ISEC Labs #10

Esquema Nacional de Seguridad

Javier Moreno
jmoreno<arroba>isecauditors.com

1. Introducción

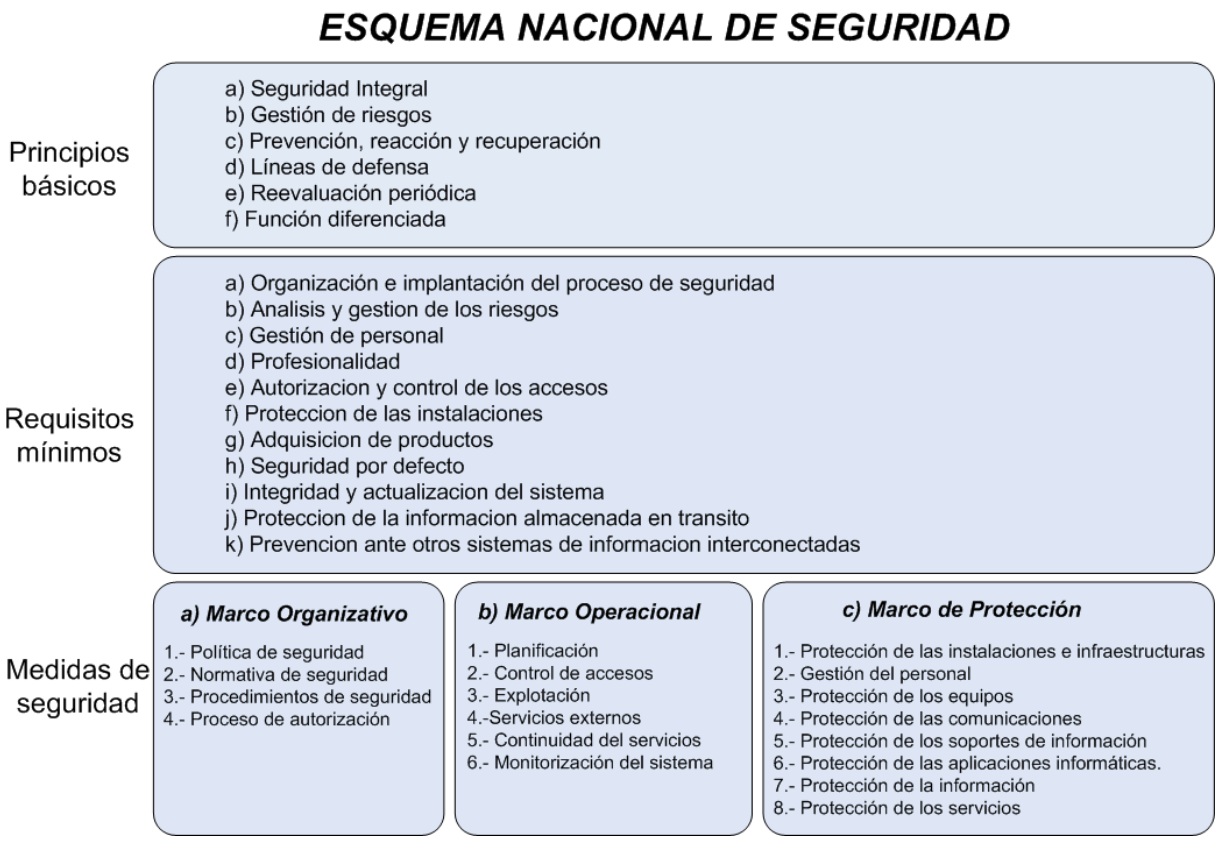
La utilización de medios electrónicos en las comunicaciones es cada vez más frecuente en la sociedad actual. El correo ordinario, el teléfono o incluso las reuniones presenciales están siendo sustituidos por el correo electrónico, por Internet, por la voz sobre IP, por videoconferencias o simplemente por un formulario HTML de recogida de información.

Las Administraciones Públicas no han querido quedarse atrás en este aspecto y están implantando los medios necesarios para permitir la comunicación electrónica de los ciudadanos con las distintas entidades locales, autonómicas y estatales. La ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) [1] se encarga de regular este derecho de los ciudadanos.

