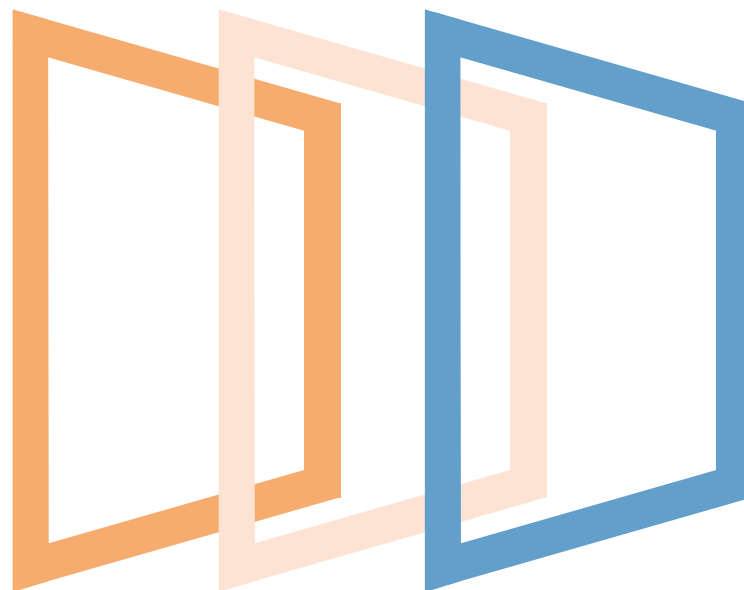




1001- Esquema Nacional de Seguridade

minsa



An Indra company

Índice

- 01. La esencia de la Ley 11/2007, el ENS y el ENI
- 02. Principios básicos del ENS
- 03. Requisitos mínimos del ENS
- 04. Las medidas de seguridad. Intensidades de aplicación
- 05. Visión global de las medidas de seguridad
- 06. Guías de ayuda para las actividades bajo el ENS
- 07. Roles y responsabilidades en el ENS
- 08. La seguridad orientada al riesgo: Análisis de riesgos
- 09. Gestión de los riesgos: El Plan de acción
- 10. Metodología de análisis y gestión de riesgos empleada en la Diputación
- 11. Normativa y procedimientos de seguridad existentes
- 12. Ingeniería social
- 13. Sofisticación del cibercrimen
- 14. Buenas prácticas

La esencia de la Ley 11/2007, el ENS y el ENI

minsait

01

An Indra company

3

01. La esencia de la Ley 11/2007, el ENS y el ENI

Ley 11/2007 (derogada por las leyes 39/2015 y 40/2015)

La Ley 11/2007 (Ley de acceso electrónico de los ciudadanos a los servicios públicos) es la ley que (hasta su derogación por las leyes 39/2015 y 40/2015) regulaba lo que se ha dado en llamar Administración Electrónica.

Su objetivo es dar carta de naturaleza a la Administración Electrónica; esto es, permitir llevar a cabo el Procedimiento Administrativo por medios exclusivamente electrónicos (este objetivo está explícitamente recogido en la Ley 39/2015, que plantea el canal electrónico como principal y el papel como residual, en todo caso).

Para poder llevar a cabo lo anterior, la ley se ocupa de manera especial los aspectos principales ligados a la seguridad de la “información administrativa electrónica” (expediente electrónico, documento electrónico, notificaciones electrónicas, sede electrónica, registros de entrada electrónicos,...)

01. La esencia de la Ley 11/2007, el ENS y el ENI

El modelo de la Ley 11/2007 para la regulación de la información electrónica.

La Ley 11/2007 se centra en dos elementos principales:

- Interoperabilidad: garantizar el flujo completo de información administrativa a lo largo de toda la cadena de tramitación (incluyendo intercambios entre distintas administraciones, la remisión de expedientes a la autoridad judicial y la gestión de archivos).
- Seguridad: custodia de los expedientes, integridad de los mismos, confidencialidad, trazabilidad,...

