centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 883

Guía de Implantación del ENS para EELL

Mayo 2020

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

© Centro Criptológico Nacional, 2020
NIPO :083-19-183-2

Fecha de Edición: mayo de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Las Administraciones Públicas se han fijado como objetivo crear las condiciones adecuadas para el desarrollo de nuevos servicios ligados a la evolución de la tecnología y promover e impulsar, de igual modo, su uso entre la ciudadanía y las empresas. Esta evolución conlleva también una mayor facilidad para el tratamiento de gran cantidad de información, la cual debe ser debidamente protegida.

Para dar respuesta a un marco común de seguridad de la información en las administraciones públicas y su sector público, en desarrollo de la Ley 11/2007, de 22 de junio, se aprobó el Real Decreto 3/2010, de 8 de enero, por el que se reguló el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, mediante el que se establecen los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios. Tras la aprobación de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, se da un impulso definitivo a la implantación de los procesos electrónicos en las administraciones públicas consagrándose la comunicación electrónica entre la Administración y la ciudadanía, haciéndose imprescindible garantizar el cumplimiento de los mencionados principios básicos y requisitos mínimos estableciendo las medidas de seguridad necesarias que habrán de ser proporcionales a las dimensiones de seguridad relevantes y a la categoría del sistema de información a proteger.

El apoyo para la implantación del ENS a las Entidades Locales, tiene su principal objetivo en que estas dispongan de sistemas seguros para el ejercicio de sus competencias, de asistencia y cooperación económica y técnica en el caso de las Diputaciones, Cabildos, Consejos Insulares o los órganos competentes equivalentes, y en los Ayuntamientos en su relación directa con la ciudadanía.

2. OBJETIVO Y ALCANCE DE LA GUÍA

Esta guía va dirigida a las Entidades Locales, con el objetivo de proporcionar unas líneas generales para abordar el proceso de implantación del ENS en sus sistemas. Se ha diferenciado por un lado las Diputaciones, Cabildos, Consejos Insulares o los órganos competentes equivalentes y por otro, teniendo en cuenta también el papel que estas desempeñan en lo relativo a la colaboración con los Ayuntamientos en la provisión de servicios o soluciones de administración electrónica acordes al ENS, en Ayuntamientos de menos de 20.000 habitantes y Ayuntamientos de más de 20.000 y menos de 75.000 habitantes. También se ha tenido en cuenta la relación de las Entidades Locales con el sector privado como proveedor de servicios o soluciones para las Administraciones Públicas acordes también al ENS.

En cuanto al proceso de implantación el objetivo es comenzar con el desarrollo del Plan de Adecuación, que se iniciará con la organización de la seguridad en la Entidad Local, mediante la designación de roles de seguridad y constitución de un comité de seguridad, siendo estos instrumentos esenciales en la implantación del ENS. Esta

organización junto con los compromisos de seguridad se reflejará en la Política de Seguridad documento que tiene carácter público. El resto de documentos del Plan, ya de carácter interno, identificarán y planificarán las medidas de seguridad que será necesario llevar a cabo.

Los Ayuntamientos de menos de 20.000 habitantes podrán apoyarse en las Diputaciones u Organismos competentes durante este proceso. Los Ayuntamientos de más de 20.000 habitantes deberán tener en cuenta que cuando recurran a servicios externalizados, estos deberán disponer de la conformidad con el ENS.

Una vez realizado y aprobado el Plan de Adecuación, se llevará a cabo el plan de medida de seguridad, con el objetivo final de superar el proceso de Certificación del sistema. Iniciando así el ciclo de mejora, mediante la revisión y mejora continua de los procesos de seguridad.

3. PLAN DE ADECUACIÓN AL ENS

El plan de adecuación es el punto de partida para abordar el proceso de implantación del ENS, y está compuesto por las siguientes actuaciones:

- Elaborar la **Política de seguridad.**
- **Categorizar los sistemas**. Valoración de Servicios e Información.
- Realizar el **análisis de riesgos.**
- Elaborar la **declaración de aplicabilidad**- Perfil de Cumplimiento Específico.
- Desarrollar un **Plan de mejora de la seguridad** en base al informe de insuficiencias detectadas.

Con su elaboración, por un lado, se identificarán las personas u órganos responsables de que la implantación del ENS se lleve a cabo y por otro las medidas de seguridad que será necesario implantar, los recursos necesarios para llevarlas a cabo, y los plazos para ejecutarlas.

3.1 Política de seguridad

La **Política de seguridad** es un documento de alto nivel, mediante el cual la Entidad Local define su compromiso respecto a la seguridad de los servicios (trámites electrónicos) proporcionados a la ciudadanía y la información que estos gestionan. En la Política se describirán los mecanismos que se han implementado para garantizar la gestión continuada de la seguridad y los responsables que se han establecido para velar por su cumplimiento. Entre otros, en su redacción se contemplará la inclusión de los siguientes contenidos:

- El compromiso de la organización con el cumplimiento de todo el articulado del Real Decreto ENS (principios básicos y requisitos mínimos).
- El marco legal y regulatorio.

