Xunta de Galicia

Plan director de Seguridade TIC

2015-2020

Elaborado por Axencia de Modernización Tecnolóxica de Galicia

XUNTA DE GALICIA

amtega
Axencia para a Modernización Tecnolóxica

CONTROL DE VERSIÓNS E DISTRIBUCIÓN			
NOME DO DOCUMENTO:	**Plan director de seguridade TIC**	**VERSIÓN:**	01.00
COD. DO DOCUMENTO:			
ELABORADO POR:	Amtega	**DATA:**	Abril 2015
VALIDADO POR:	Comisión de Seguridade e Goberno Electrónico	**DATA:**	19 maio 2015
APROBADO POR:	Consello da Xunta de Galicia	**DATA:**	25 xuño 2015

REXISTRO DE CAMBIOS		
Versión	**Causa da nova versión**	**Data de aprobación**
01.00	Elaboración do documento	

LISTA DE DISTRIBUCIÓN (opcional)		
Nome	**Número de copia**	**Área/Centro/Localización**

Índice

1. Introdución

As tecnoloxías de información e das comunicacións convertéronse nos últimos anos nun instrumento fundamental para a Administración Pública no seu trato coa cidadanía. Fronte aos soportes tradicionais, a información dixital está suxeita a unha serie de riscos propios dos que a Administración debe protexerse adecuadamente. Os roubos, modificacións ou perdas de información poden afectar a millóns de datos. A suplantación de identidade pode dar acceso a información confidencial. Os servizos deben estar dispoñibles en todo momento, todos os días do ano. **A relación de confianza que a cidadanía deposita na Administración non debe romper por un problema de seguridade**.

O presente Plan Director de Seguridade contempla as actuacións en materia de seguridade TIC que a Xunta de Galicia acometerá no próximos seis anos para **asegurar que se mantén o grao de protección adecuado para a información xestionada pola Administración Xeral e do Sector Público de Galicia**.

1.1. Alcance

Queda dentro do alcance deste plan:

- ✓ Os sistemas de información do sector público autonómico de Galicia, competencia da Amtega en virtude do decreto 252/2011, de 15 de decembro, polo que se crea a Axencia para a Modernización Tecnolóxica de Galicia e apróbanse os seus estatutos.
- ✓ Os sistemas de información dos órganos da Administración de Xustiza de Galicia.
- ✓ A infraestrutura TIC dos centros educativos.
- ✓ Os sistemas de información transversais a toda a administración, incluíndo a administración local.
- ✓ No relativo a concienciación, o persoal do sector público, os cidadáns e as empresas de Galicia.

O prazo de execución cuberto por este plan é de seis anos, **desde 2015 a 2020**. Ao final do documento indícase a prioridade das actuacións e o prazo previsto para alcanzar os distintos obxectivos.

Non entra dentro do alcance deste plan a aplicación de medidas de seguridade da información nos sistemas que non estean xestionados pola Amtega.

1.2. Participantes

Para protexer adecuadamente a información requírese involucrar a todas as persoas que participan na súa xestión. Os principais responsables da execución deste plan son:

- ✓ A **Comisión de Seguridade e Goberno Electrónico**, como órgano colexiado de carácter transversal con competencias en materia de seguridade da información e goberno electrónico para a coordinación, asesoramento, impulso e promoción das actuacións en materia de seguridade da información, administración electrónica e seguimento da aplicación efectiva das medidas aprobadas no seu ámbito de actuación.
- ✓ A **Subcomisión de Seguridade**, como órgano de apoio en materia de seguridade á Comisión anterior, encargada de propoñer obxectivos estratéxicos, políticas e plans de acción, de aprobar as directivas e instrucións de seguridade, de velar polo cumprimento dos plans de auditoría, de promover a formación e a concienciación e de velar polo cumprimento das normas, directrices e instrucións de seguridade.

- ✓ A **Amtega**, como responsable da xestión dos sistemas de información do sector público autonómico de Galicia.
- ✓ As distintas **Consellerías**, como responsables da información que xestionan.

Toda organización está composta por persoas, e é fundamental que se comprenda que son estas as encargadas finais de facer que este plan se materialice con éxito, para o que se difundirá de forma axeitada segundo o nivel de responsabilidade de cada cal.

1.3. Obxectivos

O obxectivo deste plan a seis anos é mellorar a seguridade dos sistemas de información da Xunta de Galicia, cuxa xestión se atopa centralizada na Amtega. Este plan está aliñado coa **Estratexia Nacional de Ciberseguridade** aprobada en 2013 polo Goberno do Estado, que inclúe entre os seus principios reitores os de responsabilidade compartida, proporcionalidade, racionalidade e eficacia.

Pártese dunha situación transitoria na que os distintos organismos foron integrando os seus sistemas de información baixo o paraugas da Amtega. Unha vez rematada unha primeira fase de integracións en 2014, os esforzos centraranse en consolidar a xestión da seguridade para lograr que en 2020 se dispoña dunha xestión da seguridade:

- ✓ Transversal a todos os organismos da Xunta.
- ✓ Consolidada e madura, con todas as características dun Sistema de Xestión da Seguridade da Información.
- ✓ Baseada en análise de riscos.
- ✓ Que permita ter uns sistemas de información resistentes aos incidentes máis graves.
- ✓ Completamente adecuada aos requisitos legais.

Para lograr estes obxectivos, necesítase ampliar o persoal dedicado a xestionar a seguridade coa **creación dun novo Centro de Operación de Seguridade**, incrementaranse os esforzos na **concienciación dos empregados da Xunta** e implantaranse **novas medidas de seguridade**.

