Guía de Seguridad de las TIC
CCN-STIC 883

Guía de Implantación del ENS para Entidades Locales

Mayo 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.05.28 11:00:28 +02'00'

NIPO: 083-19-183-2

Fecha de Edición: mayo de 2019

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

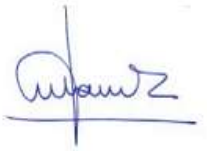
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

La confianza es la base de la sociedad actual. Confianza en nuestras instituciones, en nuestras infraestructuras, en nuestro sistema sanitario, en nuestros cuerpos y fuerzas de seguridad del Estado, en nuestra administración. El mundo de internet no ha de ser una excepción y el Esquema Nacional de Seguridad (ENS) nace para establecer una base de seguridad buscando garantizar que los sistemas gestionados bajo sus directrices, esto es la Administración Electrónica, están adecuadamente salvaguardados.

El ENS ayuda a crear y estandarizar unas condiciones de seguridad que, enfocadas a generalizar la confianza en el uso de los medios electrónicos, a través de medidas e indicadores que, implantados, mejoran la seguridad de los servicios, los sistemas, las comunicaciones, y en definitiva los datos y la información gestionada. Todo ello redunda en la confianza de la ciudadanía y los empleados públicos para el uso de la Administración Electrónica.

Los servicios proporcionados a través de la Administración Electrónica, basados principalmente en aplicaciones, sistemas y comunicaciones deben tener la capacidad adecuada para mantener un nivel de servicio proporcional a la importancia del servicio prestado. Los incidentes, las acciones ilícitas o malintencionadas que comprometan los fundamentos de la seguridad (disponibilidad, integridad, confidencialidad) de los datos almacenados o transmitidos deben poder ser gestionados para evitar o minimizar su impacto. El Esquema Nacional de Seguridad nos ayuda en esa tarea.

Hasta hace muy poco, el mundo físico se correspondía con el mundo real. Esta es la primera generación donde el mundo real se ve afectado, además, por el mundo virtual. Así que debemos ser conscientes que aquellas acciones que llevemos a cabo en el mundo virtual pueden tener repercusión en el mundo real y muy probablemente en el mundo físico.

Esta es una aproximación al tema de la ciberseguridad que nos parece relevante porque busca concienciar y sensibilizar como paso previo y necesario para poder acceder a un punto de partida que nos permita influir en las personas que debemos asimilar y formarnos sobre cómo debemos comportarnos cuando accedemos al mundo virtual.

A las Entidades Públicas y a las empresas aún queda otro paso más. Conformar un comportamiento colectivo de aquellos empleados que acceden al mundo virtual desde sus respectivas organizaciones para que no pongan en riesgo los activos la propia entidad. Dicho de otra manera, un desarrollo de comportamiento colectivo que permita garantizar que los activos que gestionan (datos de los ciudadanos entre otros) en el mundo virtual están salvaguardados de miradas ajenas.

2. OBJETIVO Y ALCANCE DE LA GUÍA

Uno de los objetivos principales de esta Guía es ayudar a enfocar los esfuerzos, indicando los pasos necesarios para adoptar las medidas adecuadas dentro de nuestra organización que permitan asegurar la gestión de la seguridad de la información.

Esta guía desarrolla las etapas de un plan que establece con precisión la secuencia de pasos para alcanzar la órbita de Cumplimiento del ENS, aplicando para ello una metodología que prioriza la obtención de resultados y la agilidad para gestionar la seguridad de la tecnología.

3. Claves para implantar el ENS en Ayuntamientos

El Esquema Nacional de Seguridad deben cumplirlo todas las Entidades Públicas independientemente del tamaño que tengan. Así debe implementarlo igualmente un Ministerio, una Comunidad Autónoma o un Ayuntamiento de 100 habitantes, habiendo entre todos ellos diferencias de mucha consideración.

Así que, teniendo en cuenta que el fin último de todos ellos debe ser el cumplimiento de la ley, bien es cierto que debemos adaptar su cumplimiento en función de algunos factores que podemos adelantar ahora y que condicionarán la implantación del ENS en cada uno de los organismos: Organización, servicio, información y tecnología.

En los siguientes apartados, basada en la experiencia y en una metodología de trabajo con implantaciones llevadas a cabo con éxito, se han desarrollado varias claves para facilitar el cumplimiento en Entidades Locales.

3.1 La seguridad sin Responsable de Seguridad

Es seguramente unas de las mayores dificultades a las que se enfrentan los Ayuntamientos ¿Cómo abordar la implantación y gestión de la seguridad sin contar con una persona enfocada y dedicada, al menos parcialmente, al ámbito de la seguridad de la información?

Sea como sea, esa situación es complicado que cambie en el corto y medio plazo. La Metodología Ágil de Adaptación Continua (MADAC) propone una manera de trabajar que ayuda a gestionar esa circunstancia y permite avanzar facilitando que la entidad sea consciente de las implicaciones en todos los aspectos de la Entidad que es el ámbito de la ciberseguridad.

La clave se centra en diferenciar las funciones principales sobre las que trabaja el responsable de seguridad y encontrarle una correspondencia en la estructura de la entidad local y que se pueden resumir en:

- Riesgo legal,
- Riesgo reputacional y
- Riesgo tecnológico

Cada uno de estos riesgos tiene una relación clara con responsabilidades en el Ayuntamiento. Los riesgos legales recaen sobre la figura de la secretaría general, riesgo tecnológico sobre informática y los riesgos reputacionales sobre la alcaldía. De esta manera se consiguen dos objetivos:

- Que los puestos de responsabilidad sean conscientes de que la seguridad de la información no es solo responsabilidad de Informática.
- Que las decisiones sean tomadas por aquellos roles o personas que realmente tienen autoridad y responsabilidad dentro de la organización.

En adelante, a la hora de tomar decisiones, y las normativas son precisamente decisiones, buscaremos enfocar sobre qué riesgo se trabaja para que las decisiones tomadas tengan recorrido.

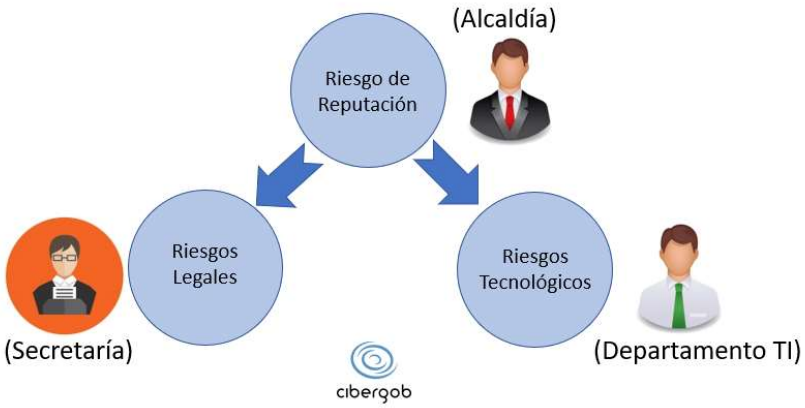


Ilustración 1. Riesgos principales en el Ayuntamiento

El Riesgo Tecnológico tiene su campo de actuación sobre, lógicamente, la tecnología. El Riesgo Legal extiende su ámbito de actuación hacia la normativa de seguridad que va a ser la que canalice en cumplimiento de la Ley (Decretos y Reglamentos, como el ENS o el RGPD).

No significa esto que deba desarrollarla, ya veremos que hay otros cauces, pero sí debe preocuparse, porque le afecta directamente, de que esté desarrollada, debidamente estructurada y aprobada por los órganos internos adecuados. También que los elementos principales de la entidad estén representados y tengan su cuota de autoridad y responsabilidad.

La figura que a estar más expuesta es sobre la que recae el Riesgo Reputacional porque no tiene un ámbito material de actuación definido. Dicho de otra manera, su ámbito de actuación, y su función principal, es que los Riesgos Legales y los Riesgos Tecnológicos sean gestionados de la mejor manera posible. Así, su objetivo en la implantación y mantenimiento de la Seguridad de la información está relacionado con la supervisión y facilitación de los recursos necesarios para que el Riesgo Legal y el Riesgo Tecnológico puedan abordar sus respectivas tareas con garantías.

3.2 Empezando por el principio

Para cumplir el Esquema de Seguridad en su nivel Básico hay que cumplir un 60% de las Medidas de Seguridad explicitadas en el Anexo II del ENS. Alcanzar el nivel Medio una vez cumplido el Básico requiere cubrir un 24% más de Salvaguardas. Un exigente ENS de nivel alto, destinado a Entidades con unos requisitos muy específicos implica, además, cumplir el restante 16% de las medidas de Seguridad.

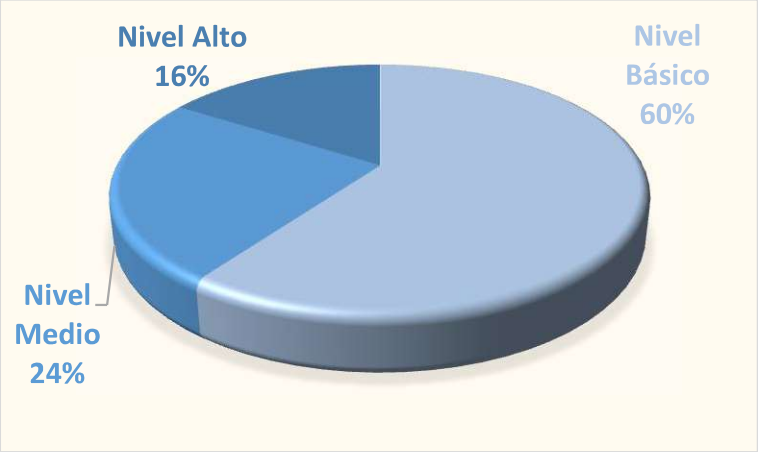


Tabla 1. Distribución de las Medidas de Seguridad del ENS

El nivel de cumplimiento del ENS se asigna principalmente en función del servicio prestado y de la información gestionada, pero también es verdad que, antes de cumplir con un nivel Medio de ENS, por ejemplo (si así surgiera después de un análisis de riesgos), es recomendable abordar primero la tarea de alcanzar un nivel Básico.

En realidad, la dificultad de cumplir el ENS (bien sea básico, medio o alto) radica en lo complejo que resulta cambiar las dinámicas internas para adaptarlas a la nueva situación de incorporar ciberseguridad en el día a día del trabajo.

> La cuestión no radica en cuán lejos estamos del cumplimiento del ENS, sino cómo vamos a generar la dinámica que nos permita movernos en la dirección correcta para alcanzar el cumplimiento y cómo mantener esa dinámica. Si conseguimos eso, poco importará donde esté la meta.