- Referencia a la forma en la que la organización da cumplimiento a la normativa de protección de datos.
- Los roles de seguridad designados, sus funciones, el proceso de designación, así como de renovación, contando al menos con los siguientes:
    - El Responsable de la Información y el Responsable de los Servicios, para aquellos sistemas de información que no sean operados por terceros públicos o privados.
    - El Responsable de Seguridad y El Responsable del Sistema, (siempre que sea posible, estos deberán estar diferenciados), la estructura del Comité de Seguridad y sus funciones.
- Los mecanismos que se han implementado para que los roles de seguridad actúen de forma coordinada y consensuada, así como los mecanismos implementados para la resolución de los conflictos que pudieran surgir entre estos (pudiendo ser el propio Comité de Seguridad).
- La forma en la cual se va a desarrollar la Política de Seguridad, indicando que está se articulará, mediante el desarrollo de un sistema de gestión de la seguridad de la información documentado y con un proceso regular de aprobación. Así como la periodicidad de la revisión de la política.

Los Ayuntamientos podrán elaborar su propia Política de seguridad o bien acogerse a la Política de la Entidad Local comarcal o provincial a la que pertenecen. No obstante, en estos casos, los Ayuntamientos deberán designar sus propios roles de seguridad, al menos deberán contar con Responsables del Servicio y Responsables de la Información.

En los anexos se proporcionan modelos para la designación de roles y la constitución del Comité de Seguridad y para la elaboración de Política de seguridad.

3.2 Categorizar los sistemas

Para realizar la categorización de sistemas, se procederá a la identificación de los servicios y la información que estos gestionan para posteriormente proceder a su valoración, y en base a esta determinar la categoría del sistema.

La valoración de los servicios y la información se realizará conforme a las instrucciones del Anexo I del RD ENS, determinando el impacto, que tendría un incidente de seguridad que afectaría a la información tratada o a los servicios prestados, en cada una de las cinco dimensiones de seguridad (Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C], Trazabilidad [T]). Este impacto se mide en tres niveles BAJO, MEDIO O ALTO y la realizarán sus respectivos responsables, que podrán tener en cuenta la opinión del Responsable de Seguridad y/o del Responsable del Sistema. Una vez valorados, se procederá a la determinación de la **Categoría del Sistema**, pudiendo ser en este caso BÁSICA, MEDIA o ALTA, de acuerdo a lo indicado en el Anexo I del Real Decreto ENS. La categorización de los sistemas se plasmará en un documento que será aprobado por el Responsable del Sistema.

En los anexos se proporciona un inventario tipo de servicios e información, junto con su valoración.

3.3 Análisis de riesgos

El **análisis de riesgos**, será acorde a lo establecido en el Anexo II del RD ENS. Para su realización se recomienda utilizar la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica -. MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA en http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html. Esta metodología permite estudiar los riesgos que soporta un sistema de información determinando, de este modo, las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Para realizar el análisis de riesgos se puede utilizar la herramienta de referencia PILAR, que implementa la metodología MAGERIT, en cualquiera de sus versiones (PILAR, PILAR Basic, µPILAR y online a través de la plataforma INÉS). Las Guías CCN-STIC-470 PILAR proporcionan manuales de uso en sus diferentes versiones.

3.4 Declaración de aplicabilidad

Se elaborará la **declaración de aplicabilidad** mediante la selección de las medidas de seguridad del Anexo II del Real Decreto ENS, que sean de aplicación al sistema, de acuerdo con los valores máximos de impacto obtenidos en cada una de las dimensiones de seguridad y/o de acuerdo con la categoría del sistema y las medidas de seguridad adicionales resultantes del análisis de riesgos. La declaración de aplicabilidad se plasmará en un documento que debe ser aprobado formalmente por el Responsable de Seguridad. Para realizarla, se puede tomar como referencia el Informe de Buenas Prácticas (BP). En los anexos se proporciona un modelo para su elaboración.

En este punto se estaría en condiciones de acogerse a uno de los **Perfiles de Cumplimiento Específico para EELL,** siendo entonces de aplicación la declaración de aplicabilidad asociada a este perfil en concreto. Su adopción deberá estar argumentada formalmente.

3.5 Plan de mejora de la seguridad

El **informe de Deficiencias del sistema (gap analysis)**, recogerá el estado de cumplimiento de las medidas de seguridad, reflejando el nivel actual de madurez de las medidas de la declaración de aplicabilidad. Este informe se puede completar también con aquellas medidas que sea necesario implantar para garantizar el cumplimiento de la normativa de protección de datos.

El informe contendrá, por tanto, lo que se consideran los riesgos residuales del sistema, que deberán ser aceptados formalmente por los Responsables de los Servicios y por los Responsables de la Información.

Finalmente, habrá que identificar las tareas que será necesario realizar para subsanar las deficiencias del sistema, planificarlas, asignarles los recursos necesarios (personales y/o económicos, según sea el caso) y recogerlas en un documento, que se denominará **Plan de mejora de la seguridad**, que deberá ser aprobado formalmente por el Comité de Seguridad, comprometiéndose la organización, de este modo, con la mejora de la seguridad. En los anexos se proporciona un modelo a seguir.

4. IMPLANTANDO MEDIDAS

4.1 Marco organizativo [org]

La primera medida que se encuentra dentro de este grupo es el desarrollo de la **política de seguridad**, documento que se habrá elaborado para la realización del Plan de Adecuación.