Para llevar a cabo lo anterior, la Ley define dos “esquemas”: El Esquema Nacional de Interoperabilidad (ENI) y el Esquema Nacional de Seguridad (ENS). Las previsiones para estos dos esquemas se mantienen en la Ley 40/2015 (Art. 156).

ENI y ENS. Planteamiento general

La plasmación legislativa del ENI y el ENS ha sido parecida pero diferente:

- Desarrollo de dos Reales Decretos: en el ENI, un RD “paraguas”; en el ENS, una normativa operativa.
- Desarrollo, bajo el amparo legislativo de dichos Reales Decretos, de un conjunto extenso de normas técnicas específicas, que en el ENI constituyen el “esquema” en sí, y en el ENS son de apoyo:
 - Normas Técnicas de Interoperabilidad, para el ENI.
 - Normas CCN-STIC 800, para el ENS.

Nota: a diferencia de las Normas Técnicas de Interoperabilidad, las CCN-STIC NO son de obligado cumplimiento... pero, tal como advierte el CCN “No se trata, por tanto, de normas imperativas, sino de la expresión de metodologías y recomendaciones para el adecuado cumplimiento de lo dispuesto en el ENS. Recomendaciones que tendrán especial significación para aquel organismo administrativo afectado por un incidente grave de seguridad, motivado por la inobservancia de las recomendaciones descritas”.

Principios básicos del ENS

minsait

02

An Indra company

7

02. Principios básicos del ENS.

El objetivo del ENS: el establecimiento de políticas de seguridad de la información

El objetivo del ENS es **establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.**

Y su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Antes de continuar, aclarar un poco el significado de los elementos anteriores.

Cómo debe entenderse el concepto de seguridad en el ENS

Seguridad es un concepto relativamente etéreo, por lo que resulta necesario aclarar el concepto antes de seguir.

El R.D. 3/2010 define en su anexo IV “Seguridad de las Redes y la información” como:

“la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que compromentan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen y hacen accesibles”.

A pesar de lo anterior, al definir en el anexo I las “dimensiones de seguridad”, el RD 3/2010 cita una más”

- a) Disponibilidad [D].
- b) Autenticidad [A].
- c) Integridad [I].
- d) Confidencialidad [C].
- e) Trazabilidad [T].

Cómo debe entenderse el concepto de seguridad en el ENS

Es imposible un nivel de garantía infinito en cualquier tarea humana; por eso, el 3/2010 habla de “un determinado nivel de confianza”

En la terminología habitual de seguridad, este nivel de confianza se refiere al denominado “riesgo residual”, esto es, el riesgo que queda después de administrar medidas de control y que ha de ser inferior al denominado “nivel de riesgo” que se considera aceptable en base a una metodología coste / beneficio de análisis de riesgos.

Así, podría resumirse, a efectos prácticos (y sin entrar en todos sus detalles) como objetivo principal del ENS:

“Definir los criterios para demostrar que el / los responsables de una organización de la Administración Pública han hecho lo necesario para que el riesgo de que la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos por una organización sea en todo momento menor que un umbral establecido de antemano”.

Objetivos principales del ENS

Mas en detalle, los objetivos principales del ENS son los siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un tratamiento continuado de la seguridad.

Ámbito de aplicación del ENS

El ámbito de aplicación del ENS es, tal como indica el Art. 2 de la Ley 40/2015, es como sigue:

- a) La Administración General del Estado.
- b) Las Administraciones de las Comunidades Autónomas.
- c) Las Entidades que integran la Administración Local.
- d) El sector público institucional

Los sistemas de información afectados por el ENS son, como regla general:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información accesibles electrónicamente por los ciudadanos.
- Sistemas de Información para el ejercicio de derechos.
- Sistemas de Información para el cumplimiento de deberes.
- Sistemas de Información para recabar información y estado del procedimiento administrativo.

Sistemas de información fuera del ámbito de aplicación del ENS

Aquellos sistemas para los que se cumpla en su totalidad lo siguiente:

- No esté relacionado con el ejercicio de derechos por medios electrónicos, o
- No esté relacionado con un cumplimiento de deberes por medios electrónicos, o
- No esté relacionado con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

Podrán excluirse del ámbito de aplicación del ENS (aunque opcionalmente podrán estar incluidos).