2. Accións previstas

A continuación descríbense as distintas accións a executar dentro do ámbito deste plan, deseñadas para alcanzar o obxectivo descrito anteriormente.

2.1. Formación e concienciación

Manter o nivel axeitado de seguridade é unha tarefa de todos. É sumamente importante que o persoal da Xunta coñeza os riscos aos que se expón a información e como mitigalos, así como a política corporativa, a normativa e os procedementos a seguir.

Dentro deste plan, continuarase o esforzo de concienciar e implicar na xestión da seguridade aos responsables dos distintos organismos, aos traballadores da Administración pública, aos cidadáns e ás empresas galegas.

Isto desenvolverase nos próximos anos mediante:

- ✓ **Campañas divulgativas**.
- ✓ **Cursos** dirixidos a empregados e directivos.
- ✓ **Material de concienciación**.

Farase especial fincapé na **formación técnica do persoal da Amtega**, encargado de xestionar os sistemas de información da Xunta, e en especial a do persoal encargado da seguridade, que debe velar pola protección da información e a súa dispoñibilidade en todo momento.

2.2. Cumprimento normativo

2.2.1. LOPD

O cumprimento da lexislación vixente é un dos obxectivos de máxima prioridade para as administracións públicas. A Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal e o Real Decreto 1720/2007, de 21 de decembro, polo que se aproba o seu regulamento de desenvolvemento, impoñen requisitos organizativos, de xestión e técnicos sobre o tratamento dos datos de carácter persoal, máis estritos canto máis sensibles sexa a información tratada.

A adecuación á LOPD **estase a desenvolver desde hai varios anos**, realizándose desde a Amtega un gran esforzo en facilitar aos distintos organismos autónomos todo o necesario para cumprir con ela (definición de ficheiros transversais, procedementos estándar, modelos para a documentación, un servizo de axuda,...). Ademais, cóntase cun rexistro central para relacionar os ficheiros declarados na Axencia Española de Protección de Datos coas aplicacións que almacenan os datos, de forma que a Amtega, como encargada de tratamento, poida establecer as medidas de seguridade adecuadas a cada caso.

Como parte deste plan, está previsto facer unha **revisión do estado de adecuación actual** e unha **revisión das medidas implantadas nos ficheiros automatizados**, o que constitúe a **maduración do proceso seguido en anos anteriores**.

Así mesmo, avanzarase no proceso de **recollida, clasificación e notificación de incidentes aos organismos afectados por fallos de seguridade**, posto que a compartición actual dos recursos cambiou o escenario onde se xestionan os sistemas, despois de pasarse de áreas informáticas propias nas distintas consellerías a un modelo xestionado pola Amtega con persoal común. Isto fai necesario revisar as ferramentas de xestión de incidentes utilizadas na actualidade, e establecer un mecanismo para

notificar automaticamente aos responsables dos ficheiros os problemas que poidan estar a afectar ás súas aplicacións e sistemas que traten datos de carácter persoal.

2.2.2. ENS

A Lei 11/2007, de 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos e o Real Decreto 3/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica (ENS), requiren medidas organizativas, de xestión e técnicas para protexer adecuadamente os servizos prestados por medios electrónicos, segundo a valoración dos seus responsables.

A creación da Amtega e da Comisión de Seguridade e Goberno Electrónico fixeron necesario **reformular o modo de lograr a adecuación completa ao ENS**. A Amtega, como xestor dos sistemas de información, é responsable da implantación das medidas técnicas de seguridade que deriven das valoracións realizadas polos responsables da información e dos servizos (fundamentalmente, as consellerías).

A concentración na Amtega da xestión dos sistemas de información **facilita a aplicación dunhas medidas técnicas comúns** de seguridade. Con todo, aínda **é necesario concretar as medidas organizativas e de xestión** e, sobre todo, contar cun medio para xestionar as valoracións da información e dos servizos e axustar as medidas de seguridade de acordo a elas.

Ata que se dispoña desa ferramenta, farase unha primeira revisión das medidas de seguridade aplicadas na actualidade, adecuándoas ao requirido para o nivel básico nas distintas dimensións de seguridade consideradas no ENS.

É necesario revisar as medidas de seguridade existentes nos sistemas de información que se integraron na Amtega, e nos novos que se vaian integrando, e adecuar as medidas de seguridade se fose necesario.

As medidas de seguridade para os sistemas xestionados pola Amtega evolucionaranse durante os anos da duración deste plan para adaptalas ás necesidades cambiantes dos sistemas de información e ós novos riscos, así como ás variacións do marco normativo que puideran xurdir.

2.3. Marco organizativo

A constitución en outubro de 2014 da **Comisión de Seguridade e Goberno Electrónico** supón dispoñer dun órgano colexiado do máximo nivel que aproba e supervisa a execución dos plans corporativos en materia de seguridade.

Así mesmo, en decembro de 2014 constituíuse a **Subcomisión de Seguridade**, que conta con representantes de todas as consellerías, e que será dinamizada dende a Amtega ao longo da execución deste plan director para que a estratexia corporativa se manteña aliñada coas súas necesidades.

A introdución desta estrutura marcará un antes e un despois na xestión da seguridade da información da Xunta de Galicia. Permitirá **homoxeneizar as liñas de actuación** postas xa en marcha nos distintos organismos e dispoñer dun **foro de discusión** onde poñer en común a experiencia gañada e discutir as actuacións a levar a cabo fronte á aparición de novas ameazas. Ademais, **establecerá obxectivos comúns** de seguridade, e **reducirá o gasto** relativo aos recursos necesarios para alcanzalos.