La siguiente medida es el desarrollo de la **normativa de seguridad,** que consiste en la elaboración de un conjunto de normas, mediante la cual se dará traslado a los usuarios del sistema de información, de las normas de uso aceptable de los recursos TIC (Tecnologías de la Información y Comunicaciones), que se ponen a su disposición. Respecto a su estructura y contenidos, se contemplará que incluya al menos los siguientes aspectos:

- Alcance: ¿a quién afecta? al personal propio, cargos políticos, personal de terceros, etc.
- Vigencia: fecha de entrada en vigor.
- Aprobación y revisión: órganos a los que corresponde su aprobación y/o revisión y periodicidad de la misma.
- Regulación del uso correcto de todos los recursos TIC, correo, Internet, soportes de información, impresoras, carpetas de red, etc.
- Qué se considera uso indebido: se debe indicar claramente lo que está permitido y lo que no, en el uso de los recursos TIC.
- Régimen disciplinario: consecuencias en caso de incumplimiento.

Otro aspecto relevante a tener en cuenta, es la forma en la cual se va a dar difusión a la normativa, prestando especial atención a que los usuarios la comprendan y acepten. El cumplimiento de este control está relacionado también con los siguientes:

- **Deberes y obligaciones [mp.per.2],** mediante la normativa se da traslado al personal de sus funciones y obligaciones en materia de seguridad.
- **Concienciación [mp.per.3],** una de las materias a tener en cuenta para las actividades de concienciación es trasladar a los usuarios la normativa de seguridad. Por tanto, se recomienda, realizar las acciones de concienciación necesarias para dar a conocer la normativa de seguridad. La aceptación

expresa de su contenido se puede recabar mediante la realización de un pequeño cuestionario tras las acciones de concienciación.

- **Acceso local [op.acc.6],** esta medida indica que el sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso. Por tanto, en ese mensaje se puede recordar la existencia de una normativa de seguridad, dónde se puede consultar y que el uso del sistema implica la aceptación de dichas normas.

La "Guía CCN-STIC-821 Normas de Seguridad en el ENS" y sus apéndices, pueden servir de base para el desarrollo de la normativa de seguridad.

Para la elaboración de los **procedimientos de seguridad**, se tendrá en cuenta que estos describan las principales tareas que se realizan sobre el sistema, indicando quiénes son los responsables de su ejecución. Estos documentos podrían contener al menos los siguientes apartados:

- Objetivo: qué tareas va a describir el documento.
- Alcance: a qué sistemas y/o personal afecta.
- Desarrollo: descripción de las tareas a realizar.
- Responsabilidades: indicación de quién va a realizar cada tarea. Esto se puede reflejar en este apartado o bien puede ir indicándose en el apartado "desarrollo".
- Comunicación de deficiencias del procedimiento: correo, persona, aplicación donde se deben comunicar las inconsistencias y/o errores que presente el documento, al objeto de que los responsables del mismo procedan a su corrección.
- Otros:
    - Referencias: documentos (guías, informes, etc.) que se han tomado como referencia para la elaboración del procedimiento.
    - Definiciones: que se consideran necesarias para entender el procedimiento.
    - Registros relacionados: evidencias de cumplimiento de lo indicado en el procedimiento.
    - Otros: cualquier otro apartado que se considere que proporciona información complementaria al procedimiento.

La "Guía CCN-STIC-822 Procedimientos de Seguridad en el ENS" y sus anexos, pueden servir de base para el desarrollo de los procedimientos.

En la definición del **proceso de autorización** se contemplará que la entrada y/o utilización de los diferentes elementos que forman parte del sistema (uso de instalaciones, entrada de equipos y/o aplicaciones en producción, establecimiento de

enlaces y/o la utilización de medios de comunicación, utilización de soportes de información y/o equipos móviles o bien el uso de servicios de terceros), se realiza tras contar con la correspondiente autorización, mediante la definición y documentación de quién o quiénes tienen la capacidad de autorizar el uso o la utilización de cada uno de los mencionados recursos. Implementar este proceso en una herramienta de Help Desk o similar facilita el registro de las evidencias de su realización.

4.2 Marco operacional [op]

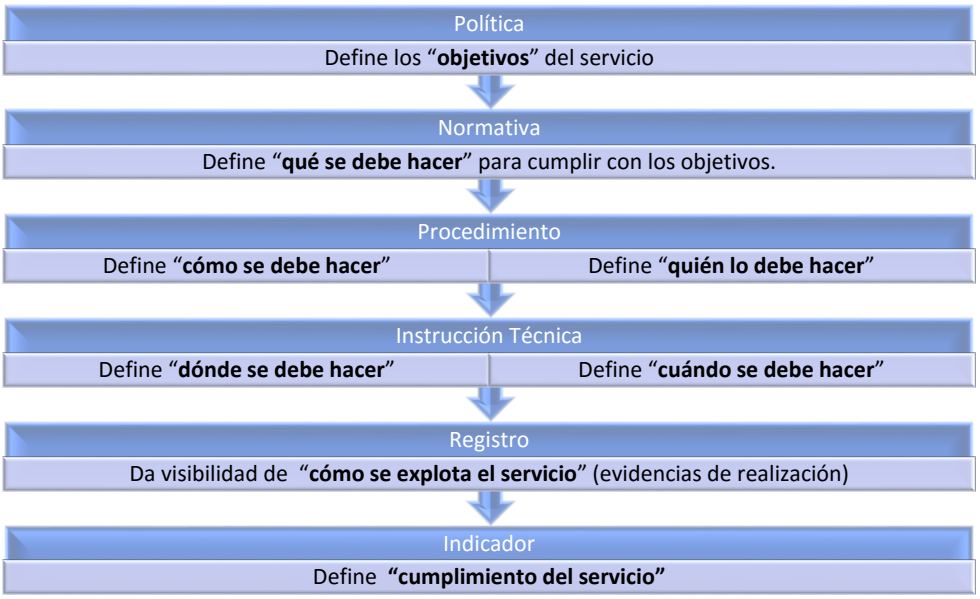
El marco operacional se estructura en varios grupos de medidas, las cuales se analizan a continuación.