La generalización de la relación electrónica de los ciudadanos con la administración pública depende, en gran medida, de la confianza que la Administración sea capaz de generar en los ciudadanos. La propia LAECSP en su artículo 42.2 enuncia la importancia de garantizar la seguridad en la utilización de los medios electrónicos para comunicar a los ciudadanos con la administración y exige la creación de un Esquema Nacional de Seguridad (ENS).

Según este artículo 42.2 de la LAECSP, el "Esquema Nacional de Seguridad tiene por objetivo establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente ley -la LAECSP- y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información".

Por lo tanto, el Esquema Nacional de Seguridad [2] es una relación de principios básicos, requisitos mínimos y medidas de seguridad que las administraciones públicas deben aplicar en sus procesos y sistemas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos e informaciones utilizados en medios electrónicos que gestionan dentro de sus competencias para generar la confianza necesaria en la comunicación entre los ciudadanos y las administraciones públicas.



Los elementos principales del Esquema Nacional de Seguridad son los siguientes:

- Principios Básicos
- Requisitos Mínimos
- Categorización de los sistemas
- Auditoria de Seguridad
- Respuesta a Incidentes
- Certificación

En los siguientes apartados se desgranará cada uno de estos elementos señalando las principales características de los mismos y como deben ser aplicados por las administraciones públicas.

2. Principios básicos

El ENS establece seis principios básicos sobre los que se sustenta todo el texto y sobre los cuales las Administraciones Públicas deberán desplegar sus acciones relativas a la Seguridad de la Información.

Los seis principios básicos son los siguientes:

- **Seguridad Integral**: La seguridad de la información debe ser entendida como un proceso integral que incluya a los elementos técnicos, humanos, materiales y organizativos. En este punto también se destaca la importancia de la concienciación de las persona.
- **Gestión de Riesgos**: El ENS destaca el análisis y la gestión de riesgos como parte importante del proceso de seguridad. Una correcta gestión de riesgos permite mantener un entorno controlado minimizando los riesgos hasta los niveles identificados como aceptables.
- **Prevención, reacción y recuperación**: La seguridad de los sistemas deben contemplar tres aspectos fundamentales:
    a. Medidas de Protección: Reducir la posibilidad de que las amenazas se materialicen. Estas medidas incluirán la disuasión así como la disminución del ámbito de exposición.
    b. Medidas de Reacción: Atajar los incidentes de seguridad en el tiempo.
    c. Medidas de Recuperación: Restaurar la información y los servicios después de un incidente.
- **Líneas defensa**: El ENS señala la defensa en profundidad o defensa en capas como uno de los factores (organizativos, físicos y/o lógicos) más importantes dentro de una entidad. Esta defensa basada en niveles debe actuar de forma que cuando una de las capas falle, permita:
    a. Ganar tiempo para una reacción adecuada.
    b. Evitar que el incidente afecte al sistema completo.
    c. Minimizar el impacto final.
- **Reevaluación periódica**: El esquema nacional de seguridad indica que las medidas de seguridad deben ser revisadas de forma periódica con el objetivo de adaptar los sistemas y las medidas de protección a la constante evolución de las amenazas.
- **Función diferenciada**: En el último de los principios básicos extiende la importante diferenciación de roles y funciones entre el responsable de la información, el responsable del servicio y el responsable de la seguridad. Los responsables de la información y del servicio son los que determinan, respectivamente, los requisitos de la información y del servicio. El responsable de la seguridad es el responsable de satisfacer las necesidades de seguridad de la información y de los servicios.

3. Requisitos mínimos

En el capítulo II del Esquema Nacional de Seguridad se requiere a las Administraciones Públicas disponer de una Política de Seguridad. Esa política de seguridad se debe desarrollar aplicando una serie de requisitos mínimos:

El acceso a los sistemas deberá ser controlado, limitándose el mismo a usuarios, sistemas o procesos que hayan sido debidamente autorizados.

Los sistemas se instalaran en salas aisladas, separadas, con control de acceso y de llaves.