Seguindo a creación dos órganos anteriores,

- ✓ Presentarase a **política de seguridade corporativa** para a súa aprobación polo Consello da Xunta, como paso fundamental na homoxeneización da xestión da seguridade.

- ✓ Identificaranse os **requisitos para os distintos perfís** necesarios para cumprir coa lexislación vixente (como responsables da información, de servizos, de seguridade ou de sistemas), e asignaranse as súas funcións e responsabilidades.
- ✓ Promoverase a **creación de comités de seguridade nas distintas consellerías**, que terán un representante na subcomisión. Coordinarán a posta en marcha no seu ámbito nos aspectos non tecnolóxicos relacionados coa seguridade da información. Estes comités contarán co apoio e asesoramento da Amtega.

A Amtega continuará coa **formalización dos procedementos de traballo** de acordo ás normativas de seguridade recoñecidas internacionalmente, introducindo a seguridade como un elemento fundamental no desenvolvemento dos proxectos e creando comités internos de colaboración con todas as áreas da organización.

2.3.1. Política de seguridade corporativa e desenvolvemento do corpo normativo

Unha das primeiras actuacións da Comisión de Seguridade e Goberno Electrónico será presentar unha **política de seguridade corporativa** que sente as bases para o desenvolvemento da protección da información na Administración xeral e do sector público autonómico de Galicia. A aprobación desta política por parte do Consello da Xunta:

- ✓ Constituirá o **compromiso** formal da alta dirección da organización coa seguridade da información.
- ✓ Establecerá os **obxectivos** en materia de seguridade que deberán cumprir todos os organismos da Xunta e aqueloutros que queiran utilizala como referencia, como universidades ou concellos, simplificando os seus procesos de adecuación ao Esquema Nacional de Seguridade e demais normativa aplicable.
- ✓ Servirá como **base para o desenvolvemento de actuacións adicionais** que busquen alcanzar eses obxectivos.

Tras aprobarse a política, continuarase co plan actual de desenvolver o corpo normativo e os procedementos para todos os procesos que o requiran.

Debido á súa natureza, algúns dos organismos xa contan con normativa de seguridade e con estruturas organizativas dedicadas ao seu desenvolvemento, como é o caso do **Fondo Galego de Garantía Agraria**. Esta normativa revisarase e integrarase coa que se desenvolva a nivel corporativo.

Dentro deste capítulo, revisarase o Decreto 230/2008, do 18 de setembro, que establece as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia, para adecualo ás necesidades actuais.

2.3.2. Centro de operacións de seguridade

Dentro deste plan crearase un Centro de operacións de seguridade (máis coñecido polas súas siglas en inglés, SOC), que se encargue de **monitorizar en tempo real o estado da seguridade dos sistemas críticos**, notificando os incidentes importantes para poñer en marcha as accións correctivas adecuadas, chegando mesmo a **convocar ao comité de crise** no caso de que sexa necesario.

Este centro terá acceso a novas **ferramentas de monitorización** que se implantarán en 2015, así como ao estado dos sistemas involucrados na prestación dos servizos transversais (correo, portal, servidores de nomes, directorios corporativos, infraestrutura de rede,...).

Tamén participará na **revisión das vulnerabilidades** presentes nos sistemas actuais, **coordinándose co equipo de auditoría** e axudando a resolver os problemas detectados, para o que terán presenza activa nos foros de seguridade máis recoñecidos.

Os participantes do SOC **colaborarán co CCN-CERT,** CERT gobernamental español de referencia para a administración pública, para notificar incidentes e tomar accións de acordo ao grao de alerta indicado polo mesmo, en liña cos principios da Estratexia Nacional de Ciberseguridade.

A introdución deste Centro de operacións supón un paso máis no proceso de maduración da xestión da seguridade que está a acometer a Amtega. Reforzará os recursos dedicados á seguridade reactiva, permitindo poñer en marcha en menos tempo as medidas necesarias para para mitigar os efectos dos incidentes, ou para deter os posibles ataques antes de que teñan ningunha consecuencia sobre os sistemas da Xunta.

2.3.3. Creación dun equipo de auditoría de seguridade interna

A necesidade de revisar continuamente o estado da seguridade dos sistemas de información, fai que sexa adecuado dispoñer dun equipo de auditoría de seguridade que teña como obxectivo:

- ✓ A **análise das vulnerabilidades técnicas** presentes nos sistemas de información da Xunta.
- ✓ A realización de **test de intrusión** para verificar as posibilidades reais de explotación das vulnerabilidades anteriores.
- ✓ A **revisión do estado de adecuación á normativa vixente** (principalmente, LOPD e ENS), e a outros estándares de seguridade, como ISO 27001.

Trátase de constituír un **equipo independente dentro da Amtega** que realice estas funcións co obxecto de aforrar custos e mellorar os resultados, ao manter coherente o coñecemento que se ten sobre a organización.

Este equipo virá a reforzar os recursos dedicados a seguridade preventiva para diminuír a cantidade de vulnerabilidades presentes nos sistemas de información e velar pola correcta posta en práctica da normativa aplicable. Desta forma conseguirase diminuír a exposición ao risco e rebaixar a cantidade de incidentes sufridos pola organización.

Este equipo estará coordinado co Centro de Operacións de Seguridade.

2.3.4. Implantación dun SXSI ISO/IEC 27001

A seguridade da información non debe basearse en actuacións puntuais, senón que debe estar **fundamentada en procesos continuos** que permitan manter un nivel protección axeitado de forma permanente.