4.2.1 Planificación [op.pl.1]

Para el **análisis de riesgos**, que ya se habrá realizado para la elaboración del Plan de Adecuación, se tendrá en cuenta que se debe actualizar, al menos, anualmente o bien cuando haya cambios relevantes en el sistema.

La definición de la **arquitectura de seguridad** se estructura en dos bloques, por un lado, hay que detallar de forma precisa las instalaciones, equipos, redes, puntos de acceso al sistema, líneas de defensa, etc., esta información se puede reflejar en esquemas de red físicos y lógicos. Por otro lado, hay que disponer de un Sistema de Gestión de Seguridad de la Información que recoja toda la documentación que da soporte al cumplimiento del ENS. Es recomendable que el sistema esté actualizado y que se apruebe periódicamente. La organización, estructura, ubicación, etc. de esta documentación es conveniente reflejarla en un procedimiento que contenga al menos los siguientes apartados:

- Tipo de documentos: políticas, normativas, procedimientos, instrucciones técnicas, registros, indicadores.
- Organización de la documentación: organización de la documentación (estructura de carpetas).
- Identificación de la documentación: nomenclatura de los documentos.
- Estructura de la documentación: portada, encabezado, primera página del documento, desarrollo del documento (contenido). Esto deberá estar alineado con lo indicado en Procedimientos de seguridad [org.3].
- Responsables de elaboración, revisión y aprobación de la documentación: teniendo en cuenta las obligaciones establecidas por el Real Decreto ENS.
- Ubicación y difusión de la documentación: lugar donde se almacenará la documentación y como se dará a conocer a las partes afectadas.
- Documentos vigentes y obsoletos: cómo se identificarán los documentos vigentes, donde se almacenarán los obsoletos.
- Registros: donde se almacenarán los registros: ofimática, aplicaciones, etc.



Tipo de documentos

Antes de la **adquisición de nuevos componentes** con carácter previo, se realizará un estudio donde se reflejará que se han tenido en cuenta los resultados del **análisis de riesgos**, y que es acorde a la **arquitectura de seguridad**. También incluirá las necesidades técnicas, de formación y de financiación.

Antes de la puesta en explotación de un nuevo elemento se llevará a cabo un estudio de las necesidades que requerirá respecto al **dimensionamiento /gestión de capacidades** relativos al procesamiento, almacenamiento de información, comunicación, personal, instalaciones y medios auxiliares, dejando constancia de su realización. Se recomienda dicho estudio, no solo antes de la puesta en explotación, si no de manera continua y mediante la utilización de herramientas de monitorización de la capacidad.

También es recomendable que se valore la adquisición **de componentes certificados**, mediante la utilización de sistemas, productos o equipos certificados cuyas funcionalidades de seguridad hayan sido evaluadas conforme a normas europeas o internacionales y estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Se tendrá en cuenta:

- Los recogidos en la "Guía CCN-STIC 105. Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación, CPSTIC", recomendados por el CCN. (https://oc.ccn.cni.es/index.php/es/)
- Los que dispongan de la certificación LINCE, para productos de seguridad TIC desarrollada por el Centro Criptológico Nacional, que acredita la capacidad de un producto TIC para manejar información de forma segura.
- Los que dispongan de la certificación Common Criteria (commoncriteriaportal.org).

4.2.2 Control de acceso [op.acc]

El proceso de **identificación** de usuarios (o procesos) en el sistema se implementará asegurando que cuenten con un identificador único (cuentas individualizadas) de tal forma que permita conocer a quién pertenece, y con qué privilegios. Cuando los usuarios dejen la organización, hayan sido cesados en su función o se les hayan revocado los permisos, se inhabilitarán sus cuentas, manteniendo los registros de actividad asociados durante el periodo de retención, que previamente se haya establecido.

Los **requisitos de acceso** a la información se recogerán en una política o normativa que indique quiénes tienen capacidad de otorgar los accesos a los recursos y la forma de solicitarlos. Este **proceso de gestión de derechos de acceso** se realizará en base al cumplimiento de los principios de "mínimo privilegio", "necesidad de conocer" y "capacidad de autorizar".

Se definirá una política de acceso de los usuarios, teniendo en cuenta que se debe establecer una **segregación de funciones y tareas**, asegurando la concurrencia de dos o más personas, para aquellas tareas consideradas como críticas y separando funciones incompatibles: desarrollo de operación; configuración y mantenimiento de operación; y auditoría de cualquier otra función. Si esta medida no se puede aplicar por falta de personal, será necesario implementar una medida compensatoria, como por ejemplo la activación de registros de actividad de las actuaciones de estos usuarios sobre el sistema de información. Registro que solo podrá ser accesible por personal autorizado. Como apoyo a estas actividades pueden emplearse las guías CCN-STIC 819 Medidas compensatorias y CCN-STIC 831 Registro de la actividad de los usuarios.