En CUALQUIER OTRO CASO, se aplica el ENS

El Anexo II

Un punto especialmente importante del ENS es su anexo II.

- El anexo II marca un conjunto de medidas mínimas que deben aplicarse y auditarse en un sistema de información, en base a la información que se maneje y a la criticidad de la misma.
- Podría decirse que, esencialmente, el ENS consiste en garantizar que la “checklist” proporcionada por el Anexo II se cumple en todo momento.

Requisitos mínimos del ENS

minsait

03

An Indra company

15

Cuáles son los requisitos mínimos del ENS

Los requisitos mínimos que impone obligatoriamente el ENS vienen indicados en el **Art. 11**.

Artículo 11. Requisitos mínimos de seguridad.

1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.*
- b) Análisis y gestión de los riesgos.*
- c) Gestión de personal.*
- d) Profesionalidad.*
- e) Autorización y control de los accesos.*
- f) Protección de las instalaciones.*

03. Requisitos mínimos del ENS.

Cuáles son los requisitos mínimos del ENS

Los requisitos mínimos que impone obligatoriamente el ENS vienen indicados en el **Art. 11. (Cont.)**

g) Adquisición de productos.

h) Seguridad por defecto.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Que significan los requisitos mínimos

Los requisitos mínimos consisten en que toda Administración (en el caso de ayuntamientos, pueden delegar esta política en diputaciones o cabildos) ha de tener un documento formal de obligado cumplimiento que regule los procedimientos indicados anteriormente, y que será auditada periódicamente

IMPORTANTE: Los Requisitos Mínimos deben cumplirse siempre. Lo más habitual es que se plasmen por medio de la aplicación de las medidas de seguridad establecidas en el Anexo II del ENS; pero si, por alguna razón, motivada y documentada, las medidas de seguridad del citado Anexo II son sustituidas por otras medidas compensatorias, los requisitos mínimos, en todo caso, deben cumplirse igualmente.

03. Requisitos mínimos del ENS.

Que significan los requisitos mínimos

En otras palabras: en **todo organismo** que forme parte de la Administración, aspectos tales como la compra de productos informáticos, los cursos de formación, el registro de la actividad relevante, en todos los ámbitos relacionados con los sistemas objeto del ENS, deben **llevarse a cabo necesariamente** mediante unos procedimientos que deben estar **definidos a priori**.

Las medidas de seguridad. Intensidades de aplicación

minsait

04

An Indra company

20

04. Las medidas de seguridad. Intensidades de aplicación.

Concepto de categoría de un sistema.

El R.D. 3/2010, en su Art. 43, Categorías, define el concepto de categoría de un sistema.

- *1. La categoría de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.*
- *2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.*

La categoría de un sistema determina, en base al criterio de proporcionalidad, el nivel de aplicabilidad de las medidas de seguridad que se le apliquen. Los criterios para determinar las categorías se definen en el Anexo I.

Tipos de categorías.

El R.D. 3/2010 define tres categorías para sistemas de información:

- Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados
- Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

La categoría de un sistema será LA MAS ALTA alcanzada en cualquier dimensión (esto es, por ejemplo, si tiene categoría baja en cuatro dimensiones pero alta en una, se puntuará como ALTA).

04. Las medidas de seguridad. Intensidades de aplicación.

Concepto de medidas de seguridad.

Una vez determinado la categoría del sistema, se procederá a la aplicación de las medidas de seguridad.

Las medidas de seguridad se enumeran en el Anexo II (que, como se ha indicado previamente, es el elemento central del R.D. 3/2010).

Las medidas de seguridad son un conjunto de acciones (expresadas a alto nivel en el Anexo II, pero que deben concretarse para cada caso concreto, que aplicadas a cada una de las 5 dimensiones de seguridad indicadas en el Anexo I (esto es, Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C] y Trazabilidad [T]) permiten reducir el riesgo de compromiso de cada una de estas dimensiones a un nivel considerado aceptable.