Sin embargo, la decisión de abordar inicialmente el nivel Básico nos va a facilitar el trabajo porque el mundo de la ciberseguridad tiene su complejidad y la gestión de los riesgos, que es en la que se basa, también. Al decidir un nivel Básico de protección nos estamos ahorrando tener que entender, por ahora, el proceso de por qué un Sistema es de nivel Básico, Medio o Alto.

Al fin y al cabo, en los tres casos los requisitos a cumplir son de cierta envergadura, así que intentemos evitar la parálisis por el análisis y vayamos a lo realmente importante: tomar decisiones orientadas.

Una vez generada y dominada la dinámica que nos permita alcanzar el cumplimiento del nivel Básico (60% de las medidas), importará menos si debemos cubrir algunas más. El secreto del cumplimiento del ENS es en realidad tener una dinámica que permita avanzar con ritmo, en la que los pasos iniciales son claves y los que más resistencias suelen generar.

Una vez consolidada la dinámica de cumplimiento, es el momento de avanzar y establecer si nuestro sistema es de nivel Básico, Medio o Alto. Esto se resuelve a través del Análisis de Riesgos que debe tener en cuenta el servicio prestado y la información gestionada.

3.3 Alcance del cumplimiento del ENS: la Sede Electrónica

Son los servicios prestados por el ayuntamiento los que deben cumplir el Esquema Nacional de Seguridad. Es decir, no es un organismo en concreto el que cumple con el ENS sino los servicios que presta ese organismo. Más concretamente servicios prestados al ciudadano.

Se suele simplificar a “el ayuntamiento cumple con el ENS” pero no es una afirmación correcta y lógicamente induce a errores. De hecho, lo habitual es que un mismo ayuntamiento tenga varios servicios que deban cumplir con el ENS (Sede electrónica, web oficial del ayuntamiento, WIFI ciudadana, …). Solo en el caso de que todos los servicios prestados por el consistorio cumplan con el ENS se estaría en condiciones de poder afirmar que el Ayuntamiento cumple con el ENS.

> Son los servicios telemáticos que los organismos prestan a los ciudadanos los que deben cumplir con el Esquema Nacional de Seguridad.

En el caso que nos ocupa, hemos decidido trabajar con el servicio de Sede Electrónica del Ayuntamiento para que sea el que cumpla con el Esquema Nacional de Seguridad. El motivo principal es que bajo la Sede se deben congregar los servicios telemáticos principales que un ayuntamiento presta a sus ciudadanos.

La selección del servicio que debe cumplir con el ENS es importante porque nos ayuda a concretar y priorizar sobre qué aspectos concretos se aborda en primera instancia el cumplimiento de la legislación. Es lo que en el argot de las auditorías se llama 'alcance'.

3.4 Alcance: A más tecnología "en casa", más salvaguardas del ENS

El ENS está basado en Medidas Organizativas y Medidas Técnicas. Las Medidas Organizativas debe desarrollarlas el Ayuntamiento por razones obvias. Ahora bien, las Medidas Técnicas las debe aplicar quien albergue la tecnología que da el servicio.

> Si la Sede Electrónica solo se presta desde el Ayuntamiento, con tecnología que está ubicada solo en instalaciones del Ayuntamiento, aplicar toda la carga de protección que exige el ENS es responsabilidad directa y única del Ayuntamiento.

Por otra parte, la opción de contratar un servicio de sede electrónica a un tercero da la posibilidad de, sin abandonar la responsabilidad del Ayuntamiento de cumplir el ENS sobre el servicio, que sea ese tercero el que debe implementar gran parte de las Medidas Técnicas del Esquema Nacional de Seguridad asociadas al servicio prestado y a la información gestionada.

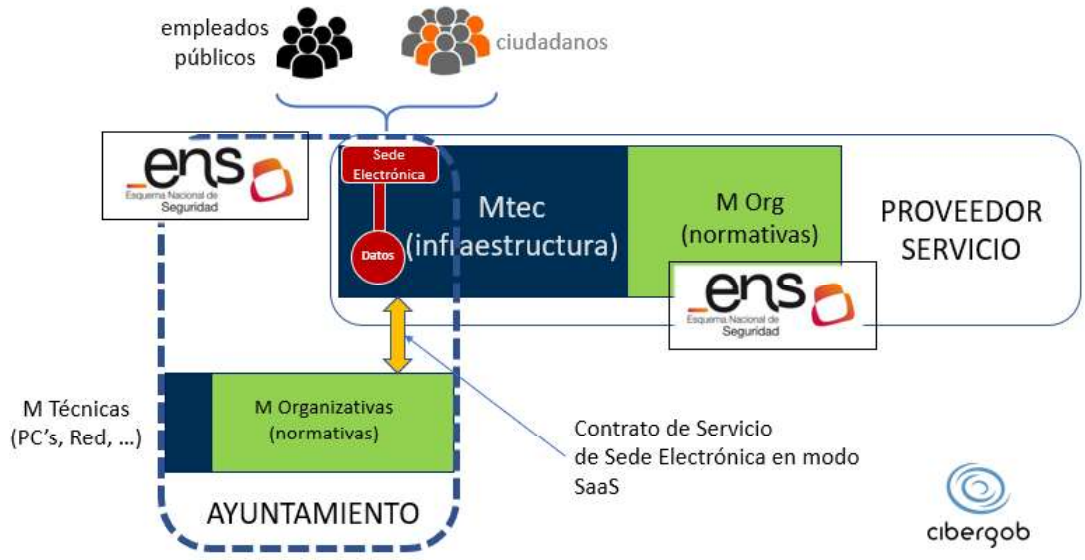


Tabla 2. Esquema de Alcance cumplimiento del ENS para una Sede Electrónica basada en Servicio SaaS

El Esquema Nacional de Seguridad es un Sistema de Gestión de la Seguridad de la información que se focaliza mucho en la protección del ámbito tecnológico. Es decir, para el ENS, lo que prima, lo fundamental, es que estén implantadas y revisadas las medidas de seguridad sobre la tecnología que presta, en nuestro caso, el servicio de Sede Electrónica, al ciudadano.

Por otra parte, las medidas de seguridad a aplicar sobre esa tecnología están explicitadas en el propio ENS que, con las Instrucciones Técnicas de Seguridad (ITS), van a ir actualizándose permanentemente. La implicación es sencilla: el ENS ha sido creado para no quedarse obsoleto con el tiempo y adaptarse a los cambios de la tecnología. Si el ENS cambia, también debe adaptarse a la misma velocidad quien gestione tecnología.

En resumen, si la tecnología de sede electrónica la alberga el Ayuntamiento, éste debe hacer permanentemente ese esfuerzo de cumplimiento de las Medidas Tecnológicas. Si la tecnología está albergada en un tercero certificado, será este quien deba demostrar el cumplimiento de las Medidas Tecnológicas. El Ayuntamiento, como responsable último del servicio, debe hacer seguimiento como parte de sus Medidas Organizativas y de control.

De cara a analizar el caso más habitual en los Ayuntamientos, establecemos que la Sede Electrónica, aun siendo el titular el propio Ayuntamiento, se ayuda de un tercero que provee del servicio telemático (certificado en el ENS) al ciudadano y al empleado público para que puedan hacer las gestiones que la Administración Electrónica posibilita.

3.5 La Aplicabilidad proyectada en un Cuerpo Normativo

Habiendo concretado inicialmente el nivel de cumplimiento, el servicio sobre el que vamos a realizar el cumplimiento, y por lo tanto el alcance, es más sencillo abordar la Aplicabilidad del ENS.

Vaya por delante que la Aplicabilidad es una de las claves del cumplimiento del ENS, tanto es así que debe generarse un documento con ella que debe estar firmado por el Responsable de Seguridad utilizado como evidencia en auditoría de certificación.

La Aplicabilidad resume las exigencias del Anexo II del ENS y elabora una relación de las medidas que son de aplicación al servicio de Sede Electrónica, para el caso que nos ocupa. En la Metodología MADAC todas las medidas de seguridad indicadas en la Aplicabilidad encauzan las salvaguardas a través del Cuerpo Normativo.

Es decir, para todas las Medidas de Seguridad debe detallarse una Salvaguarda (medida de protección) en forma de normativa que indicará cómo se lleva a cabo esa protección (desde el punto de vista organizativo, técnico y de control). Ahora bien, con una normativa se puede cubrir una o varias Medidas de Seguridad

Código	Medida de Seguridad	B	Salvaguardas existentes
org.1	Política de Seguridad	aplica	Política de Seguridad
org.2	Normativa de seguridad	aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información
org.3	Procedimientos de seguridad	aplica	Procedimiento Operativo del Servicio ENS
org.4	Proceso de autorización	aplica	Normativa de Gestión de Autorizaciones
op.pl.1	Análisis de riesgos	aplica	Normativa de Gestión de Riesgos
op.pl.2	Arquitectura de seguridad	aplica	Normativa de Arquitectura de Seguridad
op.pl.3	Adquisición de nuevos componentes	aplica	Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas
op.acc.1	Identificación	aplica	Normativa de Gestión de cuentas de usuario
op.acc.2	Requisitos de acceso	aplica	Normativa de Gestión de Acceso Lógico
op.acc.4	Proceso de gestión de derechos de acceso	aplica	Normativa de Gestión de Autorizaciones
op.acc.5	Mecanismo de autenticación	aplica	Normativa de Gestión de Acceso Lógico
op.acc.6	Acceso local (local logon)	aplica	Normativa de Gestión de Acceso Lógico
op.acc.7	Acceso remoto (remote login)	aplica	Normativa de Gestión de Acceso Lógico
op.exp.1	Inventario de activos	aplica	Normativa de Gestión de Activos
op.exp.2	Configuración de seguridad	aplica	Normativa de Gestión de Bastionados
op.exp.4	Mantenimiento	aplica	Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas
op.exp.6	Protección frente a código dañino	aplica	Normativa de Gestión del Código Dañino
op.exp.8	Registro de la actividad de los usuarios	aplica	Normativa de Gestión Logs de Sistemas y Aplicaciones
op.exp.11	Protección de claves criptográficas	aplica	Normativa de Gestión de Claves de Acceso a Sistemas y Cifrado
op.mon.2	Sistema de métricas	aplica	Normativa de Métricas Indicadores de Seguridad
mp.if.1	Áreas separadas y con control de acceso	aplica	Normativa de Seguridad Física y del Entorno
mp.if.2	Identificación de las personas	aplica	Normativa de Seguridad Física y del Entorno
mp.if.3	Acondicionamiento de los locales	aplica	Normativa de Seguridad Física y del Entorno
mp.if.4	Energía eléctrica	aplica	Normativa de Seguridad Física y del Entorno
mp.if.5	Protección frente a incendios	aplica	Normativa de Seguridad Física y del Entorno
mp.if.7	Registro de entrada y salida de equipamiento	aplica	Normativa de Seguridad Física y del Entorno
mp.per.2	Deberes y obligaciones	aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información
mp.per.3	Concienciación	aplica	Normativa de Gestión de Formación de Concienciación y Sensibilización
mp.per.4	Formación	aplica	Normativa de Gestión de Formación de Concienciación y Sensibilización
mp.eq.1	Puesto de trabajo despejado	aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información
mp.eq.3	Protección de equipos portátiles	aplica	Normativa de Gestión del Parque de Puesto de Trabajo de Digital
mp.com.1	Perímetro seguro	aplica	Normativa de Gestión de Redes y Comunicaciones
mp.com.3	Protección de la autenticidad y de la integridad	aplica	Normativa de Gestión de Redes y Comunicaciones
mp.si.1	Etiquetado	aplica	Normativa de Gestión y Soportes
mp.si.3	Custodia	aplica	Normativa de Gestión y Soportes
mp.si.4	Transporte	aplica	Normativa de Gestión y Soportes