Para la implementación del doble factor como **mecanismo de autenticación,** se podrán combinar los siguientes factores: "algo que se sabe" (contraseñas o claves concertadas), "algo que se tiene" (certificados, aplicaciones móviles, etc.) y algo que se es" (elementos biométricos). Por ejemplo, si los equipos de usuario, se encuentran en zonas controladas que no son de acceso al público y disponen de un control de acceso, este sería uno de los factores, y el segundo factor sería el mecanismo de autenticación lógico realizado desde los equipos para el acceso al sistema. Para las contraseñas, se aplicarán políticas de calidad de las contraseñas: complejidad, longitud, etc. y se cambiarán con la periodicidad marcada en la política de la organización, siendo recomendable que no sea superior a seis meses.

En el **acceso local**, el realizado desde los puestos de trabajo dentro de las propias instalaciones, se procurará que en los diálogos de acceso se proporcione solamente la información indispensable. También se establecerá una limitación de intentos de acceso, se registrarán los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad. Una vez otorgado el acceso se informará al usuario de sus obligaciones.

Para el **acceso remoto**, el realizado desde fuera de las instalaciones, se implementará doble factor de autenticación y se establecerá una normativa específica de lo que puede hacerse remotamente.

4.2.3 Explotación [op.exp]

El **inventario de activos** detallará todos los elementos del sistema indicando su naturaleza e identificando a su responsable. Las herramientas de detección automática de los elementos que se encuentran conectados a la red permitirán mantener actualizado el inventario.

Se definirá y documentará la **configuración de seguridad** (bastionado) mínima de los principales componentes del sistema: equipamiento (seguridad perimetral, electrónica de red, servidores (físicos, virtuales), bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.), de tal forma que se asegure que antes de que estos elementos entren en operación se les haya aplicado dicha configuración. Para su elaboración es posible apoyarse en los recursos proporcionados por el CCN-CERT: Clara, Rocío, etc. Así mismo, se establecerán responsables de la **gestión de la configuración**, que se encargarán de su actualización cuando surjan cambios derivados de la aparición de vulnerabilidades, anuncios del fabricante, gestión de un incidente de seguridad, acciones de mantenimiento del sistema, cambios programados, etc.

Para el **mantenimiento** físico y lógico del sistema se atenderá principalmente a las especificaciones del fabricante y se analizará, priorizará y determinará cuándo se deben aplicar las actualizaciones de seguridad o la corrección de defectos, siendo recomendable que las pruebas se realicen en un entorno aislado, que no se encuentre en producción.

Para mantener un control sobre los cambios en el sistema se implantará un proceso de **gestión de cambios**, que tenga en cuenta que deben ser planificados para reducir el impacto sobre los servicios, que deben contar con la autorización pertinente, y que contemple las pruebas necesarias antes de que se pongan en producción.

Todos los equipos (puestos de usuario, servidores, elementos perimetrales), dispondrán de **protección frente a código dañino,** que se mantendrá conforme a las instrucciones del fabricante.

Se contará con un procedimiento integral para la **gestión de incidentes y registro de la gestión de incidentes de seguridad**, que, además, tenga en cuenta las obligaciones impuestas por la normativa de protección de datos. A este respecto, serán de aplicación la **"Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad[1]"**, aprobada por Resolución de 13 de abril de la Secretaría de Estado de Función Pública, donde se establece que las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información y el **artículo 33 "Notificación de una violación de la seguridad de los datos**

[1] Establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

personales a la autoridad de control" del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). La utilización de la herramienta LUCIA, como ventanilla única para la comunicación de incidentes, facilitará notablemente la gestión de los incidentes de seguridad.

Se mantendrá un **registro de la actividad de los usuarios** en el sistema y se desarrollará una normativa que determinará, en base a los riesgos, las actividades a registrar, teniendo en cuenta que, como mínimo, se registrará la actividad sobre los servidores. Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones que resulten de aplicación. Se recomienda realizar una sincronización del reloj del sistema, mantener el registro al menos 2 años y asegurar que este solo es accesible por personal autorizado. Se recomienda disponer de herramientas que permitan analizar y revisar la actividad de los usuarios sobre el sistema. Como apoyo para el establecimiento de este registro puede utilizarse la guía CCN-STIC 831 Registro de actividad de los usuarios.

Se implantarán mecanismos que garanticen la **protección de claves criptográficas** durante todo su ciclo de vida: generación, transporte, custodia, retirada y destrucción.

4.2.4 Recursos externos [op.ext]

Con carácter previo a la utilización de recursos externos, ya sean servicios, productos, instalaciones o personal, se definirán los requisitos de seguridad a tener en cuenta en la **contratación y** en el establecimiento de los **acuerdos de nivel de servicio,** que se incorporarán en los pliegos y/o peticiones de ofertas. Así mismo, estos contemplarán lo que se considera "servicio mínimo admisible", definiendo las responsabilidades de los prestadores y las consecuencias de los incumplimientos.