La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.

04. Las medidas de seguridad. Intensidades de aplicación.

Carácter esencial de las medidas de seguridad.

Las medidas de seguridad son el elemento fundamental de todo el ENS, y son su elemento sustantivo.

Puede decirse que todo el ENS radica en garantizar que se pueda demostrar en todo momento que se han elegido las medidas de seguridad adecuadas.

En último término, lo que determinará la responsabilidad de una determinada organización y de su personal en términos del ENS consistirá en la constatación de si se habían aplicado las medidas de seguridad adecuadas en un momento dado (aunque, por ejemplo, se haya producido un problema importante de seguridad. La seguridad informática es un objetivo que evoluciona en el tiempo, y es perfectamente posible (aunque no probable) que un atacante descubra un método revolucionario de ataque. Lo importante es aplicar, en todo momento, el conocimiento disponible.

Visión global de las medidas de seguridad

minsait

05

An Indra company

25

Estructura de las medidas de seguridad.

Las medidas de seguridad se agrupan en tres categorías:

- Marco organizativo (Org): Que se refiere a medidas de tipo procedimental general, tales como la existencia de política de seguridad y su adecuada supervisión o la existencia de una Normativa de seguridad
- Marco operacional (Op): Que se refieren a medidas de tipo procedimental ligadas a la operación de los sistemas de información, tales como la existencia de una metodología de análisis de riesgos adecuada, de una arquitectura de seguridad adecuada y al día o un procedimiento para la adquisición de nuevos componentes adecuado y al día.
- Medidas de protección(Mp): Que define medidas más específicas a nivel de seguridad informática, tales como la existencia de áreas separadas y con control de acceso, la existencia de sistemas de identificación de las personas, o la existencia de mecanismos de securización perimetral.

05. Visión global de las medidas de seguridad.

Cómo se consulta el Anexo II, de medidas de seguridad.

Pongamos un ejemplo práctico:

Supongamos que el sistema de gestión de expedientes de ayudas para personas con SIDA tiene nivel de seguridad alto, y el de solicitudes de ocupación de la vía pública nivel bajo.

El Anexo II tiene una tabla inicial, en el que obtendríamos las medidas.

05. Visión global de las medidas de seguridad.

Cómo se consulta el Anexo II, de medidas de seguridad.

En la tabla (páginas 20 y 21 del R.D. 3/2010) veríamos que para ambos sistema aplican las cuatro medidas Org (estas aplican siempre), y veríamos que, por ejemplo:

La medida op.pl.1 aplica a ambos sistemas, pero con dos intensidades (básica para el segundo sistema, muy alta para el segundo).

- En la página 23, encontraríamos el apartado 4.1.1 Análisis de riesgos [op.pl.1], que nos indica:
- Para el sistema de nivel bajo, las medidas a adoptar son:
 - Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:
 - a) Identifique los activos más valiosos del sistema.
 - b) Identifique las amenazas más probables.
 - c) Identifique las salvaguardas que protegen de dichas amenazas.
 - d) Identifique los principales riesgos residuales.

Cómo se consulta el Anexo II, de medidas de seguridad.

- Para el sistema de nivel alto, las medidas a adoptar son:
 - Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:
 - a) Identifique y valore cualitativamente los activos más valiosos del sistema.
 - b) Identifique y cuantifique las amenazas posibles.
 - c) Identifique las vulnerabilidades habilitantes de dichas amenazas.
 - d) Identifique y valore las salvaguardas adecuadas.
 - e) Identifique y valore el riesgo residual.

La auditoría consistirá en comprobar que se existe, para el sistema de nivel bajo, un documento en el que se identifiquen los elementos citados, y para el segundo, que se dispone de un sistema con las capacidades analíticas indicadas y que se ha aplicado a este sistema de información de forma adecuada.

05. Visión global de las medidas de seguridad.

Cómo se consulta el Anexo II, de medidas de seguridad.

En la medida Perímetro seguro, vemos que aplica el nivel básico para el sistema de nivel bajo, y capacidades incrementadas en el sistema de nivel alto.