mp.si.5	Borrado y destrucción	aplica	Normativa de Gestión y Soportes
mp.sw.2	Aceptación y puesta en servicio	aplica	Normativa de Gestión de Desarrollo Seguro
mp.info.1	Datos de carácter personal	aplica	Normativa de Gestión del RAT
mp.info.2	Calificación de la información	aplica	Normativa de Gestión de la clasificación y tratamiento de la Información
mp.info.4	Firma electrónica	aplica	Política de Firma Electrónica
mp.info.6	Limpieza de documentos	aplica	Normativa de Gestión de la clasificación y tratamiento de la Información
mp.info.9	Copias de seguridad (backup)	aplica	Normativa de Gestión del Respaldo de la Información
mp.s.1	Protección del correo electrónico	aplica	Normativa de Gestión del Aseguramiento de Servicios
mp.s.2	Protección de servicios y aplicaciones web	aplica	Normativa de Gestión del Aseguramiento de Servicios

Tabla 3. Ejemplo de Aplicabilidad ENS Básico en Metodología MADAC. Cedido por Cibergob.

Asignar cada Medida de Seguridad a normativas, tal y como indica la metodología MADAC, va a permitir asentar las decisiones que deben llevarse a cabo en el ámbito tecnológico. La implantación o ejecución de esas decisiones puede llevar más o menos recursos (tiempo, personal, tecnología, …) , pero que las decisiones estén tomadas por el órgano competente (el Comité) es una primera garantía de que, más temprano que tarde, se llevan a cabo.

4. Implantando el ENS paso a paso

Llegados a este punto, hemos tomado algunas decisiones que se podrían resumir en:

Debe haber un **Comité de Seguridad** que, para que sus decisiones tengan vigencia y sean ágiles, debería estar formado por el **alcalde, el secretario y el responsable de informática.** El servicio sobre el que se va a trabajar es la **Sede Electrónica** porque se ajusta al objetivo fundamental del ENS de generar confianza en el Administración Electrónica. El servicio tecnológico de Sede Electrónica lo **provee un tercero como SaaS (Software como Servicio) certificado en el ENS,** tanto a ciudadanos como a los empleados públicos.

En estas condiciones el Ayuntamiento debe **completar las Medidas Organizativas y todas aquellas Medidas Técnicas relacionadas** con el servicio a certificar y que son responsabilidad directa del Ayuntamiento (los PC's, el Almacenamiento común, la red, la conexión a internet, …)

Iniciamos los trabajos de cumplimiento del Ayuntamiento con el **Nivel Básico del ENS** como objetivo primero a falta de un Análisis de Riesgos que llegará más adelante, cuando realmente sea necesario. Para abordar la **Aplicabilidad,** que es un documento clave y de referencia en la implantación del ENS, utilizamos los criterios de la Metodología Ágil de Adaptación Continua donde todas las Medidas de Seguridad deben tener reflejo normativo.

4.1 Sistema de Gestión basado en Metodologías Ágiles

Productos mínimos viables o *iteraciones* son conceptos utilizados en la Metodología Ágil de Adaptación Continua (MADAC) con la que abordamos la generación del Sistema de Gestión sobre la que se sustenta el cumplimiento del Esquema Nacional de Seguridad.

La Metodología desarrolla otros conceptos innovadores que permiten una implantación realmente ágil del Esquema Nacional de Seguridad con unas características clave: asumible en coste; eficiente y rápido; con un seguimiento sencillo y funcional; y un mantenimiento que permite a Ayuntamiento autonomía de gestión y decisión en materia de seguridad de la información.

4.2 Metodología Ágil de Adaptación Continua (MADAC)

MADAC conecta con el ENS en la Aplicabilidad donde todas las Medidas de Seguridad necesarias para cumplir con el ENS deben estar contempladas en una normativa. Son las normativas las que rigen la tecnología, con lo que todas las tecnologías que utilice el Ayuntamiento para proporcionar servicios al ciudadano deben regirse bajo normativas ágiles.

Las normativas, por otra parte, deben ser un fiel reflejo de las decisiones de la entidad, representada en el Comité de Seguridad, con respecto a cómo gobernar y gestionar la ciberseguridad.

Así, el primer paso para el cumplimiento del Esquema Nacional de Seguridad es incorporar un Cuerpo Normativo de Seguridad, que cubra de manera operativa la Aplicabilidad.

Iteraciones y fases

MADAC divide el proyecto de implantación en cuatro fases donde los primeros estadios son clave para el buen desarrollo del proyecto y donde uno de los objetivos principales al final de éste es mantenerse en órbita de cumplimiento, es decir haber creado una dinámica donde sea fácil mantener el cumplimiento del ENS.

Las cuatro fases, a su vez, las dividimos en iteraciones. El número de iteraciones puede variar en función de la Organización, el nivel del ENS a alcanzar, la complejidad de la tecnología, el servicio, …

La iteración refleja el trabajo que se debe realizar tanto desde el punto de vista del desarrollo de las normativas como de los planes de contraste. La iteración finaliza en la reunión del Comité de Seguridad, quede debe cumplir varios requisitos, además de la mera reunión de los integrantes del Comité, para convertirse en una iteración real que compute como medida de avance en el proyecto.

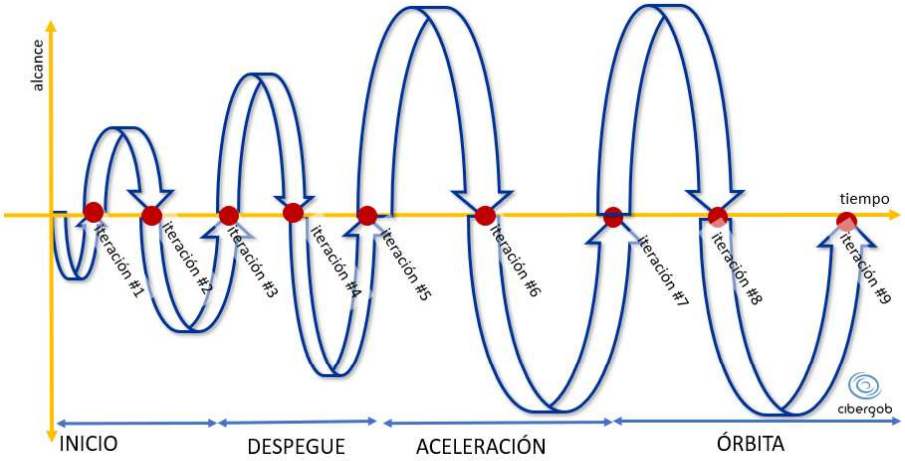


Tabla 4. Fases y ejemplo de Iteraciones según Metodología MADAC

Cuerpo Normativos y Planes de Contraste

El Cuerpo Normativo, o Cloud normativo, es el conjunto de normas interconectadas e interdependientes que construimos para que rijan las acciones que se van a llevar a cabo sobre la Tecnología. Las normativas son, en realidad, esas decisiones que toma el Comité de Seguridad sobre temas vinculados a los servicios prestados a los ciudadanos y a los datos que el ayuntamiento gestiona de ellos (con el efecto que eso pueda tener sobre la Tecnología).

Los Planes de contraste, o "Confía, pero comprueba", es una de las herramientas de MADAC para controlar, de una manera no invasiva, que se gestiona la Tecnología en base a las decisiones tomadas a cabo en el Comité de Seguridad, formalizadas en las normativas.

4.3 Generando el Cuerpo Normativo

El Sistema de Gestión según MADAC se basa en la creación de normativas ágiles que generen un marco de trabajo estable desde el punto de vista de gobierno y gestión para el control suficiente y adecuado de la seguridad de la tecnología.

Así, todas las medidas de seguridad detalladas en la Aplicabilidad del Esquema Nacional de Seguridad deben tener una correspondencia en una normativa. De la misma manera, la normativa, además de reflejar las decisiones del consistorio sobre cómo gestionar la seguridad, debe contemplar lo indicado en el Decreto del ENS.

4.3.1 Características de las normativas

La vigencia del cuerpo normativo tiene una dificultad clara en la sostenibilidad de éste que MADAC aborda trasladando a las normativas unas características que deben cumplir para que sean sostenibles:

Ágil = f (Breve, Conectada, Dirigida, Estructurada)

Así, MADAC, busca generar normativas ágiles para que puedan ser adaptadas, llegado el momento, a la velocidad adecuada. Para ello se califican las normativas que se deben generar o vincular (si vienen de otros Sistemas de Gestión, ISO27001 por ejemplo).

4.3.2 Estructura de una Normativa de seguridad

La norma de seguridad establece unos requisitos que se sustentan en la Política y que regulan determinados aspectos de seguridad. Son, por lo tanto, declaraciones a satisfacer, decisiones. Una norma debe ser clara, concisa y no ambigua en su interpretación.

En cuanto a la estructura de un documento normativo, proponemos una estructura, por otra parte habitual, en los siguientes apartados:

- **Objetivo**: declaración del propósito o intención de la redacción del documento y de los objetivos de seguridad relacionados con la política que se intentan satisfacer.
- **Definiciones:** Se indican las definiciones de aquellos términos que aparezcan en la norma y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en la norma de los términos utilizados.
- **Responsables del cumplimiento:** se define dentro de la Entidad qué departamento o responsable velará por el cumplimiento de la norma y revisará su correcta implantación o cumplimiento.
- **Incidencias en el cumplimiento:** se establecen las consecuencias que se derivarán del incumplimiento de la norma cuando éste sea detectado o las acciones disciplinarias que ocasionarán.
- **Normas que aplicar:** debe contener los requisitos de seguridad que se declaran de obligado cumplimiento. Podrán agruparse los requisitos por categorías, estableciendo apartados donde se agrupen los requisitos relacionados. También los enunciados pueden numerarse para posteriormente referenciarlos.

