PD

Plan Director de Seguridade TIC 2019 -2021

Elaborado por: CSIRT.gal -Amtega

Maio 2019

XUNTA DE GALICIA

CSIRT.gal

amtega
Axencia para a Modernización Tecnolóxica

ÍNDICE

1 INTRODUCIÓN

Nesta sección defínense as accións previstas no período 2019-2021, debidas á **AMPLIACIÓN DO ALCANCE DO PLAN DIRECTOR DE SEGURIDADE**, ocasionada polas recentes modificacións na lexislación e normativa aplicables no ámbito da seguridade da información e a protección de datos persoais e a evolución das novas tecnoloxías.

De xeito adicional ao anterior plan, e dentro do compromiso da Amtega para a evolución da seguridade e a mellora continua, incluíuse un **NOVO MARCO DE APLICACIÓN DA SEGURIDADE** relacionado coa Seguridade no Ciclo de Vida do Desenvolvemento do Software.

Ademais, neste novo plan inclúense medidas de seguridade que se adaptan aos **NOVOS RETOS TECNOLÓXICOS** como os servizos na nube (*cloud*) ou infraestrutura como servizo (IaaS - *Infraestructure as a Service*), que na actualidade supoñen unha forma habitual de definición de arquitecturas nos novos proxectos.

2 ALCANCE

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 se aproban os seus estatutos.

Os **sistemas de información dos órganos da Administración de Xustiza de Galicia** xestionados pola Amtega.

A **infraestrutura TIC dos centros educativos**.

Os **sistemas de información transversais a toda a administración**, incluíndo a administración local.

No relativo á concienciación, o **persoal do sector público, os cidadáns e as empresas de Galicia**.

O prazo de execución cuberto por este plan é de tres anos, **desde 2019 a 2021**.
Non entra dentro do alcance deste plan a aplicación de medidas de seguridade da información nos sistemas que non estean xestionados pola Amtega.

3 OBXECTIVOS

O obxectivo deste plan 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 2019 polo Goberno do Estado. Os esforzos centraranse en consolidar a xestión da seguridade para lograr que en 2021 se dispoña dunha **XESTIÓN DA SEGURIDADE**:

- **Transversal a todos os organismos da Xunta**
- **Consolidada e madura**
- **Baseada en análise de riscos**
- **Con 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**, incrementaranse os esforzos na **concienciación dos empregados da Xunta** e implantaranse **novas medidas de seguridade**.

4 PLAN DE ACCIÓN

- Continuarase coa execución de accións formativas en colaboración coa **EGAP**, en materia de seguridade da información e protección de datos persoais.
- Levaranse a cabo campañas de **CONCIENCIACIÓN** por correo electrónico e na Intranet da Xunta de Galicia.
- Haberá **FORMACIÓN ESPECIALIZADA** para o persoal que participa na execución de proxectos TIC na Amtega e **FORMACIÓN ESPECÍFICA PARA OS DPD** da Xunta de Galicia.

*Orientadas a diferentes **tipos de perfil** (usuario final, persoal con responsabilidade en materia de seguridade da información en protección de datos persoais, persoal técnico, etc.).*

*Esta formación inclúe **cursos presenciais, charlas divulgativas presenciais e divulgación mediante xogos** (gamificación).*

4 PLAN DE ACCIÓN

FORMACIÓN E CONCIENCIACIÓN | **CUMPRIMENTO NORMATIVO** | MARCO ORGANIZATIVO | MARCO OPERACIONAL | MEDIDAS DE PROTECCIÓN | SEGURIDADE DO SOFTWARE

RXPD e LOPD | ENS | OUTRA NORMATIVA

- Reelaboración do **rexistro de actividades de tratamento** de datos persoais.
- Elaboración das **guías de análise de riscos** e avaliacións de impacto na privacidade con arranxo ao RXPD e á nova valoración dos activos.
- Revisión ou deseño e elaboración de todos aqueles procedementos e guías necesarios para dar cumprimento ao esixido polo RXPD na Xunta de Galicia.
- Revisión da **valoración actual dos activos** para a categorización segundo o RXPD.
- Establecemento das medidas de seguridade apropiadas para garantir un **control de acceso seguro** e aliñado coas necesidades da Xunta e para cumprir coa normativa vixente.
- Implantación dunha **ferramenta para a xestión** integral de todo o relacionado co RXPD.
- **Apoio aos Delegados/as de protección** de datos da Xunta de Galicia.