Con esa finalidade proponse a implantación, no ámbito da Amtega, dunha **sistema de xestión da seguridade da información (SXSI), baseado na norma ISO/IEC 27001**, que permita establecer os mecanismos necesarios para manter a xestión da seguridade de forma ordenada e sostible co paso do tempo.

Aínda que na actualidade non se conta cun SXSI formal, si que se seguen os principios recollidos de forma xeral neles: protección dos activos en función do seu valor, vixilancia do estado dos activos, recollida de indicadores de rendemento, normativa a seguir, procedementos para as tarefas habituais e para as continxencias, mellora continua,...

A implantación dun SXSI de acordo á norma internacional ISO/IEC 27001 supoñerá a **maduración dos procesos actuais**, o que repercutirá en:

- ✓ A **redución do risco** ao que se expón a organización.

- ✓ A **redución dos custos debidos a incidentes**.
- ✓ A **mellora a confianza** na organización de todas as persoas relacionadas con ela.

2.4. Marco operacional

2.4.1. Cadro de mando de seguridade

Nunha organización preocupada pola seguridade, é importante dispoñer das ferramentas adecuadas para a toma de decisións. A implantación dun cadro de mando de seguridade permitirá dispoñer dunha serie de medidas de elementos chave para a xestión da seguridade. Para iso:

- ✓ Determinaranse os **indicadores e métricas máis adecuados** para estimar o grao de seguridade e a súa evolución, tendo en conta o esforzo necesario para obtelos.
- ✓ Configuraranse as **ferramentas de monitorización** dispoñibles para obter automaticamente, sempre que sexa factible, a maior cantidade posible dos indicadores anteriores.
- ✓ Prepararanse **informes periódicos** cos indicadores anteriores, complementándoos con outros que axuden a comprender o contexto (por exemplo, os niveis de alerta publicados polo CCN-CERT).

Esta información permitirá coñecer o **nivel real de seguridade alcanzado**, e axudará a tomar decisións de alto nivel sobre posibles vías de actuación para mellorar a xestión da seguridade.

Unha vez que esta ferramenta alcance un grao de madurez axeitado, publicarase un indicador do estado da seguridade na Xunta de Galicia, para que os cidadáns coñezan o nivel de risco ao que se expoñen os datos tratados pola Administración.

2.4.2. Análise e xestión de riscos

O estándar **ISO/IEC 27001** e o **Esquema Nacional de Seguridade** perseguen dispoñer dunha xestión da seguridade baseada na adopción de medidas axeitadas para as ameazas ás que se enfronta a organización, ata alcanzar un nivel de risco aceptable. Para iso, é necesario **determinar o nivel de risco actual** no que se encontran os activos da organización ante unha hipotética materialización das ameazas, adoptando as medidas adecuadas para **rebaixalo a niveis aceptables** pola dirección, seguindo os seguintes pasos:

- ✓ Identificar os recursos máis importantes para a organización, en base a uns criterios claramente establecidos (custo, facilidade de substitución, dependencias con outros recursos,...).
- ✓ Identificar as ameazas sobre eses recursos, estimando a probabilidade de ocorrencia e o impacto producido.
- ✓ Determinar as salvagardas presentes que reducirían o impacto anterior en caso de incidencia.
- ✓ Identificar os puntos de mellora e elaborar un plan para poñelos en marcha.

Estas accións deben **repetirse periodicamente** e integrarse no resto de procesos da organización.

A medida que se vai completando a integración dos organismos da Xunta na Amtega, está a alcanzarse un punto de madurez no que se fai factible a realización dunha análise de riscos inicial sobre os recursos xestionados por ela, o que requirirá a **colaboración** de todos os organismos para **identificar e valorar** os seus activos importantes como primeiro paso do proceso.

Na actualidade xa se realizaron análise de riscos coa metodoloxía MAGERIT e a ferramenta PILAR nalgúns dos organismos da Xunta. A experiencia gañada con eles servirá para afrontar este proxecto con maiores garantías de éxito.

2.4.3. Xestión de continuidade e dispoñibilidade

A concentración dos sistemas de información nos Centros de Proceso de Datos xestionados pola Amtega fai necesaria a realización dun **plan de continuidade** que garanta o funcionamento dos organismos da Xunta en caso de sufrir un contratempo.

A elaboración deste tipo de plans require a identificación dos sistemas chave para o funcionamento dos distintos organismos da Xunta, os seus **requisitos de dispoñibilidade** e as **medidas a poñer en marcha** para cumprilos. Isto necesita a participación dos distintos organismos da Xunta, que deberán especificar os seus **obxectivos de negocio**, da Amtega, que deberá implantar as medidas adecuadas para lograr estes obxectivos, e da Subcomisión de Seguridade, que deberá aprobar o plan e supervisar a súa correcta execución.

Ademais do anterior, é necesario elaborar **plans de actuación en caso de desastre** para garantir unha resposta rápida a problemas graves, que deben probarse periodicamente para garantir o seu bo funcionamento antes de que sexan necesarios. Tamén se require a formalización dun comité de crise que xestione as situacións máis problemáticas e se encargue de coordinar todas as actuacións recollidas nos plans.

2.5. Medidas de protección

2.5.1. Seguridade física

Unha parte ás veces descoidada da seguridade da información é a que se refire á infraestrutura física que soporta os tratamentos de datos: instalacións físicas, subministracións, equipamento e persoal.

Dentro deste capítulo contémplanse as seguintes medidas de mellora:

- ✓ **Revisar os sistemas de control de acceso** das instalacións da Amtega para identificar posibles debilidades e aplicar medidas correctoras.
- ✓ **Implantar novas medidas de seguridade** nos Centros de Proceso de Datos.
- ✓ Continuar co despregamento gradual da solución de **control de acceso á rede**.
- ✓ Aumentar a presenza de **persoal de vixilancia nas instalacións chave**.