En cuanto a las recomendaciones en la redacción del documento, es clave que:

- El cumplimiento debe ser factible a nivel organizativo y técnico.
- La redacción debe ser clara y resumida.
- Las afirmaciones realizadas dentro del apartado "Normas a aplicar" deben ser taxativas, no ambiguas y deben permitir la revisión o auditoría del cumplimiento del hecho reglado.
- El tiempo verbal de las normas debe ser presente del indicativo. Evitar el futuro y el condicional.
- La divulgación se debe realizar entre las áreas afectadas o implicadas en el cumplimiento.
- Su aprobación debe estar formalizada, indicando los plazos de vigencia y de revisión de la norma. Debe estar bajo un control de versiones y firmada digitalmente por el presidente y el secretario del Comité de Seguridad.

4.4 Generando los Planes de Contraste

La realización de comprobaciones sobre las Tecnología es fundamental para poder implementar una correcta Adaptación Continua del Sistema de Gestión. En el ámbito de la Seguridad, con la rápida de evolución de la Tecnología y la obligación legal tener la información sensible protegida, realizar comprobaciones sobre ésta para comprobar que es segura, conforme al marco normativo, es fundamental.

Al fin de asegurar su correcto funcionamiento y evitar vulnerabilidades, la tecnología debe ser comprobada de manera periódica para minimizar en lo posible el riesgo de que se vea comprometida su seguridad y, en consecuencia, de los datos que sobre esos sistemas se alojan.

Los Planes establecen la necesidad de realizar las comprobaciones necesarias y progresivas para alimentar la Adaptación Continua.

4.4.1 Estructura de un Plan de contraste

En cuanto a la estructura de un documento de Plan de Contraste, proponemos una estructura en los siguientes apartados:

- **Objetivo**: declaración del propósito del Plan de contraste y su vinculación con la normativa o normativas que comprueba.

- **Definiciones:** Se indican las definiciones de aquellos términos que aparezcan en el documento y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar ambigüedad en la interpretación.
- **Roles y Responsables:** se define dentro de la Entidad qué departamento o responsable velará por el cumplimiento del Plan y revisará su correcta implantación o cumplimiento.
- **Plan de Comprobación:** debe concretar el Plan, cuando está previsto hacerlo, quien debe implementarlo, el alcance de la comprobación y finalmente los registros y evidencias que el plan va a generar.

4.5 Los contextos: Clasificación de Normas y Planes de Contraste

La seguridad tiene una componente transversal que es, por una parte, uno de sus factores más complejos, pero que también conlleva un gran potencial por su capacidad de transformación. MADAC utiliza esa componente transversal para abordar la implantación del ENS.

Todos los ámbitos de la Entidad se ven afectados por la seguridad y la seguridad afecta a todos los ámbitos, es decir, la normativa de seguridad que se genera no solo afecta a aspectos técnicos, sino que, de una manera u otra, va a tener reflejo en varios ámbitos del Ayuntamiento. Es por eso por lo que la MADAC clasifica las normativas en función de a qué contextos afecta a la seguridad:

Contextos		Decisiones reflejadas en normativas
Clasificación de normativas de seguridad por contextos		
Organización	1.ORG	sobre la organización de la seguridad dentro de la entidad
Usuarios	2.USU	enfocadas a los usuarios
Seguridad	3.SEG	Decisiones generales sobre ciberseguridad
Tecnología	4.TEC	Decisiones concretas sobre las plataformas tecnológicas
Puesto de Trabajo Digital	5.PTD	Decisiones concretas sobre PC's, portátiles, móviles
Monitorización	6.MON	Para establecer el control adecuado de los servicios
Software	7.SOFT	Decisiones concretas sobre el desarrollo software en la entidad

Esta clasificación facilita la comprensión sobre los ámbitos en los que se está avanzando cuando se toman las decisiones (que se ven reflejadas en las normativas y comprobadas en los planes de contraste).

5. Implantación del Sistema de Gestión para el ENS

Todo proyecto de implantación del Sistema de Gestión en MADAC está dividido en cuatro fases. Cada fase corresponde a un estadio que tiene con fin último alcanzar una dinámica que permita a la Entidad entender, integrar, utilizar y gobernar la ciberseguridad como una herramienta más de la gestión del Ayuntamiento.

Alcanzar la última fase, la órbita (de cumplimiento), significa haber consolidado la integración de la ciberseguridad en el Ayuntamiento y haber asimilado las claves que permiten un gobierno real de la seguridad de la información.

La 'órbita de cumplimiento' es la capacidad de la entidad de mantener una dinámica continua de adaptación para cumplir con los cambios tecnológicos, organizativos o/y legislativos.

Las tres fases primeras, son los pasos naturales para alcanzar esa Órbita de Cumplimiento. Inicio, fase clave porque se va a asentar la manera de trabajar durante los siguientes pasos. Despegue y Aceleración, son las fases que abordan el núcleo de las decisiones y comprobaciones para llevar a buen puerto el cumplimiento del ENS.

Cada una de las fases contiene iteraciones y dependiendo del tipo de entidad y del servicio a certificar puede contener más o menos iteraciones.

En base al tipo de entidad, el servicio que estamos analizando, el nivel de ENS que buscamos alcanzar en primera instancia, establecemos que con 6 iteraciones repartidas en las cuatro fases tal y como se indica en la tabla podemos abordar el proyecto:

FASE		CONTEXTOS	iteraciones
FASE I	INICIO	1.ORG; 2.USU	it#1, it#2
FASE II	DESPEGUE	3.SEG; 4.TEC; 5.PTD; 6.MON	it#3, it#4
FASE III	ACELERACIÓN	3.SEG; 7.SOFT; 6.MON	it#5
FASE IV	ÓRBITA (de cumplimiento)	4.TEC	it#6

Tabla 5. Distribución de las iteraciones en las fases. Base del plan de riesgos

A partir de esta decisión, vamos a poder ir viendo los avances conseguidos y proyectando previsiones sobre las siguientes iteraciones en los Cuadros de Mando.

Los proyectos de implantación son diferentes unos de otros, puede cambiar el alcance, puede cambiar los sistemas que soportan el servicio, y pueden combinarse los sistemas y los servicios. Es por esa razón que MADAC subdivide los proyectos en FASES, que son siempre cuatro, y éstas en iteraciones que pueden variar en número dentro de las propias fases.

En cada fase se abordan una serie de normativas. La priorización de unas u otras normas va en función de criterios que siempre deben ir orientados a facilitar el cambio y a activar la dinámica de cumplimiento. En todo caso, es importante remarcar que la agrupación de las normativas en iteraciones y fases va a ser la manera en que el Ayuntamiento priorice los aspectos de seguridad más relevantes para la entidad. Es decir, gestione el riesgo. En otras palabras, el orden en el que abordemos y distribuyamos las normativas se convierte de facto en el plan de gestión del riesgo.

5.1 FASE I. INICIO

En estas primeras iteraciones es fundamental enfrentarse a los dos grandes retos de cualquier Ayuntamiento con respecto a la ciberseguridad: mejorar la coordinación interna (Contexto Organización) y contar con los empleados públicos para que formen parte de la solución (Contexto Usuarios)

Se abordan también aspectos generalistas de la seguridad (Contexto de Seguridad), con ciertas normativas, que en las siguientes fases se verán complementadas.

Tal y como quedaba introducido en la base de plan de gestión de riesgos, la fase I contiene dos iteraciones donde se deben abordar las normativas que hemos detallado en la Aplicabilidad. Una manera de abordar la fase de Inicio podría ser esta:

Normativas	iteración	Contexto
Normativa de Organización de la Seguridad	It#1	1.ORG
Normativa de Gestión del Marco Normativo	it#1	1.ORG
Normativa de Arquitectura de Seguridad	it#1	3.SEG
Normativa de Clasificación y Tratamiento de Información	it#1	3.SEG
Normativa de Gestión de Cuentas de Usuario	it#2	2.USU
Normativa de Autorizaciones	it#2	2.USU
Normativa de Uso de Recursos y Acceso a Sistemas	it#2	2.USU
Normativa de Gestión de Acceso Lógico	it#2	2.USU
Normativa de Gestión Formación Concienciación y Sensibilización	it#2	3.SEG

Tabla 6. Fase I. Plan de Gestión del Riesgo

Llegado el momento y finalizada la Fase I, es decir cuando se han completado la primera y la segunda iteración, el grado de avance sobre el proyecto se muestra a través del cuadro de mando que MADAC permite generar.

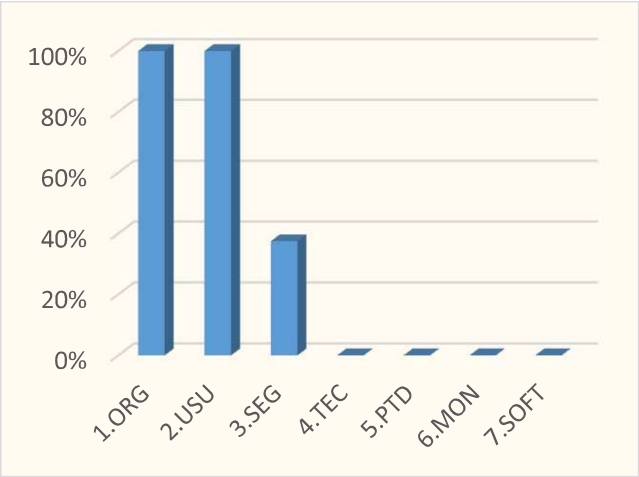


Tabla 7. Cobertura del Cuerpo Normativo – Fase I

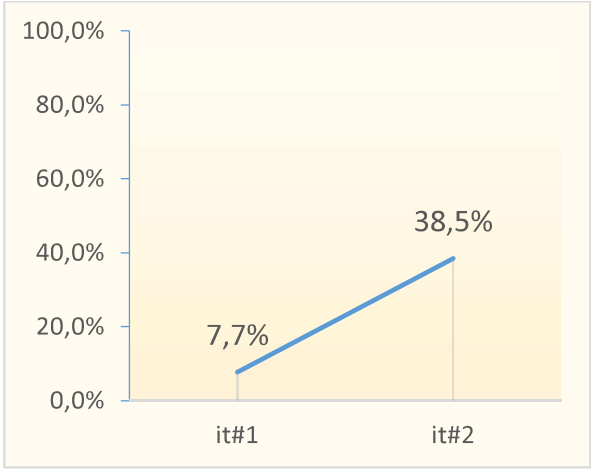


Tabla 8. Progresión del cuerpo normativo sobre la Aplicabilidad

En el gráfico se puede interpretar sin dificultad que se han completado los contextos de Organización y de Usuario, que se está avanzando en temas de la Seguridad (un 40%) pero que, de Tecnología, Puesto de Trabajo, etc. aun no se ha avanzado nada. Lo que también ayuda al Comité de Seguridad a crear consciencia del trabajo que queda por delante y qué ámbitos de la ciberseguridad del Ayuntamiento no se han cubierto aún.