En la contratación de servicios se solicitará la conformidad con el ENS, en la categoría alcanzada por los sistemas afectados, de acuerdo con lo establecido en la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se describe la obligación de exigir a los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, la conformidad con el Esquema Nacional de Seguridad.

Para medir el cumplimiento de lo que se ha establecido como calidad mínima del servicio se implantará un proceso rutinario de **gestión diaria,** para medir los niveles acordados, que defina también los procedimientos de coordinación necesarios para las tareas de mantenimiento, así como la reacción frente a incidentes y desastres. Se recomienda tener en cuenta, en caso de que sea necesario, la protección de la cadena de suministro, mediante el análisis de las consecuencias que pudiera tener sobre el sistema un incidente en la misma. De igual modo, se recomienda que, para la **i**nterconexión de sistemas para el intercambio de información y prestación de servicios,

se cuente siempre con autorización expresa, que irá acompañada de documentación detallada sobre la interfaz, las medidas de seguridad, etc.

4.2.5 Continuidad del servicio [op.cont]

Se determinarán los requisitos de disponibilidad de cada servicio, y los elementos críticos para su prestación, mediante la realización de un **análisis de impacto.** Si se considera conveniente, se puede desarrollar un **plan de continuidad** que contemple la disponibilidad de los **medios alternativos** necesarios para garantizar la prestación de los servicios. En caso de que se elabore tal plan, se deberán prever **pruebas periódicas** del mismo.

4.2.6 Monitorización del sistema [op.mon]

El sistema contará con herramientas de **detección o prevención de intrusión,** preferentemente basadas en reglas y se recomienda disponer de un sistema automático de recolección de eventos de seguridad, a ser posible que permita la correlación de los mismos.

Para la recopilación de los datos necesarios para dar respuesta a la encuesta INES (Informe Nacional sobre el Estado de la Seguridad- artículo 35), será necesario definir un **sistema de métricas,** junto con los indicadores asociados, que permita conocer el grado de implantación de las medidas de seguridad que son de aplicación al sistema, así como la información necesaria para cumplimentar la encuesta. También se definirán los indicadores necesarios para conocer el estado del sistema de gestión de incidentes. Para apoyar esta definición de indicadores puede utilizarse la guía CCN-STIC 815 Esquema Nacional de Seguridad. Métricas e indicadores.

4.3 Medidas de protección [mp]

4.3.1 Protección de las instalaciones e infraestructuras [mp.if]

El equipamiento estará protegido mediante su disposición en **áreas separadas y con control de acceso**, que permita la **identificación de las personas** que acceden a las mismas, mediante su registro de entrada y salida. Estos accesos se revisarán a intervalos regulares.

En el **acondicionamiento de los locales** se tendrá en cuenta que estos dispongan de unas condiciones adecuadas de temperatura y humedad, que el cableado se encuentra protegido y que se han implementado las protecciones necesarias, fruto del análisis de riesgos. Se evidenciarán los mantenimientos y revisiones realizadas.

Los locales dispondrán de la **energía eléctrica** necesaria mediante el establecimiento de las suficientes tomas eléctricas y se garantizará el suministro eléctrico, siendo recomendable que, aun fallando el suministro general, se disponga del tiempo suficiente para la terminación ordenada de todos los procesos. Se evidenciarán los mantenimientos y las revisiones realizadas.

La **protección frente a incendios** será acorde, como mínimo, a la normativa industrial. Se evidenciarán los mantenimientos y revisiones realizadas. En caso de que sea necesario también se contará con **medidas de protección frente a inundaciones**.

Se mantendrá un **registro de entrada y salida de equipamiento,** que contará con la autorización correspondiente.

4.3.2 Gestión del personal [mp.per]

Las responsabilidades en materia de seguridad estarán asociadas a la **caracterización del puesto de trabajo** y se definirán en base a los riesgos. El personal conocerá los **deberes y responsabilidades** de su puesto de trabajo y las medidas disciplinarias en caso de incumplimiento. Para personal de terceros, estos requisitos se establecerán en los contratos de prestación de servicios.

La Entidad Local realizará acciones de **concienciación** sobre las responsabilidades del personal respecto a la seguridad del sistema, especialmente relacionadas con la normativa de seguridad, la identificación de incidentes de seguridad y la forma de comunicarlos. Se recomienda realizar una planificación anual. También realizará acciones de **formación** en materia de seguridad de la información, necesarias para el desempeño de las funciones del personal, especialmente relativas a la configuración de sistemas, detección y reacción frente a incidentes y gestión de la información en cualquier tipo de soporte. Se recomienda realizar una planificación anual.

4.3.3 Protección de los equipos [mp.eq]

Para garantizar la seguridad de la información se realizará una normativa que establezca la necesidad de mantener los **puestos de trabajo despejados** del material que no es necesario, guardándolo en lugar cerrado, siempre que sea posible. Esta normativa podrá formar parte de la normativa de seguridad general.

Los equipos incluirán en su configuración la activación del **bloqueo de puesto de trabajo** para que, transcurrido un tiempo de inactividad, sea requerida una nueva autenticación. Si fuera posible, se recomienda que, tras el suficiente tiempo de inactividad, se cancelaran las sesiones abiertas. Se recomienda establecer una normativa al respecto, para que los usuarios bloqueen de forma proactiva sus equipos en sus ausencias del puesto de trabajo. Esta normativa podrá formar parte de la normativa de seguridad general.