Al consultar el apartado “5.4.1 Perímetro seguro [mp.com.1]”, obtenemos:

- Para el sistema de nivel bajo:
 - Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.
- Para el sistema de nivel alto.
 - a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.
 - b) Se dispondrán sistemas redundantes.

La auditoría consistirá en comprobar que existen los sistemas anteriores y que el tráfico de red pasa en su totalidad por ellos.

Guías de ayuda para las actividades bajo el ENS

minsait

06

An Indra company

31

06. Guías de ayuda para las actividades bajo el ENS.

Normas de Apoyo al ENS: CNI-CCN-STIC serie 800.

El CCN (Centro Criptológico Nacional) ha desarrollado un conjunto extenso de normas (disponibles en <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>).

Son un total de 55 normas, pero las siguientes son especialmente interesantes:

- CCN-STIC-**800** Glosario de términos y abreviaturas del ENS
- CCN-STIC-**801** Responsabilidades y Funciones en el ENS
- CCN-STIC-**802** Auditoría del ENS
- CCN-STIC-**803** Valoración de Sistemas en el ENS
- CCN-STIC-**804** ENS. Guía de implantación
- CCN-STIC-**805** Política de Seguridad de la Información
- CCN-STIC-**806** Plan de Adecuación al ENS
- CCN-STIC-**807** Criptología de empleo en el ENS
- CCN-STIC-**808** Verificación del cumplimiento de las medidas en el ENS
- CCN-STIC-**809** Declaración de conformidad con el ENS

06. Guías de ayuda para las actividades bajo el ENS.

Normas de Apoyo al ENS: CNI-CCN-STIC serie 800.

El CCN (Centro Criptológico Nacional) ha desarrollado un conjunto extenso de normas (disponibles en <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>).

Cabe destacar la publicación de la guía CCN-STIC 819 de Medidas Compensatorias, en octubre de 2018, donde se recogen una serie de medidas de seguridad alternativas cuando no sea posible la adecuada implantación de las medidas contempladas en el Anexo II del ENS, siempre y cuando se justifique documentalmente que protegen igual o mejor del riesgo sobre los activos y se satisfagan los principios básicos y los requisitos mínimos:

- CCN-STIC-**819** Medidas Compensatorias

Roles y responsabilidades en el ENS

minsait

07

An Indra company

34

Cuál es el modelo de roles y responsabilidades.

Para la definición de roles y responsabilidades, es conveniente consultar la Guía de Ayuda “CCN-STIC-801 Responsabilidades y Funciones en el ENS”

En su Art. 10, el R.D. 3/2010 indica que han de cumplirse los siguientes criterios:

- En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
- El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
- La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

07. Roles y responsabilidades en el ENS.

Cuál es el modelo de roles y responsabilidades.

CCN-STIC-801 profundiza en la definición anterior.

- Diferencia 3 grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, la operación del sistema de información que se atiene a aquellos requisitos y la función de supervisión de acuerdo al principio básico del ENS “La seguridad como función diferenciada”. La especificación de requisitos de seguridad corresponde a los responsables de la información y el servicio, junto con el responsable del fichero si hubiera datos de carácter personal. La operación corresponde al responsable del sistema. La supervisión corresponde al responsable de la seguridad.
- Puede que exista por encima de todos ellos un Comité de Seguridad Corporativa
- Puede que exista un Comité de Seguridad de la Información que aúne las responsabilidades sobre información y servicios.

07. Roles y responsabilidades en el ENS.

Cuál es el modelo de roles y responsabilidades.

CCN-STIC-801 profundiza en la definición anterior.

De existir un nivel de gobierno jerárquico en la organización (con Nivel 1 – Órganos de Gobierno; Nivel 2 – Dirección Ejecutiva y Nivel 3: Operacional, entonces:

- El Responsable de la Información estará en el nivel 1
- El Responsable de la Seguridad estará en el nivel 2.
- El Responsable del Sistema estará en el nivel 3.
- Cuando exista un Comité de Seguridad Corporativa, estará en el nivel 1.
- Cuando existe un Comité de Seguridad de la Información, estará en el nivel 1.