MADAC facilita, con sus sprints e iteraciones, la entrega de valor rápida a la entidad, es decir, materializa una de las características fundamentales de las metodologías ágiles. La tabla de progresión de Aplicabilidad así lo muestra. Completando correctamente las dos primeras iteraciones la Aplicabilidad del ENS sobre el servicio que queremos certificar se acerca ya al 40% del trabajo que debemos realizar.

Desde el punto de vista del riesgo también hay avances puesto que la toma de decisiones y su comprobación a través de los Planes de Contraste permite valorar con precisión la implementación de las salvaguardas.

La Metodología MADAC se complementa perfectamente con la Metodología MAGERIT y con PILAR, herramienta de Análisis de Riesgos que el CCN pone a disposición de todas las Entidades Públicas, y de las que hay guías del propio CCN que explican cómo utilizarla.

Del uso de la herramienta PILAR con Metodología MADAC, se desprende el siguiente gráfico de cumplimiento del ENS en cada uno de los ámbitos que indica el ANEXO II.

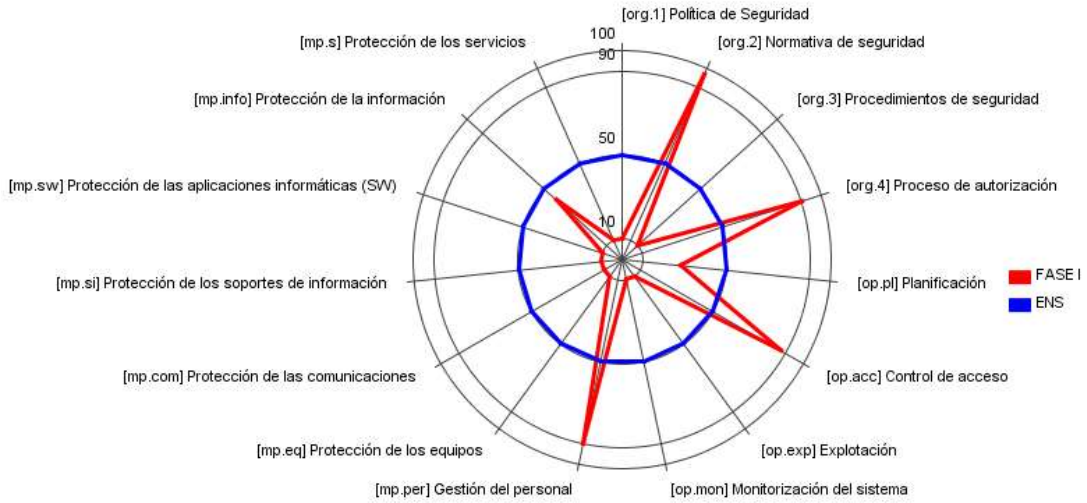


Ilustración 2. Gráfica del AARR en Herramienta PILAR (al completar la Fase I)

Lógicamente el avance se produce en aquellos aspectos que se han ido cubriendo con las normativas y que se han ido comprobando con los planes de contraste.

Para poder seguir avanzando es necesario que el Comité de Seguridad tome consciencia de que la figura del Responsable de Seguridad va a seguir sin aparecer en Ayuntamiento. Esa figura ha se suplirse con los roles principales que comentábamos en apartados anteriores.

Independientemente de quien lleve a cabo la redacción de las normas, éstas tienen una importancia ineludible puesto que deben ser capaces de incluir las decisiones necesarias para gestionar (léase reducir) adecuadamente los riesgos derivados del uso de la tecnología.

En otras palabras, que no haya una normativa de organización de la seguridad es un riesgo que impacta más en el alcalde y en el secretario que en el informático. Luego podremos entrar a concretar si el contenido es más o menos adecuado, pero si no existe esa normativa el cumplimiento legal está en entredicho. puesto que el ENS así lo indica.

La metodología MADAC propone una distribución del Peso del Riesgo de cada uno de los roles del Riesgo en las diferentes normativas, con el objetivo que el Comité de Seguridad sea plenamente consciente de la relevancia de tomar decisiones y que estas queden por escrito.

Normativa	***Peso del Riesgo***		
	Alto	*Medio*	*Bajo*
Normativa de Organización de la Seguridad	*Riesgo Reputacional*	*Riesgo Legal*	*Riesgo Tecnológico*

Normativa de Gestión del Marco Normativo	*Riesgo Reputacional*	*Riesgo Legal*	*Riesgo Tecnológico*
Normativa de Arquitectura de Seguridad	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Normativa de Clasificación de Tratamiento de Información	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*
Normativa de Gestión de la Cuentas de Usuario	*Riesgo Reputacional*	*Riesgo Legal*	*Riesgo Tecnológico*
Normativa de Gestión de las Autorizaciones	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*
Normativa de Uso de los Recursos y Acceso a los Sistemas de Información	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*
Normativa de Gestión de Acceso Lógico	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Normativa de Gestión de la Formación Concienciación y Sensibilización	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*

Tabla 9. Peso del Riesgo en las Normativas

5.2 FASE II: DESPEGUE

En la segunda fase, una vez asentada la manera de trabajar, se abordan decisiones y comprobaciones relacionadas explícitamente con la seguridad y con la tecnología. Los contextos de Seguridad, Tecnología, Puesto de Trabajo y monitorización del cumplimiento del ENS son los que amplían el Cuerpo Normativo en estas dos iteraciones.

El Esquema hace referencias legales externas con las que tiene mucha interrelación: el Reglamento General de Protección de Datos y el Esquema Nacional de Interoperabilidad. En esta fase vinculamos al ENS con el RGPD, enlazando la Aplicabilidad con la Política de Protección de Datos que el Ayuntamiento debe tener desarrollada, con lo que no la incluimos dentro del proceso de implantación del ENS.

La evolución de la gestión del Plan de Riesgos, la concretamos así:

Normativas	iteración	Contexto
Normativa de Gestión de Soportes	it#3	5.PTD
Normativa de Gestión de Activos	it#3	3.SEG
Normativa de Gestión del Parque de Puesto de Trabajo Digital	it#3	5.PTD
Normativa de Gestión del Respaldo de la Información	it#3	3.SEG
Política de Protección de Datos	it#3	RGPD
Normativa de Métricas e Indicadores de Seguridad	it#4	6.MON
Normativa de Gestión del ciclo de vida de la Tecnología	it#4	4.TEC
Normativa de Gestión de Claves de Accesos a Sistemas	it#4	3.SEG
Normativa de Gestión de Logs de Sistemas y Aplicaciones	it#4	6.MON

Como consecuencia de esa distribución de los esfuerzos y la predictibilidad que permite la Metodología MADAC, se puede conocer el avance sobre el cumplimiento incluso antes de abordar los trabajos. Sea como fuere, una vez finalizadas las dos iteraciones previstas en la presente fase, la Aplicabilidad está a un 72% de cumplimiento y con ella, de una manea muy directa, el cumplimiento del Esquema Nacional de Seguridad.

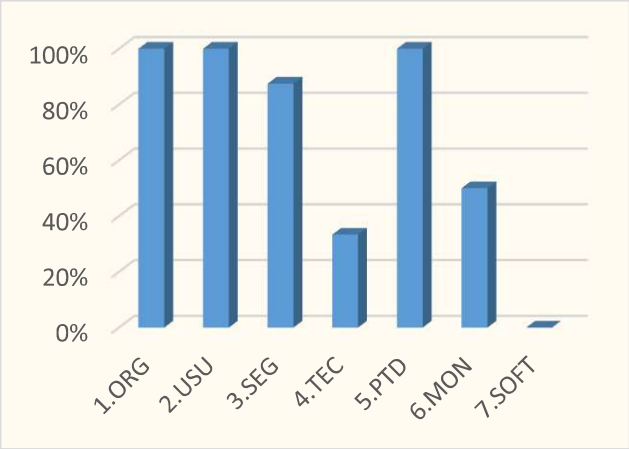


Tabla 10. Cobertura del Cuerpo Normativo – Fase II

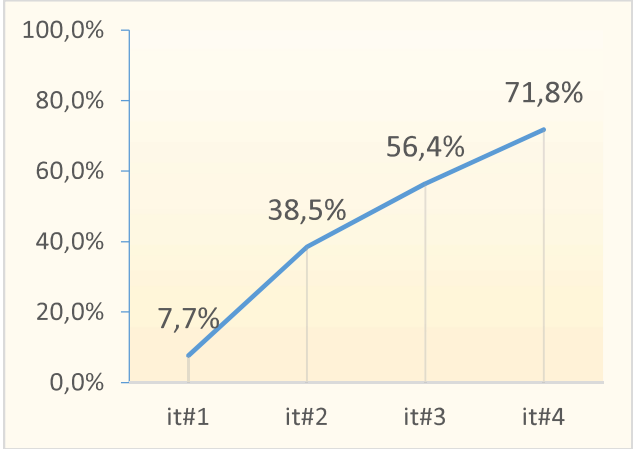


Tabla 11. Progresión del cuerpo normativo sobre la Aplicabilidad

Sin perder de vista el análisis de riesgos, podemos visualizar con la herramienta PILAR también el avance y cumplimiento en cada una de las Medidas de Seguridad que nos indica el ENS.

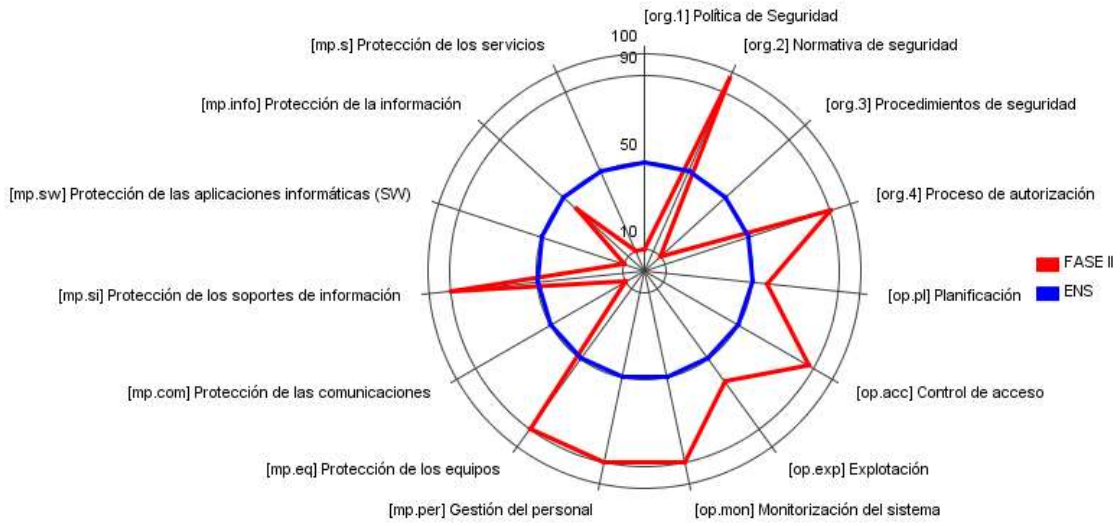


Ilustración 3. Gráfica del AARR en Herramienta PILAR (Fase II)

El peso de Riesgo de las normativas en estas iteraciones se decanta más en el ámbito tecnológico aunque también hay aspectos claves que deben interesar al ámbito legal

(la gestión de los logs, por ejemplo) o del ámbito reputacional (control sobre el propio funcionamiento de los sistemas con las métricas) .