Para poder desenvolver este capítulo, será necesario establecer previamente un criterio común para a valoración das instalacións físicas, que se utilizará para decidir que medidas implantar en cada situación (por exemplo, arcos de detección de metais, cámaras de videovixilancia, detectores de presenza, fume ou auga, gardas de seguridade, clausura de entradas múltiples...).

2.5.2. Novas plataformas de seguridade

As medidas técnicas son tan importantes como as organizativas para garantir a protección da información. Como parte deste plan, implantaranse tres ferramentas importantes para protexer a información da Xunta:

- ✓ Un sistema de **protección contra os ataques distribuídos de denegación de servizo** (coñecido polas súas siglas en inglés, DDoS). Unha ferramenta deste tipo cobra especial importancia coa aparición da Amtega que, ao concentrar os recursos de comunicacións, fai que estes ataques poidan ter repercusións en varios organismos. Considérase necesario mellorar as medidas de seguridade actuais coa introdución dunha plataforma especializada.
- ✓ Un **sistema de xestión da información e eventos de seguridade, con capacidade de correlación de eventos**, que permita detectar problemas nos centos de miles de mensaxes de estado por

segundo que xeran actualmente os dispositivos de rede e outros sistemas xestionados pola Amtega, para tomar decisións máis rapidamente do que é posible hoxe.

- ✓ **Devasas a nivel de aplicación** (WAF), que permita detectar e deter ataques dirixidos contra os protocolos máis habituais.

Está previsto que a implantación destas plataformas se faga ao longo de 2015, consolidándose a súa utilización nos seguintes anos do plan.

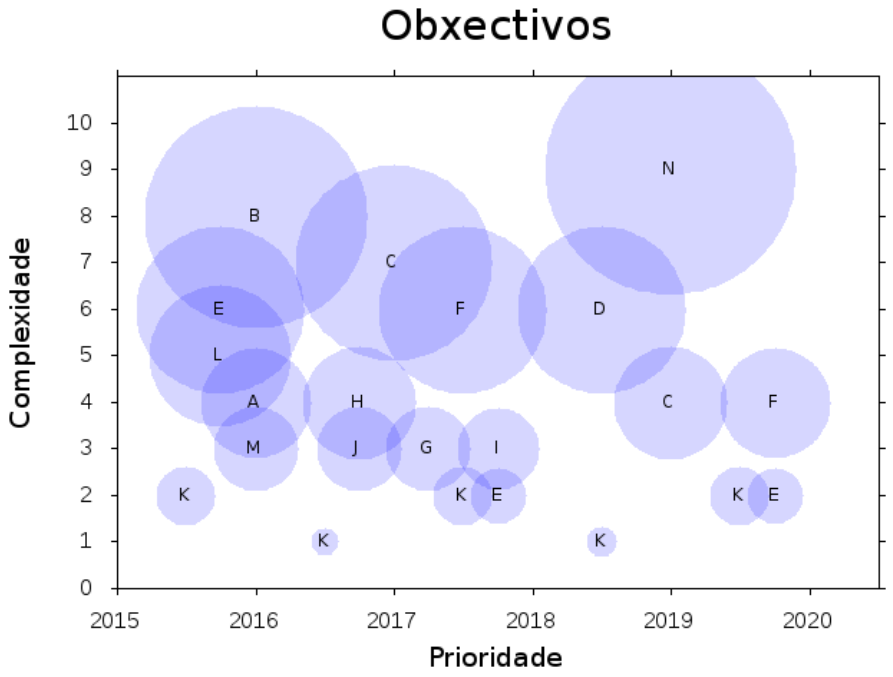
2.5.3. Outras melloras técnicas

Ademais das medidas de seguridade técnicas indicadas antes, acometeranse as seguintes:

- ✓ A implantación dunha nova barreira de devasas de nova xeración
- ✓ A implantación dunha **plataforma específica de detección e protección contra malware avanzado, con capacidades de análise dinámica**.
- ✓ A mellora na **seguridade da navegación** dos usuarios.
- ✓ A mellora na **configuración dos postos de usuario**: eliminación de sistemas operativos obsoletos, integración nos directorios corporativos, aplicación de políticas corporativas, restricións no uso do hardware,...
- ✓ A mellora nas medidas relativas a **xestión de identidades**: unificación dos directorios actuais, revisión dos procedementos de alta, baixa e modificación de usuarios, políticas de credenciais,... Automatización da xestión de identidades mediante unha ferramenta específica.
- ✓ Unha nova **plataforma para o acceso remoto** á rede corporativa.
- ✓ A evolución das plataformas específicas de seguridade (**antivirus**, **análise de vulnerabilidades**, **PKI**,...).
- ✓ A mellora da seguridade da arquitectura actual das **redes sen fíos**.
- ✓ A mellora da **seguridade nos dispositivos móbiles corporativos**.
- ✓ Evolución da plataforma de firma electrónica e mellora do almacén e custodia de **certificados dixitais**.

