a como se pode levar a cabo unha determinada tarefa respectando os principios de seguridade da organización, e os procesos internos establecidos nela. Os Procedementos STIC e as Instrucións Técnicas STIC serán aprobados polo Responsable de Seguridade da Información e coa participación na súa elaboración do Responsable do Sistema.

- Cuarto Nivel: Informes, rexistros e evidencias electrónicas. Documentos de carácter técnico que se poidan apoiar en formatos normalizados que inclúan os resultados e conclusións dun estudo, actividade ou avaliación; documentos técnicos que inclúan ameazas e vulnerabilidades nos sistemas de información, así como evidencias electrónicas xeradas durante todas as fases do ciclo de vida do sistema de información. A responsabilidade da existencia deste tipo de documentos é do Responsable do Sistema.

O Responsable de Seguridade da Información e o Responsable do Sistema serán os encargados de manter actualizada e organizada a documentación de seguridade e de xestionar os mecanismos de acceso á mesma.

10 Formación e concienciación

Todos e cada un dos usuarios dos sistemas de información da Deputación de Lugo son responsables da seguridade dos activos de información mediante un uso correcto dos mesmos, sempre de acordo coas súas atribucións profesionais e académicas.

Todos os membros da Deputación de Lugo teñen a obrigación de coñecer e cumprir esta política de seguridade da Información e a Normativa de Seguridade, sendo responsabilidade do Comité de Seguridade dispoñer os medios necesarios para que a información chegue aos afectados.

Os membros da Deputación de Lugo recibirán formación en seguridade da información. Establecerase un programa de concienciación continua para atender a todos os membros da Deputación de Lugo, en particular aos de nova incorporación.

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

11 Incumprimento

O incumprimento da presente Política de Seguridade da Información poderá carrexar o inicio das medidas disciplinarias que procedan, sen prexuízo das responsabilidades legais correspondentes.

12 Terceiras partes

Cando a Deputación de Lugo preste servizos a outros organismos ou manexen información doutros organismos, faráselles partícipes desta Política de Seguridade da Información, estableceranse canles para reporte e coordinación dos respectivos Comités de Seguridade TIC e estableceranse procedementos de actuación para a reacción ante incidentes de seguridade.

Cando a Deputación de Lugo utilice servizos de terceiros ou cedan información a terceiros,

faráselles partícipes desta Política de Seguridade e da Normativa de Seguridade que incumba aos devanditos servizos ou información. Dicha terceira parte quedará suxeita ás obrigacións establecidas en dicha normativa, podendo desenvolver os seus propios procedementos operativos para satisfacela. Estableceranse procedementos específicos de reporte e resolución de incidencias. Garantirase que o persoal de terceiros está adecuadamente concienciado en materia de seguridade, polo menos ao mesmo nivel que o establecido nesta Política.

Cando algún aspecto da Política non poida ser satisfeito por unha terceira parte segundo requírese nos parágrafos anteriores, requirirase un informe do Responsable de Seguridade que precise os riscos en que se incorre e a forma de tratalos. Requirirase a aprobación deste informe polos responsables da información e os servizos afectados antes de seguir adiante.

13 Histórico de revisións

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	REALIZADO	DATA	APROBADO
1.0	Primeira emisión	-	-	-
2.0	Segunda revisión e actualización	-	-	-
3.0	Revisión e integración con RGPD	-	-	-
4.0	Revisión e asignación de roles. Actualización con LOPDGDD	-	-	-
5.0	Actualización normativa vixente	SNT	14/10/2019	25/11/2019
6.0	Adaptación da PSI ao Real Decreto 311/2022. Revisión de funcións. Integración Política Protección de Datos	SNT	09/02/2023	27/03/2023
7.0	Modificación do Delegado Protección de Datos	CSI	13/10/2023	13/10/2023