Los sistemas deberán ser diseñados de forma que garanticen la seguridad por defecto:

Los sistemas de información deben protegerse de su perímetro especialmente si están conectados a redes públicas. Se deben analizar los riesgos derivados de la interconexión de los sistemas con otros sistemas no confiables o con confianza desconocida.

Los sistemas de información deben registrar las actividades realizadas por cada usuario con el objetivo de monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas.

Los sistemas dispondrán de sistemas de copias de seguridad para garantizar la continuidad de las operaciones.

El proceso de seguridad se la información debe ser actualizado y mejorado de forma continua para lo cual se aplicaran normativas internacionales de gestión de tecnologías de la información.

1. **Organización e implantación del proceso de seguridad**
    1. La seguridad afecta a todos los miembros de la organización.
    2. La política de seguridad identificará a los responsables de la seguridad de la información.
    3. Todos los miembros de la organización deben conocer la política de seguridad.
2. **Análisis y gestión del riesgos**
    1. Se debe realizar una correcta gestión de riesgos.
    2. A efectos de realizar esa gestión de riesgos se realizará un análisis de riesgos basado en alguna metodología de reconocido prestigio internacional.
3. **Gestión de personal**
    1. Todo el personal relacionado con la información y/o con los sistemas deberá estar formado en materia de seguridad.
    2. El alcance del uso seguro de los sistemas se reflejará en unas normas de seguridad.
    3. Cada usuario que acceda a un sistema debe estar identificado de forma única con el objetivo de quién ha realizado qué actividad.
4. **Profesionalidad**
    1. La seguridad de los sistemas estará atendida por personal cualificado, dedicado e instruido
    2. El personal recibirá la formación necesaria para garantizar la seguridad de las tecnologías de la información en la Administración correspondiente.
    3. Las Administraciones Públicas exigirán que las entidades que les presten servicios cuenten con los niveles de madurez en seguridad idóneos.
5. **Autorización y control de los accesos**
6. **Protección de las instalaciones**
7. **Adquisición de productos**
    1. En la adquisición de los productos de seguridad que vayan a ser utilizados por las Administraciones Públicas se valorara positivamente aquellos que estén certificados de acuerdo con las normas y estándares de mayor reconocimiento internacional.
    2. El Organismo de Certificación del Esquema Nacional de Seguridad de Evaluación y Certificación de Seguridad de las Tecnologías de Información, determinara el criterio a cumplir en función del uso previsto del producto.
8. **Seguridad por defecto**
    1. El sistema proporcionara la mínima funcionalidad requerida.
    2. Las funciones de administración serán las mínimas necesarias
    3. Se eliminaran o desactivaran las funciones innecesarias.
    4. El uso del sistema ha de ser sencillo y seguro.

9. **Integridad y actualización del sistema.**
    1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación.
    2. En todo momento se deberá conocer el estado de la seguridad de los sistemas en relación sobre todo a vulnerabilidades o actualizaciones que pudieran afectarles.
10. **Protección de la información almacenada y en tránsito**
    1. El ENS define como entornos inseguros a los equipos portátiles, asistentes personales (PDAs), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o de cifrado débil.
    2. Las administraciones públicas deben prestar especial atención a la información almacenada o en tránsito a través de entornos inseguros.
    3. La seguridad debe incluir los procedimientos de recuperación y conservación de los documentos electrónicos.
    4. Aquella información reflejada en medios no electrónicos, pero que haya sido causa o consecuencia de información electrónica, se protegerá con el mismo grado de seguridad que ésta.
11. **Prevención ante otros sistemas de información interconectados**
12. **Registro de actividad**
13. **Incidentes de seguridad**
    1. Se establecerá un sistema de detección y reacción frente a incidentes de seguridad.
    2. Estos incidentes deben registrarse de cara a la mejora continua de la seguridad de la información.
14. **Continuidad de la actividad**
15. **Mejora continua del proceso de seguridad**

4. Categorización de los sistemas

El ENS indica que los sistemas de información y servicios de las Administraciones Públicas deben ser clasificados en categorías. Existen tres categorías: ALTA, MEDIA y BAJA. Esta clasificación permitirá conocer qué medidas de seguridad deben ser aplicadas a cada sistema de información o servicio. El artículo 43 y el Anexo I del Esquema Nacional de Seguridad describen como calcular la categoría en la que se incluirían cada uno de los sistemas de las administraciones públicas.