La seguridad orientada al riesgo: Análisis de riesgos

minsait

08

An Indra company

38

08. La seguridad orientada al riesgo: Análisis de riesgos.

El modelo de análisis de riesgos en el ENI.

La gestión de riesgos como actividad obligatoria del ENS.

El art. 6 del ENS señala como obligatorio, para todos los sistemas afectados por el ENS, el desarrollo de un Análisis de Riesgos, al que deberá seguir el correspondiente proceso de Gestión de Riesgos (art. 13).

- *Artículo 13. Análisis y gestión de los riesgos.*
 - *1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.*
 - *2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.*
 - *3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.*

08. La seguridad orientada al riesgo: Análisis de riesgos.

Tipos de Análisis de Riesgos.

Análisis y la Gestión de Riesgos son la base de la Seguridad TIC. Las Directrices de seguridad de la OCDE, las normas internacionales ISO/IEC 27001/27002, las normas NIST, etc., todas ellas sustentan su aplicación a un preceptivo análisis y ulterior gestión de riesgos.

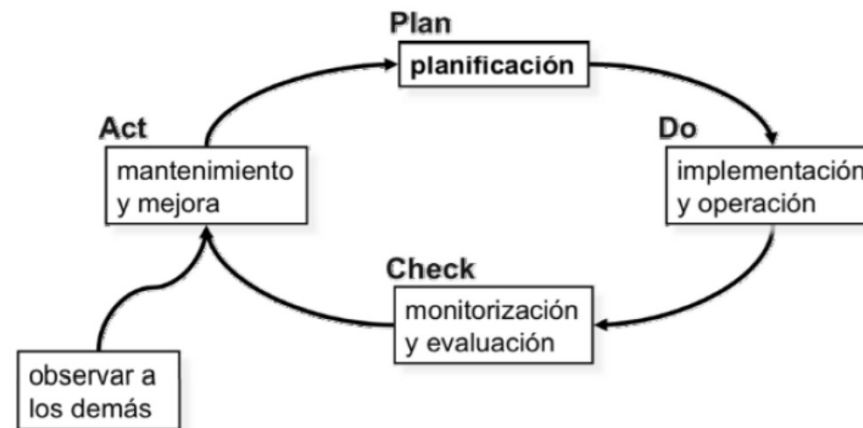
Dentro de la Administración Pública española existe una metodología específica para el análisis de riesgos (Magerit). No obstante, en el contexto del ENS sería posible utilizar cualquier otra internacionalmente reconocida (por ejemplo, ISO/IEC 27001/27002).

08. La seguridad orientada al riesgo: Análisis de riesgos.

Un ejemplo: Magerit.

Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología de análisis de riesgos tradicionalmente utilizada dentro de la Administración Pública a nivel nacional. Puede encontrarse en <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>. Habitualmente se utiliza junto con una herramienta llamada Pilar, pero esto no es necesario.

Magerit (como la mayoría de las metodologías de gestión de riesgos, se basa en un planteamiento de análisis continuo del riesgo, en base al modelo conocido como PDCA (Plan, Do, Check, Act)



Gestión de los riesgos: El Plan de acción

minsait

09

An Indra company

42

Idea general de gestión del riesgo.

Una vez valorado el riesgo, se hace necesario proceder a tratar éste para que alcance unos niveles adecuados. Existen las siguientes alternativas básicas

- Evitar o eliminar el riesgo: por ejemplo sustituyendo el activo por otro que no se vea afectado por la amenaza o eliminando la actividad que lo produce.
- Reducirlo o mitigarlo: tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:
 - reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas
 - reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas.
- Transferirlo, compartirlo o asignarlo a terceros: en ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.
- Aceptarlo: se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la organización no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada

El concepto de plan de acción.

El plan de acción o plan de tratamiento del riesgo es el resultado de la valoración del riesgo más el análisis indicado relativo a cómo acometer aquellos niveles de riesgo que se consideren excesivos.