Normativa	Peso del Riesgo		
Gestión de los Soportes	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Gestión de los Activos	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Gestión del Parque de Puesto de Trabajo Digital	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Gestión del Respaldo de la Información	*Riesgo Tecnológico*	*Riesgo Legal*	*Riesgo Reputacional*
Política de Protección de Datos Personales	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*
Gestión de las Métricas e Indicadores de Seguridad	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*
Gestión del Ciclo de Vida de las Plataformas Tecnológicas	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Gestión de las Claves de Acceso a los Sistemas y Cifrado	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*
Gestión de los Logs de los Sistemas y aplicaciones	*Riesgo Legal*	*Riesgo Tecnológico*	*Riesgo Reputacional*

5.3 FASE III: ACELERACIÓN

Se han abordado buena parte de las normativas en las anteriores iteraciones, con lo que las siguientes fases cuentan con una iteración.

Un aspecto clave sucede en esta fase: MADAC propone debatir y aprobar la Política de Seguridad ahora y no antes. La razón radica en que el Comité de Seguridad ya ha podido comprobar qué debe consolidar la Política de Seguridad y cómo se va a implementar. Aspecto que al principio del proyecto no suele estar tan claro en entidades que no han integrado la ciberseguridad. La validación de la Política sostendrá todo el cuerpo normativo enfocado en la protección de la información.

Decíamos en el punto anterior que el Esquema hace referencias legales externas con las que tiene mucha interrelación (el RGPD y el ENI). En esta fase vinculamos al ENS con el ENI, enlazando la Aplicabilidad con la Política de Firma Electrónica, no es el único punto (también la normativa de Clasificación y Tratamiento de Datos está relacionado con el ENI) pero si uno de los más claro.

Normativas	Iteración	CONTEXTO
Política de Firma Electrónica	It#5	ENI
Política de Seguridad de la Información	it#5	ENS

Normativa de Gestión de Aseguramiento de Servicios	it#5	3.SEG
Normativa de Gestión del Desarrollo Seguro	it#5	7.SOFT
Normativa de Gestión de Riesgos	It#5	3.SEG

El Sistema de Gestión del ENS cuenta con un número de normativas que puede variar en función del Nivel de cumplimiento (así, un nivel alto de ENS tiene más normativas que un básico, según MADAC). Ahora bien, el propio ENS solicita algunos documentos que son específicos del ENS, como por ejemplo el Procedimiento Operativo de Seguridad o la Política de Seguridad de la Información. Para estos documentos utilizamos el Contexto "ENS".

En esta fase el Cuerpo Normativo se acerca a un 90% del desarrollo para cubrir la Aplicabilidad. Quedan por desarrollar algunos aspectos técnicos desde el punto de vista de los sistemas y de los puesto de trabajo.

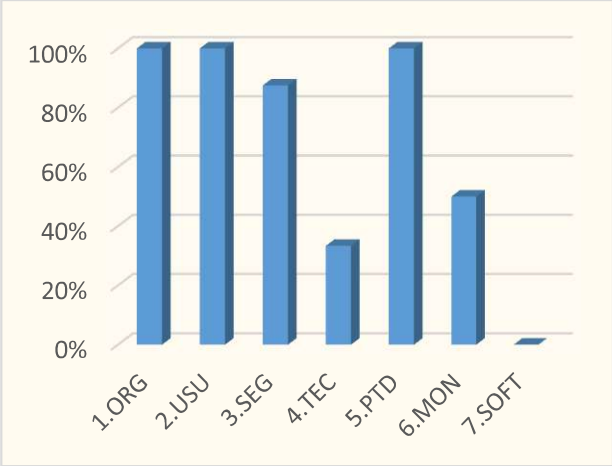


Tabla 12. Cobertura del Cuerpo Normativo – Fase III

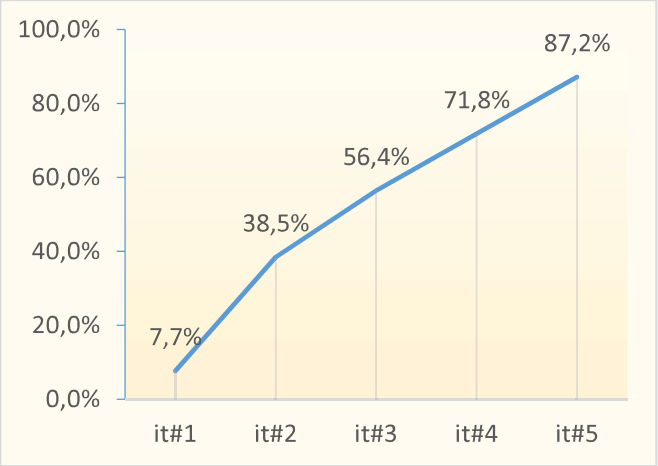


Tabla 13. Progresión del cuerpo normativo sobre la Aplicabilidad

El desarrollo de las normativas tiene un reflejo en el análisis de riesgos sobre PILAR que mostramos a continuación. Debemos tener en cuenta que la aprobación normativa es solo el primer paso para poder gestionar los riesgos de la tecnología. Junto con la normativa se deben desarrollar los Planes de Contraste que deben generar las comprobaciones adecuadas.

Una vez completada la normativa y los planes de contraste adecuados, junto con el Sistema de Gestión por iteraciones de MADAC permiten establecer una valoración de gestión del riesgo según PILAR.

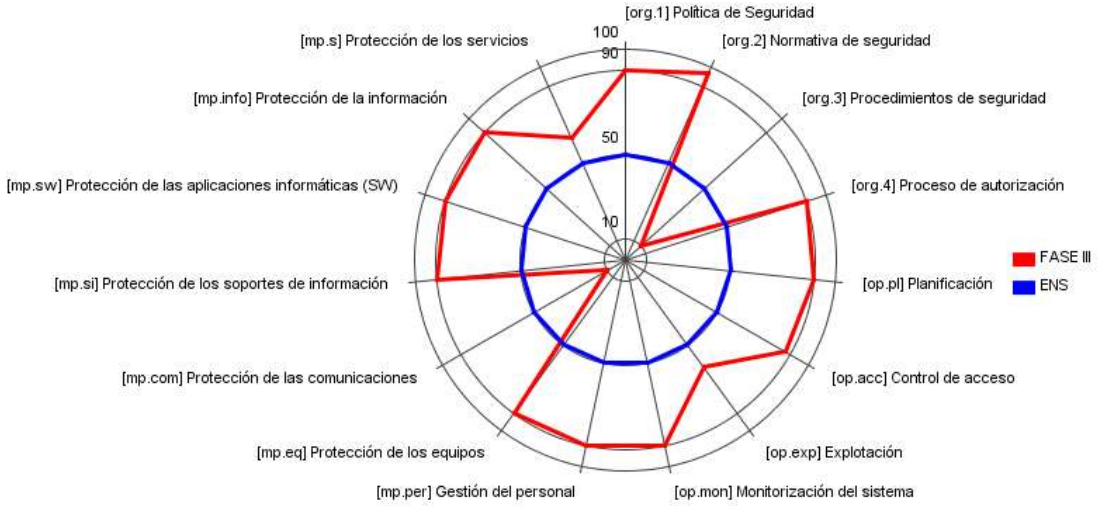


Ilustración 4. Gráfica del AARR en Herramienta PILAR (al completar la Fase III)

Llegado es este punto del proyecto, se puede advertir claramente en qué ámbitos del ENS el Ayuntamiento no ha gestionado, desde el punto de vista de gobierno, aún ningún tipo de riesgo. A nivel tecnológico lo lógico es que haya, por ejemplo, protección en las comunicaciones (VPNs, VLANS,…) pero para cumplir el ENS no es suficiente, con una solución técnica debe establecerse la conexión entre la tecnología y gobierno, que se lleva a cabo a través de las normativas.

El Peso de Riesgo de las normativas en esta iteración revela la importancia tanto del ámbito legal, por la presencia de las Políticas, como el reputacional, el aseguramiento de los servicios y la gestión de los riesgos.

Normativa	Peso del Riesgo		
Política de Firma	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*
Política de Seguridad	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*
Normativa de Gestión de Aseguramiento de Servicios	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*
Normativa de Gestión del Desarrollo Seguro	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Normativa de Gestión de Riesgos	*Riesgo Reputacional*	*Riesgo Tecnológico*	*Riesgo Legal*

5.4 FASE IV: ÓRBITA DE CUMPLIMIENTO

La última fase se desarrolla con una única iteración. Si el cumplimiento se llevara a cabo para alcanzar, directamente, un nivel Medio o un nivel Alto la fase se podría poblar con nuevas iteraciones (y normativas dentro de ellas). Para el caso que nos ocupa no es necesario.

Abordamos la iteración incorporando decisiones Tecnológicas (Bastionado de Sistemas y de gestión de las redes y comunicaciones) y de Puesto del trabajo Digital (tipo de antivirus utilizado por la entidad). La redacción del Procedimiento Operativo de Seguridad es un documento explicitamente solicitado por el ENS.

Normativa	Iteración	CONTEXTO
Normativa de Gestión del Código Dañino	It#6	5.PTD
Normativa de Gestión Redes y Comunicaciones	it#6	4.TEC
Normativa de Gestión de Bastionado	it#6	4.TEC
Procedimiento Operativo de Seguridad de Servicio Sede Electrónica	it#6	ENS

Con la progresión del marco normativo durante las fases e iteraciones, se ha ido modificando el cuadro de mando que nos permite valorar los contextos controlados desde el Comité, también el reflejo en la Aplicabilidad del ENS.