Se implementarán medidas específicas para la **protección de los equipos portátiles**, mediante el establecimiento de un control regular de los mismos, su inventario y registro de la persona responsable de su custodia, así como el establecimiento de canales de comunicación de pérdida, robo o incidentes de seguridad. Si se considera necesario, se deberán proteger mediante cifrado, desarrollándose la instrucción técnica asociada. Se elaborará una normativa específica respecto a su uso y las medidas a adoptar, que se podrá incluir en la normativa de seguridad general.

4.3.4 Protección de las comunicaciones [mp.com]

Se dispondrá un sistema de protección perimetral que establezca un **perímetro seguro** que separe la red interna del exterior. Los flujos de información deberán contar con la autorización correspondiente.

La **protección de la confidencialidad** de las comunicaciones se garantizará mediante el uso de redes privadas virtuales (VPN). La **protección de la autenticidad y de la integridad** de las comunicaciones se garantizará mediante la implementación de los mecanismos de autenticación correspondientes y se prevendrán, o como mínimo, se detectarán, los ataques habituales a la información en tránsito: alteraciones de información, inyección de información espuria o secuestros de sesión.

Cuando sea necesario, se mitigarán los efectos de propagación de los incidentes de seguridad y se controlará el acceso a la información mediante una adecuada **segregación de redes**, teniendo en cuenta que los equipos solo accedan a la información necesaria y se aíslen las comunicaciones inalámbricas.

4.3.5 Protección de los soportes de información [mp.si]

El **etiquetado** de los soportes y las medidas a aplicar sobre los mismos, se establecerán conforme a la calificación de información que contienen, siendo necesario el desarrollo de los procedimientos asociados.

Se utilizará **criptografía** para proteger la información en dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga), garantizando la confidencialidad e integridad de la información contenida en los mismos.

La **custodia** se garantizará mediante la implementación de medidas de control de acceso físico y/o lógico y atendiendo las indicaciones respecto a temperatura, humedad, etc., establecidas por los fabricantes.

Se implementará un registro de entrada y salida de soportes que identifique al transportista que efectúa el **transporte**, con indicación de las personas que lo reciben y entregan, y un procedimiento para cotejar salidas con llegadas. Si la información contenida en el soporte está clasificada con un nivel que aconseje su cifrado, se aplicará esta medida para proteger la información durante el transporte.

Se implementarán y documentarán los **métodos de borrado y destrucción** a aplicar en función del dispositivo, garantizando que los soportes que vayan a ser reutilizados sean objeto de un borrado seguro y, cuando este no sea posible, se destruya de forma segura.

4.3.6 Protección de las aplicaciones informáticas [mp.sw]

En el caso de que la Entidad Local realice su propio software se aplicará y documentará una metodología de **desarrollo de aplicaciones** que garantice que estas se llevan a cabo en un sistema independiente, separado del de producción. Cuando sea de aplicación, se seguirá una metodología de desarrollo seguro que tenga en cuenta los

principios de mínimo privilegio y seguridad desde el diseño, regulando el uso de los datos de pruebas.

Antes de pasar a producción las aplicaciones se diseñará un **plan de aceptación y puesta en servicio** que contemple su correcto funcionamiento y la verificación de los criterios de seguridad que se hayan establecido. Adicionalmente, se realizarán análisis de vulnerabilidades y pruebas de penetración antes de la puesta en servicio de las aplicaciones desarrolladas.

4.3.7 Protección de la información [mp.info]

Cuando el sistema trate **datos de carácter personal**, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el ENS.

Se implementará y documentará un proceso de **calificación de la información**, que tenga en cuenta que esta se realizará según lo establecido legalmente sobre la naturaleza de la misma (Secreto, Reservado, Confidencial, Difusión Limitada/Restringido, Uso Oficial/Uso Interno, Uso Público) y los niveles de seguridad del anexo I del Real Decreto.

En cuanto a la **firma electrónica,** se emplearán los tipos previstos en el ordenamiento jurídico. En caso de que sea de aplicación, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período, de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin, se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

En caso de que exista información que sea susceptible de ser utilizada como evidencia electrónica en el futuro, es recomendable utilizar **sellos de tiempo** para garantizar la fecha de obtención.

Cuando los documentos vayan a ser difundidos ampliamente ya sea directamente o a través de su publicación en sitios web o sedes electrónicas, se definirá y documentará un proceso de **limpieza de documentos**, de tal forma que se garantice que con carácter previo a su difusión se ha eliminado toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores.

Se implementarán políticas de **copias de seguridad** que garanticen la recuperación de la información ante un incidente de seguridad, definiéndose su periodicidad y plazos de conservación. Es recomendable realizar pruebas periódicas de restauración.

4.3.8 Protección de servicios [mp.s]

Se implementarán medidas de **protección del correo electrónico** protegiéndolo de las amenazas que le son propias, protegiendo la información tanto en el cuerpo de los mensajes como en los anexos. Se deberán implementar mecanismos de protección frente al spam, programas dañinos y código móvil. La normativa de uso de los recursos puestos a disposición del personal regulará el uso del correo electrónico, definiendo lo que se considera un uso no autorizado del mismo. Se contemplarán actividades de concienciación y formación sobre el uso seguro del correo electrónico.