- Debe tenerse en cuenta que el Plan de Acción no está directamente ligado a la adopción de las medidas de seguridad marcadas en el Anexo II del R.D. 3/2010. Por ejemplo, puede suceder que una organización no esté capacitada para implementar alguna de las medidas (por ejemplo, por coste o por complejidad), o que se determine una probabilidad elevada de que los controles puedan no estar debidamente implementados (por ejemplo, si por problemas de rotación o falta de disponibilidad de personal externo, no resulta posible garantizar medidas de formación requeridas por el Anexo II).
- En ese caso, podría optarse por transferir el riesgo (por ejemplo, mediante el uso de servicios comunes de la AGE, soporte de sistemas de la Diputación o la Xunta, etc.).
- También podría optarse por la sustitución de un sistema de información por otro, o por la externalización completa del mismo (por ejemplo, contratando un modelo cloud, si fuese posible).

Metodología de análisis y gestión de riesgos
empleada en la Diputación

Normativa y procedimientos de seguridad
existentes

minsait

10

11

Entre los años 2016 y 2018 la Diputación de A Coruña aborda la adecuación al ENS y RGPD de forma global, a través de la licitación de sendos contratos:

- **IMPLANTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN LA DIPUTACIÓN DE A CORUÑA:**

<https://www.dacoruna.gal/licitacion/licitacion/2074184>

Su objetivo se centró en la implantación del Esquema Nacional de Seguridad en los sistemas de información de la Diputación de A Coruña, estableciendo la política de seguridad en la utilización de medios electrónicos y los principios básicos y requisitos mínimos que permitan una protección adecuada de la información en el ámbito de la administración electrónica de la Diputación de A Coruña.

Su ejecución se ha dividido en dos fases:

1. Análisis, planificación y redacción de planes de adecuación
2. Implantación de las medidas y puesta en marcha

Esta licitación está ya finalizada y como resultado, se aprobó en el Pleno de la Diputación las Políticas de Seguridad de la Información, publicadas en el Portal de Transparencia de la Diputación de A Coruña

Metodología de Análisis y Gestión de Riesgos. Normativa y Procedimientos

En este momento se está llevando a cabo una auditoría para evaluar el grado de cumplimiento en la implantación de las medidas propuestas.

- SERVIZOS DE SOPORTE NA ANÁLISE DO CUMPRIMENTO DO ESQUEMA NACIONAL DE INTEROPERABILIDAD (ENI) E NA ADECUACIÓN AO NOVO REGULAMENTO EUROPEO DE PROTECCIÓN DE DATOS:

<https://www.dacoruna.gal/licitacion/licitacion/3146716>

Este proyecto se encuentra en fase de ejecución y sus dos objetivos principales se centran en:

1. Disponer de un análisis inicial de cumplimiento legal en relación al ENI.
2. Prestar soporte para el proceso de adecuación al RGPD.

Ingeniería social

minsait

12

An Indra company

48

Concepto de Ingeniería Social.

En el contexto de la seguridad de información, ingeniería social se refiere a la manipulación psicológica de las personas para conseguir que realicen acciones o divulguen información confidencial. Es un modo de “abuso basado en confianza, y puede involucrar redes de influencia y acciones de captura de información muy complejas.

La ingeniería social puede ir desde aspectos simples tales como hacerse pasar por alguien para conseguir un cambio de contraseña, o complejos como influir sobre personas cercanas a alguien (o incluso amenazas directas)

Aunque pueda parecer simple o inocente, hay que tener en cuenta que algunos de los actos de “hacking” más sofisticados de la historia están relacionados con la Ingeniería Social:

- El hacker más famoso de la historia (condenado por un juez de EEUU) a escribir varios libros contando sus métodos y a colaborar con el FBI, usaba fundamentalmente técnicas de ingeniería social (llegaba, mediante contactos múltiples, conocer detalles de una organización y para finalmente convencer a los técnicos de soporte de que le dejaran acceso a sistemas).
- El phishing es una técnica simple que consiste en hacerse pasar por un banco para solicitar la cuenta... y ha sido históricamente una de las técnicas de mayor éxito

Concepto de Ingeniería Social.