A la hora de categorizar los sistemas de información de las Administraciones Públicas hay tres conceptos fundamentales:

1. Dimensiones de Seguridad
2. Niveles de las Dimensiones de Seguridad
3. Categoría de un sistema de información

4.1 Dimensiones de Seguridad

A la hora de establecer la categoría de un sistema de información o de un servicio, se tendrá en cuenta cinco dimensiones de la seguridad, es decir, cada activo de una administración pública puede verse afectado por una o más dimensiones de seguridad. Estas dimensiones de seguridad son las siguientes:

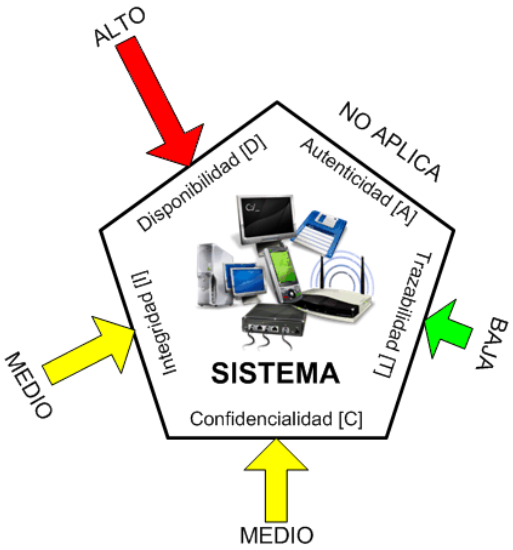
- Disponibilidad [D]
- Autenticidad [A]
- Integridad [I]
- Confidencialidad [C]
- Trazabilidad [T]

4.2 Niveles de las dimensiones de seguridad

El siguiente paso es calcular el grado o nivel en el que una dimensión de seguridad se ve afectada por la ocurrencia de un incidente de seguridad.

El grado de afectación de un incidente de seguridad a una dimensión de seguridad de un activo se adscribe a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada por un incidente, no se adscribe a ningún nivel.

1. Nivel BAJO: Se aplica cuando un incidente de seguridad que afecte a alguna de las dimensiones supone un perjuicio limitado sobre las funciones de la organización, sus activos o sobre los individuos afectados.
2. Nivel MEDIO: Se aplica cuando un incidente de seguridad que afecte a alguna de las dimensiones supone un perjuicio grave sobre las funciones de la organización, sus activos o sobre los individuos afectados.
3. Nivel ALTO: Se aplica cuando un incidente de seguridad que afecte a alguna de las dimensiones supone un perjuicio muy grave sobre las funciones de la organización, sus activos o sobre los individuos afectados



4.3 Determinación de la categoría de un sistema

A la hora de determinar la categoría de un sistema de información se tendrá en cuenta los siguientes criterios:

1. Un sistema de información será de categoría ALTA, si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
2. Un sistema de información será de categoría MEDIA, si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
3. Un sistema de información será de categoría BÁSICA, si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

4.4 Medidas de seguridad

Las AA.PP. deben cumplir los requisitos mínimos detallados en el apartado Requisitos mínimos dentro de este mismo documento, para lo cual deben aplicar una serie de medidas de seguridad.

Estas medidas de seguridad están clasificadas en tres grupos:

1. Marco organizativo [org]: Medidas de seguridad relacionadas con la organización global de la seguridad.
2. Marco operacional [op]: Medidas para proteger la operación del sistema como conjunto integral de componentes para un fin.
3. Medidas de protección [mp]: Protección de activos en concreto, según su naturaleza.