4 PLAN DE ACCIÓN

FORMACIÓN E CONCIENCIACIÓN | **CUMPRIMENTO NORMATIVO** | MARCO ORGANIZATIVO | MARCO OPERACIONAL | MEDIDAS DE PROTECCIÓN | SEGURIDADE DO SOFTWARE

RXPD e LOPD | **ENS** | OUTRA NORMATIVA

No período 2019-2021 desenvolverase e executarase o **plan de adecuación ao ENS**, na medida en que haxa dispoñibilidade orzamentaria.

4 PLAN DE ACCIÓN

RXPD e LOPD | ENS | **OUTRA NORMATIVA**

Avaliarase o impacto de calquera normativa nova de aplicación que se publique durante o período de execución deste plan, como por exemplo:

- Directiva europea 2016/680, de protección de datos persoais no ámbito policial e xudicial penal, e a súa futura lei de transposición á normativa española.
- Regulamento europeo sobre a privacidade e as comunicacións electrónicas
- Regulamento europeo 2019/881 (regulamento sobre a ciberseguridade)

4 PLAN DE ACCIÓN

IMPLANTACIÓN DUN SXSI ISO/IEC 27001

- Determinar un alcance realista para a aplicación da norma, que permita un incremento posterior.
- Análise de fenda: estudo do grao de implantación actual e das medidas necesarias para chegar ao grao de cumprimento desexado da norma.
- Establecer un plan de acción a seguir para implantar os cambios necesarios segundo a análise de fenda realizada.

Ademais, a maiores inclúense neste periodo ampliado a actividade de estandarizar, medir e auditar os principais procedementos de seguridade, aliñados coa **ISO 9001**.

Continuarase potenciando **CSIRT. gal,** traballando na mellora dos procedementos, e estudando a posibilidade de asociarse a outros grupos internacionais de xestión de incidentes, por exemplo a rede FIRST.

Continuarase apoiando a actuación dos diferentes órganos colexiados con competencias en materia de seguridade da información.

4 PLAN DE ACCIÓN

CADRO DE MANDO DA SEGURIDADE	Durante este período vaise estudar a posibilidade de automatizar e mellorar a **obtención das métricas** de seguridade do cadro de mando.
ANÁLISE E XESTIÓN DE RISCOS	Será necesario manter actualizadas as **análises de riscos** e, tal como se comentou no apartado relativo ao ENS, realizarase a avaliación de impacto no negocio nos casos nos que o ENS así o esixa.
XESTIÓN DE CONTINUIDADE E DISPOÑIBILIDADE	Elaborarase un plan de actuación en caso de desastre para **garantir unha resposta rápida a problemas graves**. Tamén se traballará na formalización dun comité de crise que xestione as situacións máis problemáticas e se encargue de coordinar todas as accións recollidas nos plans.

4 PLAN DE ACCIÓN

- Implantación dunha nova plataforma de **prevención ante intrusións** (IPS).
- Control do **uso de dispositivos/portos**; mellora da xestión de soportes e o seu uso.
- Implantación dunha plataforma de **protección contra o malware avanzado**.
- **Implantación de Dobre Autenticación**
- Mellora das capacidades de auditoría dos **sistemas de ficheiros**
- Inspección do **tráfico cifrado**
- **Servizos Cloud**: Implantación das medidas necesarias para a **regulación e control dos servizos na nube**.
- Ampliación das **capacidades do SIEM**: melloras no sistema de rexistro de eventos de seguridade para aumentar a súas capacidades de adquisición de datos.
- Apoio aos **grupos de xestión de infraestrutura** (telecomunicacións, sistemas, posto cliente) na mellora da seguridade das plataformas que xestionan.

Ademais, poñeranse en marcha medidas para manter en correcto estado e seguir operando as plataformas de seguridade de rede adquiridas en 2015.

4 PLAN DE ACCIÓN

- Revisión da **normativa aplicable no ámbito do desenvolvemento de software seguro**
- Revisión e auditoría das **características de seguridade e deseño do software nas aplicación principais** da Amtega para valorar a súa adecuación á política e á normativa aplicables
- Preparación de **material formativo e inclusión de anexos/acordos nos pregos de desenvolvemento** para asegurar que o persoal de terceiros que traballa no desenvolvemento de aplicacións para a Amtega teña coñecemento dos requisitos, normas e políticas de seguridade aplicables ao seu labor
- Asegurar que os **novos proxectos** cumpran cos requisitos de seguridade definidos
- Mellora do **soporte e capacidades da plataforma de integración continua**