En el contexto de la seguridad de información, ingeniería social se refiere a la manipulación psicológica de las personas para conseguir que realicen acciones o divulguen información confidencial. Es un modo de “abuso basado en confianza, y puede involucrar redes de influencia y acciones de captura de información muy complejas.

La ingeniería social puede ir desde aspectos simples tales como hacerse pasar por alguien para conseguir un cambio de contraseña, o complejos como influir sobre personas cercanas a alguien (o incluso amenazas directas)

Aunque pueda parecer simple o inocente, hay que tener en cuenta que algunos de los actos de “hacking” más sofisticados de la historia están relacionados con la Ingeniería Social:

- El hacker más famoso de la historia (condenado por un juez de EEUU) a escribir varios libros contando sus métodos y a colaborar con el FBI, usaba fundamentalmente técnicas de ingeniería social (llegaba, mediante contactos múltiples, conocer detalles de una organización y para finalmente convencer a los técnicos de soporte de que le dejaran acceso a sistemas).
- El phishing es una técnica simple que consiste en hacerse pasar por un banco para solicitar la cuenta... y ha sido históricamente una de las técnicas de mayor éxito

Concepto de Ingeniería Social.

- Mecanismos simples como hacerse pasar por “técnico de soporte” y llamar a personas al azar en una organización (y, si se encuentra a alguien con un problema, resolvérselo y luego pedirle que haga una prueba) funcionan sorprendentemente bien.
- Un método que funciona increíblemente bien es buscar páginas web que una persona utilice habitualmente (por ejemplo, mirando casualmente a su ordenador, o sacando conversación casualmente) y luego mandar un mensaje de verificación supuestamente desde ese site web pidiendo que clique una página (lo que provoca que se instale un software troyano, por ejemplo).

12. Ingeniería social

Algunos métodos para luchar contra la ingeniería social.

- Definición de un modelo estricto para el soporte informático.
- Formación al personal sobre phishing u otros modelos de ataque similares
- Impedir la instalación de software (especialmente plugins en navegadores y otro software similar)
- Definir un modelo de respuesta ante sospechas (por ejemplo, que el personal pueda consultar fácilmente si un correo sospechoso es fraudulento o legítimo)

Sofisticación del cibercrimen

minsait

13

An Indra company

53

Algunos ejemplos de cibercrimen.

- **WannaCry:** pseudo - Ransomware propagado por un gusano informático, que aprovechaba una vulnerabilidad de windows. Encriptaba todos los archivos de servidores corporativos, y reclamaba el envío de un rescate en bitcoins (pero aunque se enviaba una clave, no servía para reparar el daño). Destruyó una cantidad importante de información en el NHS (el servicio sanitario público británico), y provocó que el mayor fabricante de semiconductores del mundo (TSMC de Taiwan) parase sus instalaciones durante varios días.
- **Petya (y NonPetya):** Apareció en Ucrania e infectó (y se propagó) usando un software de declaración de la renta de Ucrania. Opera de una forma similar (pero más sofisticada) que Wannacry. Es también un pseudo – ransomware, orientado a Windows. Provocó una disrupción masiva de las operaciones de transporte de la mayor compañía naviera del mundo (Maersk, de Dinamarca), entre muchas otras.
- **Stutnex:** aunque algo más antiguo (apareció en 2010), fue particularmente destructivo. Ataca exclusivamente a ordenadores con software de control industrial instalado. En un ataque en Irán, destruyó (enviando los comandos adecuados) todas las centrifugadoras de enriquecimiento de uranio (en una de las instalaciones más vigiladas del mundo). Destruyó más de 1000 instancias de maquinaria industrial en el mundo. Se cree que fue creado (o al menos lanzado en Irán) por una operación conjunta CIA - Israel

¡Gracias!

minsait



Deputación
DA CORUÑA

An Indra company

minsait

Mark Making the way forward

An Indra company