Se implementarán medidas que garanticen la **protección de servicios y aplicaciones web** de las amenazas que les son propias: acceso a la información obviando la autenticación, ataques de manipulación de URL, manipulación de cookies, ataques de inyección de código, escalado de privilegios, etc. Los sitios web emplearán certificados digitales de autenticación de sitio web que sean acordes con la normativa europea en esa materia.

Como medidas de **protección frente a la denegación de servicio,** el sistema se planificará y dotará de la capacidad suficiente para asumir la carga prevista con holgura y se desplegarán tecnologías para prevenir los ataques conocidos. Es recomendable el establecimiento de sistemas de detección y reacción ante los ataques de denegación de servicio.

5. CICLO DE MEJORA

En consonancia con lo establecido en el artículo 9 Reevaluación periódica del RD ENS, *"las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario",* se debe implantar un proceso interno que garantice dicha reevaluación periódica, con definición de las tareas que se deben realizar, su periodicidad y los responsables de su realización. Estas tareas serán como mínimo las siguientes:

- **Revisión de la Política de seguridad**. El comité de seguridad, con la periodicidad que se haya indicado en la propia política (normalmente con carácter anual), revisará la Política de Seguridad prestando especial atención a la aparición, durante ese periodo, de nuevas normas, legislación, instrucciones técnicas, que introduzcan cambios en las obligaciones en materia de seguridad.
- **Elaboración del Plan de Concienciación y Plan de Formación anual.** Con carácter anual se diseñarán las acciones de concienciación, para todo el personal, y las de formación, para el personal con responsabilidad en la operación sobre el sistema.
- **Revisión de la Normativa de seguridad**. El comité de seguridad revisará, al menos con carácter anual, la normativa de seguridad, con objeto de identificar si se encuentran regulados todos los recursos TIC puestos a

disposición de los usuarios, si las normas son eficaces y si se han derivado medidas disciplinarias.

- **Revisión de la Información y los Servicios, su valoración y proceso de categorización del sistema.** Los Responsables de la Información y los Responsables de los Servicios comunicarán al Responsable de Seguridad la aparición de nuevos activos de Servicios o Información, o cambios que pudieran afectar a la valoración de los mismos. Esto derivará en la revisión de la categorización del sistema.
- **Actualización del análisis de riesgos.** Con carácter anual, se revisará el análisis de riesgos y se aprobarán formalmente los riesgos residuales por parte de los Responsables de la Información y los Responsables de los Servicios. Los cambios relevantes sobre el sistema (cortafuegos, cabinas, servidores, etc.) que introduzcan componentes con nuevas tecnologías, requerirán también de una actualización del análisis de riesgos.
- **Revisión de la Declaración de aplicabilidad o del Perfil de Cumplimiento Específico.** El Responsable de seguridad revisará los cambios derivados de la actualización de la categorización del sistema, del análisis de riesgos, o bien del Perfil de Cumplimiento Específico, y procederá revisar la declaración de aplicabilidad.
- **Realización de auditorías internas**. Es conveniente establecer chequeos periódicos de cumplimiento al menos con carácter anual al objeto de:
    - **Revisar las medidas de seguridad**: verificar si las medidas de seguridad están correctamente implantadas y si son eficaces.
    - **Revisar los procedimientos:** verificar si los procedimientos reflejan correctamente las tareas existentes y la forma de llevarlas a cabo.
- **Revisión del Plan de Mejora de la Seguridad.** El comité de seguridad revisará el Plan a intervalos regulares. Con ello se comprobará si se están cumpliendo los hitos marcados, reprogramándolos en caso de que sea necesario y añadiendo aquellos que hayan surgido de la realización de las auditorías internas.
- **Revisión del Estado de la Seguridad. INES.** Asegurar, mediante la designación de responsables, que la encuesta se cumplimenta anualmente**.**
- **Auditorias de conformidad con el ENS.** Con carácter bienal se procederá a realizar auditorías de conformidad con el ENS.

6. ANEXOS

La Guía se complementa con los siguientes documentos:

6.1 AYUNTAMIENTOS <20.000 HABITANTES

6.1.1 PCE 883A - Perfil de Cumplimiento Específico Ayuntamientos (en base al Abstract Marco de Certificación ENS para Entidades Locales)

6.1.2 PCE 883B - Perfil de Cumplimiento Específico Ayuntamientos <20.000 habitantes

6.1.3 Anexo I. Plan de adecuación Ayuntamientos <20.000 habitantes

6.2 AYUNTAMIENTOS >20.000 Y <75.000 HABITANTES

6.2.1 PCE 883C - Perfil de Cumplimiento Específico Ayuntamientos >20.000 y <75.000 habitantes

6.2.2 Anexo II. Plan de adecuación Ayuntamientos >20.000 y <75.000 habitantes

6.3 DIPUTACIONES, CABILDOS, CONSEJOS INSULARES u ÓRGANO COMPETENTE EQUIVALENTE

6.3.1 PCE 883D – Perfil de Cumplimiento Específico Diputaciones, Cabildos, Consejos Insulares u Órgano Competente equivalente

6.3.2 Anexo III. Plan de adecuación Diputaciones, Cabildos, Consejos Insulares y Órgano Competente equivalente