En el Anexo II del ENS se presentan unas tablas que permiten conocer a partir del nivel de clasificación de los niveles de seguridad de cada activo, que medidas de seguridad se debe aplicar a ese activo en concreto. Esas tablas se presentan a continuación:

Dimensiones Afectadas	B	M	A	MEDIDAS DE SEGURIDAD	
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

5. Metodología de la implantación

A modo de resumen de cómo desarrollar un proceso de implantación o cumplimiento del ENS, este se puede desarrollar en las siguientes Etapas de cara a seleccionar las medidas de seguridad a un activo en concreto de la forma más eficiente:

- **Etapa I**: Identificación de los tipos de activos presentes.
- **Etapa II**: Determinación de las dimensiones de seguridad relevantes para cada activo (ver apartado: Dimensiones de seguridad)
- **Etapa III**: Determinación del nivel correspondiente de cada dimensión de seguridad (ver apartado Niveles de las dimensiones de seguridad)
- **Etapa IV**: Determinar la categoría del sistema (ver apartado Determinación de la categoría de un sistema)
- **Etapa V**: Selección de las medidas de seguridad apropiadas (ver apartado: Medidas de seguridad).

Para facilitar las actividades de implantación, el CCN-CERT [3] (Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN)) organismo encargado, entre otras tareas, de la gestión del ENS, ha publicado recientemente una herramienta que ayuda a obtener las medidas de seguridad que se deben aplicar a un activo

dado a partir de las dimensiones de seguridad asignadas al activo y sus niveles de seguridad correspondientes. Esta herramienta Java puede ser descargada en el siguiente enlace: https://www.ccn-cert.cni.es/publico/ens/controles.exe.

5.1 Ejemplo de medidas de seguridad a aplicar a un activo

A continuación se detallan un ejemplo de cómo calcular las medidas de seguridad requeridas por ENS para un activo de una administración pública: la Página Web de un Ayuntamiento.

Etapa I: Las características de este activo son las siguientes

- Página web estática desarrollada en HTML, CSS y JavaScript.
- Implantada en un servidor web ubicada en las propias instalaciones del cliente.
- Consta con una única dirección IP pública que la permite sea accesible desde Internet.
- No intercambia información con ninguna base de datos.
- Es un website puramente informativo.

Etapa II: Establecemos que las dimensiones de seguridad que aplican a este activo son las siguientes:

- **Disponibilidad**: Aplica. La página web tiene que estar disponible en 24x7.
- **Autenticidad**: Aplica. El usuario quiere tener constancia de que está accediendo a la página web oficial de una administración en concreto.
- **Integridad**: Aplica. Los cambios que se produzcan en la aplicación deben ser únicamente los autorizados.
- **Confidencialidad**: No aplica. La página es completamente pública. No existen áreas con datos confidenciales o privados.
- **Trazabilidad**: No aplica. No es posible registrase en la página web por lo que no nos interesa la posibilidad de monitorizar o registrar las acciones realizadas por los usuarios.

Etapa III: Asignamos un nivel a cada dimensión según como se verían afectadas estas dimensiones ante la ocurrencia de un incidente de seguridad. De este modo, asignamos los siguientes niveles a las dimensiones:

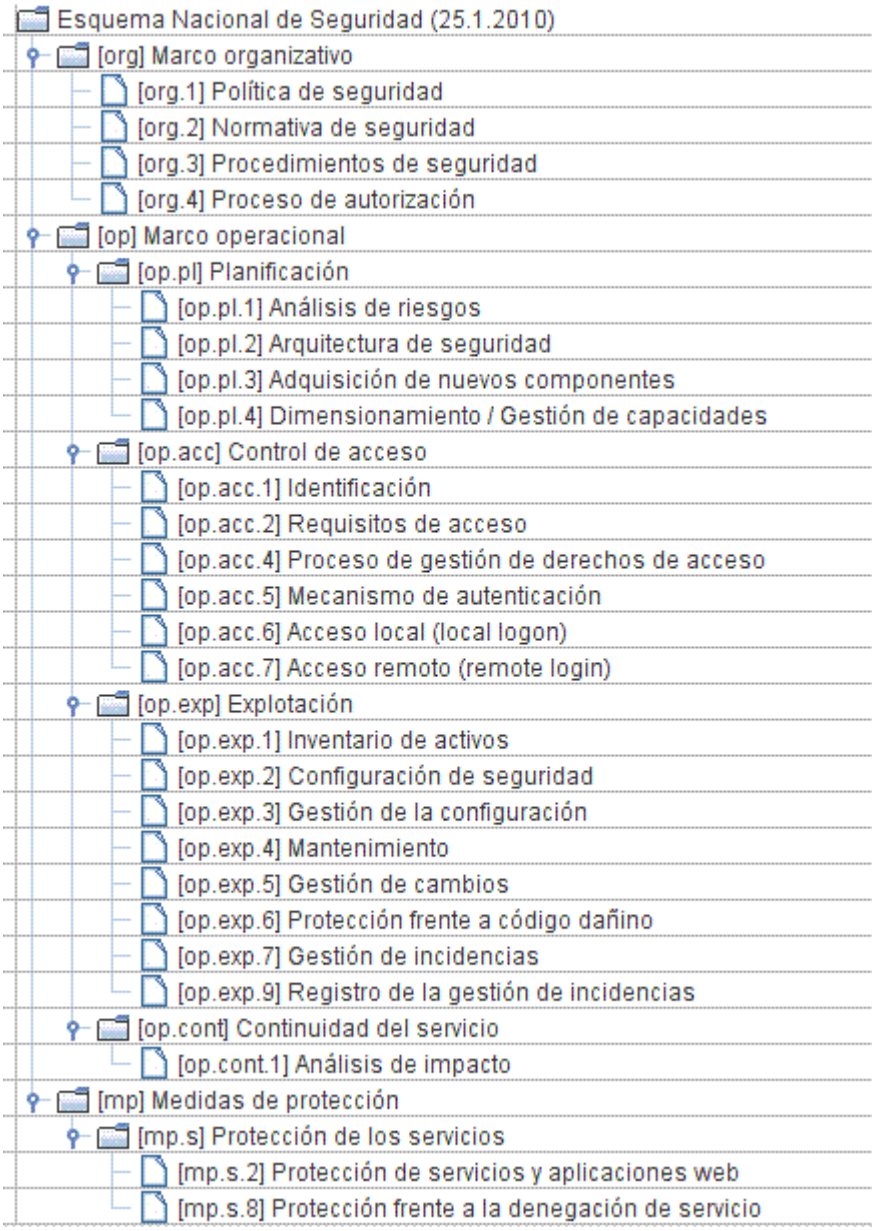
- **Disponibilidad:** Medio. Entendiendo que un incidente de seguridad que ocurriera sobre la página web provoca un prejuicio grave sobre la disponibilidad de la página web.
- **Autenticidad:** Bajo. Entendiendo que un incidente de seguridad que ocurriera sobre la página web provoca un prejuicio limitado sobre la autenticidad de la página web.
- **Integridad:** A Bajo. Entendiendo que un incidente de seguridad que ocurriera sobre la página web provoca un prejuicio limitado sobre la disponibilidad de la página web.

Etapa IV: Determinar la categoría del sistema:

El sistema es de categoría MEDIA porque al menos una de sus dimensiones de seguridad está catalogada como de nivel MEDIO y ninguna de sus dimensiones alcanza un nivel superior.

Etapa V: Seleccionar las medidas de protección a aplicar.

Utilizando la herramienta proporcionada por el CCN-CERT se obtiene que las medidas de seguridad a aplicar fueran las siguientes:



Al final del Anexo II del ENS se detallan las características de las medidas de seguridad a emplear así como las funciones que deben cubrir y las metodologías para llevarlas a cabo.

A continuación, se han seleccionado las medidas de seguridad más representativas que deben ser aplicadas a la página web de este ayuntamiento de ejemplo así como la forma que marca el ENS para llevarlas a cabo:

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que detallen de forma clara y precisa:

a) Cómo llevar a cabo las tareas habituales.
b) Quién debe hacer cada tarea.
c) Cómo identificar y reportar comportamientos anómalos.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

a) Documentación de las instalaciones:

1.º Áreas.
2.º Puntos de acceso.

b) Documentación del sistema:

1.º Equipos.
2.º Redes internas y conexiones al exterior.
3.º Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:

1.º Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet.
2.º Cortafuegos, DMZ, etc.
3.º Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:

1.º Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
2.º Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

e) Controles técnicos internos:

1.º Validación de datos de entrada, salida y datos intermedios.

f) Sistema de gestión con actualización y aprobación periódica.

4.2.5 Mecanismo de autenticación [op.acc.5].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen.
Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados a cada nivel.