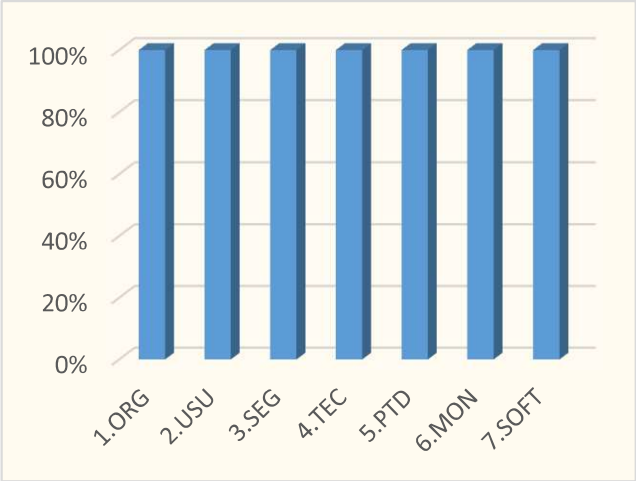


Tabla 14. Cobertura del Cuerpo Normativo – Fase IV

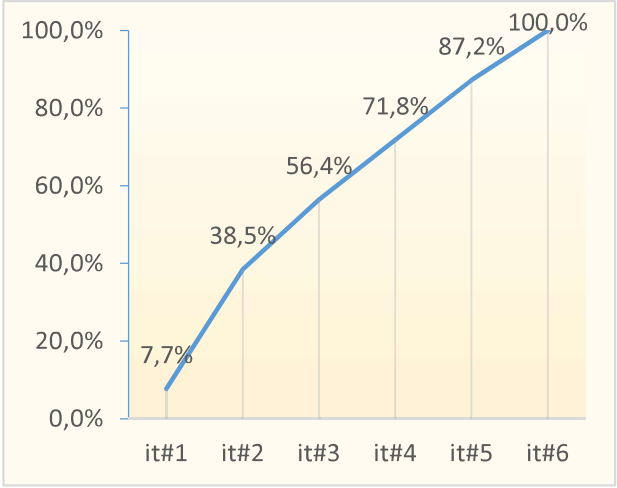


Tabla 15. Progresión del cuerpo normativo sobre la Aplicabilidad

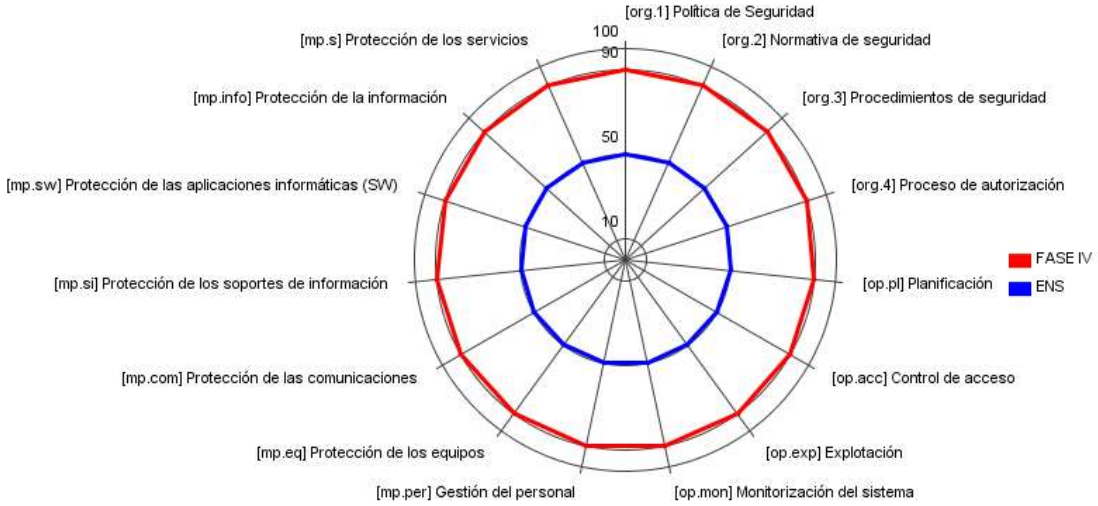


Ilustración 5. Gráfica del AARR en Herramienta PILAR (al completar la Fase I)

El Peso del Riesgo de esta fase es principalmente Tecnológico.

Normativa	Priorización del Riesgo		
Normativa de Gestión del Código Dañino	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Normativa de Gestión de las Redes y Comunicaciones	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Normativa de Gestión del Bastionado	*Riesgo Tecnológico*	*Riesgo Reputacional*	*Riesgo Legal*
Procedimiento Operativo de Seguridad de la Sede Electrónica	*Riesgo Legal*	*Riesgo Reputacional*	*Riesgo Tecnológico*

6. Desarrollo de Normativas de Seguridad

A nadie se le escapa que es costoso generar las normativas sobre todo si es desde cero. El CCN nos facilita esa tarea a través de todas las guías que ha ido emitiendo durante estos últimos años.

En cada uno de los contextos hemos indicado aquellas guías que nos han ayudado y os pueden ayudar a enfocar las decisiones que deben plasmarse en los documentos, teniendo en cuenta la situación particular del Ayuntamiento.

CONTEXTO	

1.ORG ORGANIZACIÓN	CCN-STIC-402 Organización y Gestión TIC CCN-STIC-801 Responsabilidades y Funciones en el ENS CCN-STIC-805 Política de Seguridad de la Información
2. USU USUARIOS	CCN-STIC-822 Procedimientos de Seguridad (en sus diferentes Anexos)
3. SEG SEGURIDAD	CCN-STIC-817 Gestión de Ciberincidentes CCN-STIC-823 Seguridad en entornos Cloud CCN-STIC-812 Seguridad en servicios web CCN-STIC-814 Seguridad en servicio de correo CCN-STIC-203- Estructura y Contenido de los Procedimientos Operativos de Seguridad (POS)
4.TEC TECNOLOGÍA	CCN-STIC-820 Protección contra Denegación de Servicio CCN-STIC-836 ENS - Seguridad en VPN CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS
5. PTD PUESTO DE TRABAJO DIGITAL	CCN-STIC 834 Protección ante Código Dañino en el ENS CCN-STIC-827 Gestión y uso de dispositivos móviles CCN-STIC-821 Normas de Seguridad en el ENS CCN-STIC-835 Borrado de metadatos en el marco del ENS CCN-STIC-404 Control de soportes informáticos
5.MON MONITORIZACIÓN	CCN-STIC-831 Registro de la actividad de los usuarios CCN-STIC-844 Manual de usuario de INES CCn-STIC-815 Indicadores y métricas en el ENS

En todo caso incluimos a modo de ejemplo algunas de las normativas principales que hemos ido apuntando a lo largo de la explicación, con las ideas que deben desarrollarse dentro de la estructura documental que genereis para vuestras normativas de seguridad

6.1 Normativa de Clasificación y tratamiento de la información

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Restricciones	Medida de Seguridad	B	Salvaguardas existentes
Mp.info.6	Calificación de la Información	Aplica	Normativa de Clasificación y Tratamiento de Información
Mp.info.6	Limpieza de documentos	Aplica	Normativa de Clasificación y Tratamiento de Información

Fundamento de la Normativa

La responsabilidad de la clasificación y/o reclasificación de la información es del propietario de dicha información. En todo caso, para calificar la información se estará a lo establecido legalmente sobre la naturaleza de esta.

Los niveles de clasificación se deben definir considerando las necesidades de conocer y de compartir y como norma general todo documento debe incluir la información sobre la clasificación de éste.

La clasificación por defecto del cualquier documento generado dentro de la Entidad es de Nivel Básico. Cualquier otra consideración debe modificar esta clasificación. Los criterios que determinan el nivel de seguridad requerido están basados en la gestión de los riesgos.

En función de la clasificación que asigne a la información, ésta será tratada de una manera u otra por los Sistemas de información que la gestionan.

El responsable de cada información (el responsable de la Información) debe seguir los criterios determinados por el Análisis de Riesgos para asignar a cada información el nivel de seguridad requerido, es el responsable de su documentación y de la aprobación formal. Tiene, además, la potestad de modificar el nivel de seguridad requerido, de acuerdo con los párrafos anteriores.

Aparte de la clasificación de documentos se define la Lista de Distribución del Documento (LDD). Un documento sólo puede distribuirse a las personas o roles definidos en la lista de distribución del documento que obligatoriamente debe constar en él.

Para el tratamiento de la información y sus soportes se debe utilizar, dentro de las posibilidades de la Entidad, productos certificados o acreditados.

Para toda información clasificada se debe tener en cuenta que los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales.

Como parte del proceso de limpieza de documentos, se debe retirar de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Para la gestión segura de la información es requisito indispensable clasificar la información según su naturaleza y su nivel de confidencialidad. La clasificación de la información afecta al tratamiento de los documentos y los Sistemas de Información y a los medios de almacenamiento y transferencia de la información.

La responsabilidad de la clasificación y/o reclasificación de la información es del propietario de dicha información. En nuestro caso la titularidad recae en el responsable de la Información del Ayuntamiento que está colegiado en el Comité de Seguridad.

Aspectos concretos a desarrollar en la normativa

La clasificación para un Ayuntamiento podría quedar resumida de la siguiente manera:

Ilustración 6. Clasificación de la información. Cibergob

En función de la clasificación el Comité debe decidir cómo tratar ese tipo de información. Valorando varios aspectos que son relevantes para garantizar la seguridad de la información: Cómo tratar las copias, cómo almacenar el documento, cómo transmitirlo, cómo destruirlo y si es necesario establecer una marca de agua en él para identificarlo claramente.

Un ejemplo como posible referencia este de “Uso Interno”

Restricciones	Comentarios

Copia	Puede copiarse tanto en formato electrónico como en papel.
Almacenamiento	No hay definidas restricciones especiales a su forma de almacenamiento.
Transmisión	Puede transmitirse de cualquier forma, tanto en formato electrónico como en papel, pero *únicamente entre personal del Ayuntamiento*. Si la lista de distribución es más restrictiva únicamente a las personas/roles/grupos definidos en la lista de distribución.
Destrucción	No hay definidos procedimientos especiales para su destrucción
Marca de Agua	Necesario incluir marca de Agua "Uso Interno"

Ilustración 7. Ejemplo de tratamiento en función de la clasificación de la información. Cibergob

Por otra parte, es importante remarcar que el uso inadecuado de información restringida debe quedar prohibido en el Ayuntamiento. Así, se debe prohibir a los usuarios tener acceso a la información, de cualquier naturaleza o medio, para la que no hayan sido autorizados. También compartir información restringida de cualquier índole con personas que no estén autorizadas a conocer dicha información.

En definitiva, los usuarios autorizados tienen la responsabilidad de saber que, si hacen un uso inapropiado de la confidencialidad de la información del ayuntamiento, puede negárseles el acceso futuro a la información y pueden estar sujetos a las sanciones disciplinarias establecidas. Al fin y al cabo, estamos hablando, en gran medida, de datos relacionados con los ciudadanos que confían en que son salvaguardados adecuadamente.