3. Planificación prevista

O seguinte gráfico mostra a disposición dos obxectivos deste plan tendo en conta a prioridade e a complexidade da súa posta en marcha:



O tamaño dos círculos é proporcional á complexidade dos obxectivos, que son os seguintes:

Etiqueta	Obxectivo
A	Política de seguridade corporativa e desenvolvemento do corpo normativo
B	Identificación e valoración de activos
C	Análise e xestión de riscos
D	Xestión de continuidade e dispoñibilidade
E	Cumprimento normativo: LOPD
F	Cumprimento normativo: ENS
G	Cadro de mando de seguridade
H	Centro de operacións de seguridade
I	Creación dun equipo de auditoría de seguridade interna
J	Seguridade física
K	Formación e concienciación
L	Novas plataformas de seguridade
M	Outras melloras técnicas
N	Implantación SXSI ISO/IEC 27001

Como pode observarse, dáse prioridade aos obxectivos fundamentais para a xestión da seguridade (políticas, corpo normativo e cumprimento da LOPD), despois dos cales se acometerá a determinación e clasificación dos activos, que constitúe un requisito para poder desenvolver outros obxectivos dentro do complexo ámbito dos sistemas de información da Xunta de Galicia.

No diagrama tamén se mostran algunhas das accións repetitivas que haberá que desenvolver ao longo do tempo, como as análises de riscos ou as accións formativas. Aínda que non se mostre para outras, hai que ter en conta que a xestión da seguridade é un traballo continuo, polo que algunhas das outras accións se desenvolverán ao longo dos anos despois de ser iniciadas.

3.1. Desagregación por actividades

A continuación indícase unha desagregación preliminar das actividades a desenvolver dentro de cada capítulo do plan, indicándose ademais o responsable da súa execución ou da súa revisión.

3.1.1. Formación e concienciación

Capítulo	Actividade	Descrición	Responsable
Formación e concienciación	Revisar o material de formación actual	Revisar o material do que se dispón actualmente para as campañas de formación e concienciación.	Amtega.
	Revisar o mecanismo de comunicación de incidentes ao público	Revisar o mecanismo actual de comunicación de incidentes, de forma que se facilite información responsable ao público sobre os problemas que poidan afectar de forma significativa aos seus datos.	Amtega. Consellerías. Subcomisión de Seguridade.
	Mellorar a formación de seguridade	Mellorar a formación de seguridade dos traballadores da Xunta de Galicia, especialmente entre o persoal técnico da Amtega.	Amtega. EGAP.

3.1.2. Cumprimento normativo

Capítulo	Actividade	Descrición	Responsable
LOPD	Documento de Seguridade e procedementos asociados	Revisión ou elaboración do Documento de Seguridade e dos procedementos asociados usando os modelos corporativos.	Consellerías. Amtega.

Capítulo	Actividade	Descrición	Responsable
	Nomeamento dos responsables de seguridade LOPD	Nomeamento formal dos distintos responsables de seguridade LOPD.	Consellerías.
	Comunicación dos ficheiros á Amtega	Comunicación dos ficheiros físicos dos distintos organismos e dos niveis da información persoal a través do rexistro central da Amtega.	Amtega. Consellerías.
	Adecuación das medidas de seguridade en tratamentos automatizados	Revisión das medidas de seguridade implantadas nos sistemas de información de acordo ao inventario anterior.	Amtega.
	Auditorías RLOPD	Realización das auditorías bienais esixidas polo RLOPD.	Amtega. Consellerías.
	Mecanismo para a notificación de incidentes a cada organismo	Establecer un mecanismo para notificar os incidentes que poidan afectar á seguridade dos datos persoais de cada organismo.	Amtega.
ENS	Ferramenta para a xestión da información relativa ao ENS	Proporcionar unha ferramenta para introducir e xestionar a información relativa ao Esquema Nacional de Seguridade, ou adecuar algunha das existentes.	Amtega.
	Revisión das medidas de seguridade actuais	Comprobar que as medidas de seguridade actuais se axustan, polo menos, ao nivel básico do Esquema Nacional de Seguridade.	Amtega.
	Nomeamento dos responsables da información, dos servizos e da seguridade TIC	Deben nomearse os distintos responsables indicados no Esquema Nacional de Seguridade, que deberán aprobar as valoracións da información e dos servizos dos seus respectivos organismos.	Amtega. Consellerías.

Capítulo	Actividade	Descrición	Responsable
	Valoración dos servizos e da información	Deben valorarse os activos de información e os servizos en cada unha das consellerías (isto farase ao mesmo tempo que se valoren os activos na análise de riscos).	Amtega. Consellerías.
	Establecemento de controis de seguridade	De acordo ás valoracións anteriores, debe revisarse a idoneidade das medidas de seguridade actuais e implantar as que sexa necesario, tanto as tecnolóxicas (Amtega), coma as organizativas (Subcomisión de Seguridade).	Amtega. Subcomisión de Seguridade.
	Auditorías ENS	Cando o proceso estea completo, debe realizarse unha auditoría para revisar a correcta adecuación ao ENS, que se repetirá cada 2 anos.	Amtega.

3.1.3. Marco organizativo

Capítulo	Actividade	Descrición	Responsable
Política de seguridade e desenvolvemento do corpo normativo	Aprobación da política de seguridade	Debe aprobarse a política de seguridade corporativa, cos obxectivos para toda a Xunta de Galicia.	Consello da Xunta.
	Definición de perfís con funcións e responsabilidades	Determinaranse os perfís involucrados na xestión da seguridade para todos os organismos da Xunta, e asignaranse funcións e responsabilidades. Terase en conta a normativa aplicable.	Comisión de Seguridade e Goberno Electrónico.
	Desenvolvemento do corpo normativo	Desenvolverase o corpo normativo que concrete os obxectivos definidos na Política de Seguridade Corporativa.	Amtega. Subcomisión de Seguridade.