Nivel BAJO

a) Se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, o dispositivos físicos (en expresión inglesa »tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.
b) En el caso de usar contraseñas se aplicarán reglas básicas de calidad de las mismas.
c) Se atenderá a la seguridad de los autenticadores de forma que:

1.º Los autenticadores se activarán una vez estén bajo el control efectivo del usuario.
2.º Los autenticadores estarán bajo el control exclusivo del usuario.
3.º El usuario reconocerá que los ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4.º Los autenticadores se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5.º Los autenticadores se retirarán y serán deshabilitados cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware».
Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
2.º Se prevendrán ataques de manipulación de URL.
3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».
4.º Se prevendrán ataques de inyección de código.

b) Se prevendrán intentos de escalado de privilegios.
c) Se prevendrán ataques de «cross site scripting».
d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».

- Procedimientos de seguridad (marco organizativo)
- Arquitectura de Seguridad (marco operacional – planificación)
- Mecanismo de Autenticación (marco operacional – control de acceso)
- Protección frente a código dañino (marco operacional – explotación)
- Protección de servicios y aplicaciones web (medidas de protección – protección de los servicios)

6. Auditoría de seguridad

Los sistemas de información de las AA.PP. tienen que ser objeto de auditoría al menos cada dos años con el objetivo de verificar su correcta adecuación al Esquema Nacional de Seguridad.

Además se debe realizar esa auditoría cada vez que se produzcan modificaciones sustanciales en el sistema de información correspondiente ya que estos cambios pueden afectar a las medidas de seguridad correspondientes.

Estas auditorías se realizarán basándose en la categoría en la que hay sido clasificada el sistema. Así mismo las auditorias estarán basadas en normativas de reconocido prestigio nacional e internacional. El Esquema Nacional de Seguridad en su Anexo III detalla unas pautas sobre el objetivo y alcance de estas auditorías destacando la seguridad de los sistemas de información será auditada den los siguientes términos:

a. La política de seguridad debe definir los roles y funciones de los responsables de la información, los servicios, los activos la seguridad de los sistemas de información.
b. Debe comprobarse que existen procedimientos para la resolución de conflictos entre responsables.
c. La asignación de roles a las personas se ha realizado bajo el principio de separación de funciones.
d. Se ha realizado un análisis de riesgos que debe ser revisado y aprobado anualmente
e. Se cumplen las medidas de seguridad detalladas en el Esquema Nacional de Seguridad.
f. Existe un sistema de gestión de la seguridad de la información

El informe resultado de las auditorias deber incluir el detalle sobre el grado de cumplimiento del esquema nacional de seguridad, las posibles deficiencias encontradas así como las recomendaciones para solventar dichas deficiencias.

7. Plazos para la adecuación

Según indica el Esquema Nacional de Seguridad todos los sistemas de información que se implanten en las administraciones públicas tienen que seguir las directrices marcadas por el real decreto.

Los sistemas existentes a la entrada en vigor del real decreto (Enero de 2010) se deben adecuar a los requisitos recogidos en el Esquema Nacional de Seguridad. Si a los doce meses de la entrada en vigor del ENS, alguna administración pública no ha podido aplicar los requisitos del ENS a sus sistemas de información, debe al menos disponer de un plan de adecuación que marque los plazos de ejecución, los cuales no podrán superar en ningún caso los 48 meses.

En resumen, todas las Administraciones Públicas deben:

1. Para los sistemas nuevos, recoger el ENS desde sus diseños iniciales.
2. Para los sistemas existentes antes del 29 de Enero de 2010, adaptarlos a los requisitos del ENS o al menos crear un Plan de Adecuación que planifique las acciones a realizar para cumplir con el ENS. Cualquiera de estas dos acciones debe ser realizada antes del 29 de Enero de 2011.

8. Referencias

[1] Real Decreto 11/2007. Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
Accesible en: https://boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2007-12352
[2] Real Decreto 3/2010. Esquema Nacional de Seguridad.
Accesible en: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-1330
[3] CCN-CERT. (Capacidad de Respuesta ante Incidentes del Centro Critptológico Nacional).
Accesible en: https://www.ccn-cert.cni.es/