6.2 Normativa de Acceso Lógico

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Código	Medida de Seguridad	B	Salvaguardas existentes
op.acc.2	Requisitos de acceso	Aplica	Normativa de Acceso Lógico
op.acc.5	Mecanismo de autenticación	Aplica	Normativa de Acceso Lógico
op.acc.6	Acceso local	Aplica	Normativa de Acceso Lógico
op.acc.7	Acceso remoto	Aplica	Normativa de Acceso Lógico

Fundamentos de la Normativa

La Normativa sobre la Gestión de los Accesos lógicos a los sistemas (entendido bien como servicio, bien como tecnología) se basa en requisitos de seguridad y de negocio definiendo accesos en función de uno y otro aspecto.

Como norma general el ayuntamiento no debe permitir acceder a información sin una identificación y autenticación previa del usuario que implica una verificación previa de los derechos de acceso, estableciendo pautas para gestionar la asignación de derechos y privilegios de acceso de los usuarios a los sistemas y servicios.

La normativa de control del acceso lógico a los sistemas debe marcar que se ha prevenir la revelación de cualquier información del sistema aún sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso deben proporcionar solamente la información indispensable)

El número de intentos permitidos debe quedar limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos y se deben registrar los accesos con éxito, y los fallidos y custodiar.

El Sistema debe informar al usuario de sus obligaciones inmediatamente después de obtener el acceso, así como del último acceso efectuado con su identidad.

A los Sistemas que tenga disponible el ayuntamiento acceden, bien los usuarios autorizados por el propio ayuntamiento para su uso, bien la empresa proveedora de Servicios para su administración.

Se debe garantizar la seguridad de los sistemas cuando accedan remotamente lo que implica proteger tanto el acceso en sí mismo como el canal de acceso remoto (a través de un canal seguro). Con la autorización positiva conveniente para la conexión remota, los usuarios y los administradores pueden realizar las mismas funciones en remoto que en local.

Aspectos concretos a desarrollar en la normativa

La normativa debe dejar reflejada, y por lo tanto debe implimentarse, atendiendo a las posibilidades de la entidad:

- Los recursos del sistema se deben proteger con un mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
- Los derechos de acceso de cada recurso, se establecen según las decisiones de la persona responsable del recurso (ateniéndo a la política y normativa de seguridad del sistema).
- Se debe controlar el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

- Se admite el uso de cualquier mecanismo de autenticación sustentado en un solo factor (en el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma).
- Se debe atender a la seguridad de las credenciales de forma que:

    a. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
    b. Las credenciales deben estar bajo el control exclusivo del usuario.
    c. El usuario debe reconocer que las 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.
    d. Las credenciales se deben cambiar con una periodicidad marcada por la política de la organización (atendiendo dentro de lo posible a la categoría del sistema al que se accede).
    e. Las credenciales se deben retirar y deben ser deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

- La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso deben proporcionar solamente la información indispensable).
- El número de intentos permitidos debe estar limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.
- Se deben registrar los accesos con éxito, y los fallidos.
- El sistema debe informar al usuario de sus obligaciones inmediatamente después de obtener el acceso.
- Se debe garantizar la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implica proteger tanto el acceso en sí mismo como el canal de acceso remoto.

6.3 Gestión de la Formación, Sensibilización y Concienciación

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Restricciones	Medida de Seguridad	B	
Mp.per.3	Concienciación	Aplica	Normativa de Gestión de Formación, concienciación y sensibilización
Mp.per.4	Formación	Aplica	Normativa de Gestión de Formación, concienciación y sensibilización

Fundamento de la Normativa

La implementación correcta del Principio de Concienciación, Sensibilización y Formación, contemplado en la Política de Seguridad de la Información, debe tener y tiene consecuencias directas en la capacidad de la entidad de gestionar adecuadamente la información.

Así, la correcta gestión de la concienciación, la sensibilización y la formación tiene efectos directos, reduciéndolos, sobre el coste de la administración de los sistemas y su mantenimiento, también sobre el riesgo al que se ven sometidos. Ayuda a una mejor prevención si hacemos llegar al usuario y administrador información clave y recurrente sobre cómo no poner en peligro la información.

Comunicar de manera ágil y cercana sobre las ciberincidencias y/o sobre las políticas de configuración que afectan al usuario (la configuración de los antivirus, las contraseñas, los niveles de protección de la navegación, …) también va a repercutir positivamente en la concienciación y sensibilización que permite una actitud más proactiva con respecto a la información gestionada.

La propia gestión de las ciberincidencias puede ayudar a desarrollar esta normativa, dado que con su análisis se pueden extraer conclusiones relevantes para evitar acciones que pongan en riesgo la seguridad de la información gestionada.

La manera de hacer llegar toda esta información interrelacionada a los usuarios y administradores es a través de la formación continua de los empleados públicos que es un requisito necesario e imprescindible para que estos continúen aportando valor a la entidad y a los ciudadanos.

Las decisiones del Comité de Seguridad deben ir dirigidas, y por lo tanto plasmadas en la Normativa, a concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se debe trasladar regularmente, la normativa de seguridad relativa al buen uso de los sistemas; la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado; el procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

También se debe formar regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, particularmente en el área de Sistemas, en particular en lo relativo a la configuración de sistemas, la detección y reacción a incidentes y la gestión de la información en cualquier soporte en el que se encuentre (cubriendo al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción de información)

6.4 Gestión de las Redes de Comunicaciones

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Restricciones	Medida de Seguridad	B	
Mp.com.1	Perímetro seguro	Aplica	Normativa de Gestión de las Redes de Comunicaciones
Mp.com.3	Protección de la autenticidad y de la integridad	Aplica	Normativa de Gestión de las Redes de Comunicaciones

Fundamento de la Normativa

El Ayuntamiento gestiona y controla sus redes para la protección contra posibles amenazas tanto de las propias redes como contra los sistemas y aplicaciones soportadas en ellas, a través de controles que buscan garantizar la confianza en la información que se encuentra dentro de la Entidad. Así se controla las redes internas de la entidad, así como las redes de acceso a la propia red interna.

Las redes de acceso se consideran redes de alto riesgo, especialmente las redes de acceso externas, directamente expuestas a intentos de intrusión desde el exterior de la entidad. Por esta razón, se debe minimizar el número de redes de acceso externas, con el fin de concentrar el riesgo y poder centrar los esfuerzos en los mecanismos defensivos.

Como norma general, desde entidades conectadas a través de redes de acceso externas únicamente se podrá acceder a servicios situados en redes DMZ. Se deben emplear redes privadas virtuales cuando la comunicación discurra por redes fuera del propio Dominio de Seguridad utilizando, preferentemente, dispositivos hardware para el establecimiento y utilización de red privada virtual.

Para los accesos remotos a la red corporativa, se habilitan canales VPN para tratar convenientemente la información transmitida, los sistemas y recursos accedidos, la identidad de las personas que realizan dichos accesos y las posibles implicaciones que el acceso en global conlleva.

Aspectos concretos a desarrollar en la normativa

Se debe disponer de un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico ha de atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.

- Para las comunicaciones fuera del dominio se debe asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

- Se previenen ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos:
    a. La alteración de la información en transito
    b. La inyección de información espuria
    c. El secuestro de la sesión por una tercera parte

- Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.

6.5 Gestión del Parque de Puesto de Trabajo Digital

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Restricciones	Medida de Seguridad	B	
Mp.eq.3	Protección de los equipos portátiles	Aplica	Normativa de Gestión del Parque de Puesto de Trabajo Digital

Fundamento de la Normativa

Para tener una gestión adecuada del parque del Puesto de trabajo el Ayuntamiento debe establecer sobre este, un mantenimiento preventivo programado y una gestión de incidencias y por lo tanto no programado y correctivo. El mantenimiento preventivo está basado comprobar que los PTD están configurados y operativos tal y como se definen en las políticas.

La gestión de incidencias del parque de puesto de trabajo se lleva a cabo sobre la base de la comunicación al proveedor de servicios.

Dada esta circunstancia particular sobre la contratación del mantenimiento de los puestos de Trabajo Digital, la empresa tiene la facultad de acceder a datos que puedan contener, con la alta posibilidad de que estos puedan contener información de carácter personal de los propios empleados o de los clientes. Es por eso que la

empresa prestataria se constituye en Encargado del Tratamiento y en tal calidad se compromete al cumplimiento de todo lo dispuesto en la Política de Seguridad de la Información del Ayuntamiento y las normativas de Seguridad relacionadas.

Aspectos concretos a desarrollar en la normativa

El cumplimiento de nivel básico concreta sobre todo a la gestión de los equipos portátiles, es decir, los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, y que deben ser protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se deben adoptar las siguientes:

- Se debe llevar un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.
- Se debe establecer un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.
- Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados (Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza, por ejemplo redes inalámbricas públicas (Wifi)).
- Se debe evitar, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se consideran claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

6.6 Gestión de los Logs de los Sistemas

La combinación de la Aplicabilidad y el Anexo II del Esquema Nacional de seguridad permite concretar el ámbito de actuación de la normativa:

Restricciones	Medida de Seguridad	B	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Normativa de Gestión de los Logs de los Sistemas

Fundamento de la Normativa

Los servicios, sistemas y aplicaciones del ayuntamiento generan logs que deben ser gestionados adecuadamente, bien por motivos legales, bien por motivos de regulación o/y operativos (resolución de problemas, estadísticas, respuesta ante incidentes y análisis forense y de auditoría…).

Los sistemas de información y comunicaciones de servicios del Ayuntamiento son monitorizados con la finalidad doble de garantizar la trazabilidad y de, llegado el caso, identificar comportamientos anómalos o sospechosos. Toda actividad relevante del sistema queda registrada para posibilitar su análisis posterior.

Quedan registradas las actividades de los usuarios del Ayuntamiento, así como la de los administradores de los sistemas.

Como norma general, el registro de sucesos (recolección de logs) es siempre obligatorio en todos los sistemas que contengan información CONFIDENCIAL o de CARÁCTER PERSONAL. También en aquellos equipos que conforman el perímetro de seguridad (los cortafuegos, por ejemplo).

El objetivo principal del registro de logs debe ser proporcionar trazabilidad adecuada sobre los accesos al sistema, actividades de administración y eventos relacionados de acuerdo con su nivel de criticidad.

Aspectos concretos a desarrollar en la normativa

Se registran las actividades de los usuarios en el sistema, de forma que:

a) El registro indica quién realiza la actividad, cuándo la realiza y sobre qué información.
b) Se debe incluir la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
c) Debe registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema.

Se activan los registros de actividad en los servidores.