Capítulo	Actividade	Descrición	Responsable
	Revisión do Decreto de Boas Prácticas	Revisarase o Decreto 230/2008, do 18 de setembro, que establece as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia, para adecualo ás necesidades actuais.	Amtega. Subcomisión de Seguridade.
Centro de operacións de seguridade	Creación do Centro de Operacións de Seguridade (COS)	Crear o COS e establecer as relacións necesarias co resto de áreas da organización.	Amtega.
	Monitorización dos sistemas críticos	Determinar os sistemas críticos e axustar a súa configuración para monitorizalos dende o COS.	Amtega.
	Análise de vulnerabilidades	Colaborar co EASI (Equipo de Auditoría de Seguridade Interna) na análise das vulnerabilidades presentes actualmente nos sistemas.	Amtega.
Equipo de auditoría de seguridade interna	Creación do Equipo de Auditoría de Seguridade Interna (EASI)	Crear o EASI e establecer as relacións necesarias co resto de áreas da organización, garantindo a súa independencia.	Amtega.
	Análise de vulnerabilidades	Analizar as vulnerabilidades presentes actualmente nos sistemas, utilizando tanto as ferramentas existentes coma as de nova implantación.	Amtega.
	Revisión periódica do grao de adecuación á normativa	Efectuar revisións periódicas para verificar o grao de implantación á normativa actual, tanto externa coma interna.	Amtega.

Capítulo	Actividade	Descrición	Responsable
Implantación dun SXSI ISO/IEC 27001	Determinación do alcance	Establecemento dun alcance realista e que permita un crecemento posterior	Amtega.
	Análise de brecha	Estudo do grao de implantación actual e das medidas necesarias para cumprir coa norma	Amtega.
	Plan de acción	Establecemento do plan de acción a seguir para implantar os cambios necesarios segundo a análise de brecha	Amtega.

3.1.4. Marco operacional

Capítulo	Actividade	Descrición	Responsable
Cadro de mando de seguridade	Determinación de métricas	Determinar indicadores e métricas máis adecuados para estimar o grao de seguridade e a súa evolución.	Amtega. Subcomisión de Seguridade.
	Obtención automática de indicadores	Configurar as ferramentas de monitorización para obter automaticamente os indicadores anteriores.	Amtega.
	Informes periódicos	Preparar informes periódicos cos indicadores anteriores, e analizalos na Subcomisión de Seguridade, elevando as conclusións á Comisión de Seguridade e Goberno Electrónico.	Amtega. Subcomisión de Seguridade. Comisión de Seguridade e Goberno Electrónico.
Análise e xestión de riscos	Criterios para a clasificación de activos	Elaboración duns criterios homoxéneos para valorar os activos por parte dos distintos organismos, tendo tamén en conta os necesarios para a Análise de Impacto no Negocio e para o Esquema Nacional de Seguridade.	Amtega. Subcomisión de seguridade.

Capítulo	Actividade	Descrición	Responsable
	Determinación e clasificación de activos.	Determinar os activos importantes para a organización e valoralos nas súas distintas dimensións de seguridade.	Amtega. Consellerías.
	Análise de Impacto no Negocio (BIA)	Determinar os tempos máximos que unha organización pode soportar sen que os seus activos estean dispoñibles (aínda que esta é unha actividade de Continuidade de Negocio, pero é conveniente realizala á vez que se valoran os activos).	Amtega. Consellerías.
	Identificación de ameazas	Determinar as ameazas sobre os activos anteriores e a súa posibilidade de materialización.	Amtega.
	Identificación de salvagardas	Valorar a efectividade das salvagardas actuais para mitigar os efectos das ameazas.	Amtega.
	Plan de acción	Identificar os puntos de mellora de acordo á información anterior e realizar con eles un plan de acción.	Amtega.
Xestión de continuidade e dispoñibilidade	Plan de continuidade	Determinar as medidas a tomar para cumprir cos requisitos do BIA.	Amtega. Subcomisión de Seguridade.
	Plans de actuación en caso de desastre	Documentar as formas de actuar ante distintos tipos de desastre, incluíndo plans de proba.	Amtega.

3.1.5. Medidas de protección

Capítulo	Actividade	Descrición	Responsable
Novas plataformas de seguridade	Implantar as novas plataformas de seguridade	Actualizar algunhas das plataformas de seguridade existentes na Amtega.	Amtega.
Outras melloras técnicas	Implantar o resto de melloras técnicas previstas.		Amtega.

4. Investimento

A seguinte táboa mostra o investimento previsto en euros para este Plan Director de Seguridade TIC no período 2015-2020:

	Investimento total período 2015-2020	2015	2016	2017	2018	2019	2020
Formación e concienciación	234.000,00	9.000,00	45.000,00	45.000,00	45.000,00	45.000,00	45.000,00
Cumprimento normativo	3.216.600,80	191.500,40	585.100,40	610.000,00	610.000,00	610.000,00	610.000,00
Marco organizativo	1.840.000,00	90.000,00	300.000,00	300.000,00	400.000,00	400.000,00	350.000,00
Marco operacional	720.600,00	50.600,00	55.000,00	330.000,00	95.000,00	95.000,00	95.000,00
Medidas de protección	5.631.986,31	2.591.986,31	800.000,00	950.000,00	1.000.000,00	-	290.000,00
Total investimento	**11.643.187,11**	**2.933.086,71**	**1.785.100,40**	**2.235.000,00**	**2.150.000,00**	**1.150.000,00**	**1.390.000,00**

5. Referencias

- ✓ [Lei 11] Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos.
- ✓ [ENS] Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica.
- ✓ [LOPD], [RLOPD] Lei Orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal (LOPD) e Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento desta (RLOPD).
- ✓ [Decreto 230/2008] Decreto 230/2008 do 18 de setembro de Boas Prácticas na utilización dos Sistemas de Información da Administración da Comunidade Autónoma de Galicia.
- ✓ [ISO 27001:2013] UNE-ISO/IEC 27001:2013 - Sistemas de Xestión da Seguridade da Información.
- ✓ UNE 71504:2008 - Metodoloxía de análise e xestión de riscos para os sistemas de información.

6. Glosario

Activo	Funcionalidade ou compoñente que teña valor para a organización. Inclúe: información, datos, servizos, aplicacións, equipos, comunicacións, recursos administrativos, recursos físicos e recursos humanos.
Análise de Impacto no Negocio (BIA)	Estudo dos tempos máximos que unha organización pode asumir sen ter dispoñible ningún dos seus activos, e da máxima cantidade de información que está disposta a perder en caso de que aconteza un incidente.
Axencia para a Modernización Tecnolóxica de Galicia (Amtega)	Axencia adscrita á Presidencia da Xunta de Galicia que ten como obxectivos básicos a definición, o desenvolvemento e a execución dos instrumentos da política da Xunta de Galicia no campo das tecnoloxías da información e a comunicación e a innovación e o desenvolvemento tecnolóxico.
Ameaza	Causa potencial dun incidente que pode causar danos a un sistema de información ou a unha organización. [UNE 71504:2008] As ameazas sempre están presentes, pero pódense intentar evitar ou paliar os efectos da súa materialización.
Análise de riscos	Proceso para a análise das ameazas, vulnerabilidades, riscos e impactos aos que está exposto un sistema de información, tendo en conta as medidas de seguridade xa presentes. Serve como punto de partida para identificar as melloras nas medidas de seguridade, tendo en conta tanto a efectividade coma os custos.
Auditoría	Estudo e exame que se realiza sobre un sistema de información coa finalidade de comprobar a súa conformidade respecto a algunha norma, procedemento, lei ou política, co fin de detectar incumprimentos e recomendar as medidas de corrección oportunas.
Confidencialidade	Propiedade ou característica consistente en que a información nin se pon a disposición nin se revela a individuos, entidades ou procesos non autorizados. [ENS]
Cadro de mando	Sistema de indicadores relevantes para un asunto específico (en inglés KPIs ou Key Performance Indicators), que facilitan a toma de decisións e o control.
Corpo normativo	Conxunto de normas que desenvolven de forma máis concreta o xeito de alcanzar os obxectivos dunha política.
Dato de carácter persoal	Calquera información concernente a persoas físicas identificadas ou identificables. [LOPD]
Dispoñibilidade	Propiedade ou característica dos activos consistente en que as entidades ou procesos autorizados teñen acceso a estes cando o requiren. [ENS]
Xestión de continuidade	Actividades que leva a cabo unha organización para asegurar que todos os procesos de negocio críticos estarán dispoñibles para os seus usuarios, clientes, provedores e outras entidades que deban utilizalos.
Xestión de incidentes	Procesos orientados a recuperar o nivel habitual de funcionamento do servizo e minimizar en todo o posible o impacto negativo na organización de forma que a calidade do servizo e a dispoñibilidade se manteñan.
Xestión de riscos	Actividades coordinadas para dirixir e controlar unha organización con

	respecto aos riscos. [ENS]
Incidente ou incidencia de seguridade	Suceso inesperado ou non desexado con consecuencias en detrimento da seguridade do sistema de información. [ENS]
LOPD	Lei Orgánica 15/1999 do 13 de decembro de Protección de Datos de Carácter Persoal.
Medidas de seguridade	Conxunto de disposicións encamiñadas a protexerse dos riscos posibles sobre o sistema de información, co fin de asegurar os seus obxectivos de seguridade. Pode tratarse de medidas de prevención, de disuasión, de protección, de detección e reacción, ou de recuperación. [ENS]
Monitorización	Vixilancia e rexistro de distintas medidas sobre o funcionamento dos servizos, como tempo de resposta, capacidade, número de usuarios concorrentes,...
Política de seguridade	Documento de alto nivel que especifica os obxectivos en materia de seguridade dunha organización, e reflicte o compromiso da xerencia para alcanzalos.
Proceso	Conxunto organizado de actividades que se levan a cabo para producir un produto ou servizo; ten un principio e fin delimitado, implica recursos e dá lugar a un resultado. [ENS]
RLOPD	Regulamento de Desenvolvemento da LOPD, aprobado polo Real Decreto 1720/2007, do 21 de decembro.
Risco	Estimación do grao de exposición a que unha ameaza se materialice sobre un ou máis activos causando danos ou prexuízos á organización. [ENS]
Seguridade da Información	Protección da información e dos sistemas de información fronte ao acceso, uso, divulgación, alteración, modificación ou destrución non autorizadas.
Sistema de Xestión da Seguridade da Información (SXSI)	Sistema de xestión que, baseado no estudo dos riscos, establécese para crear, implementar, facer funcionar, supervisar, revisar, manter e mellorar a seguridade da información. O sistema de xestión inclúe a estrutura organizativa, as políticas, as actividades de planificación, as responsabilidades, as prácticas, os procedementos, os procesos e os recursos. [ENS]
Sistema de información	Conxunto organizado de recursos para que a información se poida recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, poñer a disposición, presentar ou transmitir. [ENS]
Soporte	Medio físico de calquera tipo (papel, DVD, discos portátiles, etc.), utilizado para almacenar información.
Test de intrusión	Probas que simulan un ataque aos sistemas de información dunha organización co obxectivo de determinar o seu nivel de seguridade e o grao de éxito que tería un atacante sobre estes.
Vulnerabilidade	Unha debilidade que pode ser aproveitada por unha ameaza. [ENS]