AMETIC

GUÍA DE implantación del esquema nacional de Seguridad

CCN Centro Criptológico Nacional
ens Esquema Nacional de Seguridad
Gobierno de España · Ministerio de Política Territorial y Administración Pública
plan avanza2
Gobierno de España · Ministerio de Industria, Turismo y Comercio
Unión Europea · Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

GUIA DE IMPLANTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

Cofinanciado por:Proyecto de Difusión del Esquema Nacional de Seguridad (TSI-020100-2010-332). Ministerio de Industria, Turismo y Comercio, dentro del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2008-2011.
Edita: Ametic.

Con la colaboración del Centro Criptológico Nacional y el Ministerio de Política Territorial y Administración Pública.

Fecha de Edición: Enero de 2011

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, Ametic 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

ÍNDICE

0 PRÓLOGO

La Seguridad de la Información es ya hoy una realidad y algo que todas las organizaciones deben tener integrado en todos los niveles de su estructura, y principalmente en su dirección, si no quietren quedarse atrás en las medidas de actuación, dentro del hipersector TIC.

Cualquier empresa o institución debe contar ya con los profesionales y medios adecuados que le permitan dirigir y gestionar con éxito, la seguridad de sus recursos, tanto físicos como lógicos.

Para la administración pública española este proceso, de obligado cumplimiento, implica la aceptación del Esquema Nacional de Seguridad (ENS)

El ENS ayudará a que los ciudadanos puedan desarrollar, a través de medios digitales, gestiones relacionadas con la eAdministración con mayor seguridad y confianza en todos los procesos relacionados con sistemas, datos y comunicaciones electrónicas.

Lo que sin duda supone un impulso al desarrollo de la sociedad de la información.

En este desarrollo, no debemos olvidar, la necesidad de toda organización por contar con profesionales cualificados en la materia, responsables del óptimo control de los sistemas en lo que a control del riesgo y recuperación de la información se refiere.

Por ello, desde AMETIC, conscientes de la demanda de formación que en esta materia requieren tanto de las organizaciones como los profesionales, llevamos más 5 de años impartiendo un máster en dirección y gestión de seguridad de la información en colaboración con la Universidad Politécnica de Madrid.

Por esta razón, desde AMETIC, queremos animar a todas las organizaciones, tanto públicas bajo el ENS, como privadas bajo los distintos estándares existentes, a que fomenten la implantación de estos sistemas de seguridad de la información en sus organizaciones y cuenten con los profesionales y medios adecuados para lograrlo.

José Pérez García
Director general de AMETIC

1 PRESENTACIÓN

AMETIC nace como resultado de la fusión de AETIC y ASIMELEC. La nueva patronal española de la electrónica, las tecnologías de la información, las telecomunicaciones y los contenidos digitales, es un ejemplo de integración asociativa en nuestro ámbito a escala europea.

La Asociación, lidera a nivel nacional, los intereses empresariales de un hipersector tan diverso, como dinámico. AMETIC con más de 5.000 empresas asociadas, suman en su conjunto 350.000 empleados, cuya actividad económica supone en torno al 7% del PIB español. Un tercio del esfuerzo privado nacional en I+D, es llevado a cabo por nuestras empresas, lo que nos convierte en el sector más innovador, dinámico y con mayor capacidad de crecimiento de nuestra economía.

AMETIC cuenta con una Comisión de Seguridad Integral, la cual agrupa los intereses de empresas de los diferentes sectores de la Seguridad Integral.

Su misión principal es la mejora de la confianza y seguridad en la sociedad de la información, así como en el contexto integral de su desarrollo en todo el amplio espectro de la seguridad. Su objetivo se centra en concienciar y promover el uso de las tecnologías de seguridad de los sistemas de información aplicados a todos los ámbitos requeridos, ante los usuarios, administración y opinión pública en general.

En este contexto, AMETIC lidera el entorno que promueve la Seguridad de la Información, tanto para el sector privado, como para el público. La Asociación aúna lo esfuerzos de las empresas que, preocupadas por la continuidad de los sistemas, son capaces de aminorar los riesgos y definir las líneas de actuación que aporten las medidas necesarias, conforme a este Esquema recientemente aprobado, y multiplique los esfuerzos que realice en este sentido la Administración.

2 INTRODUCCIÓN

La Ley de Acceso de los Ciudadanos a la administración electrónica avisaba del desarrollo de dos Esquemas que necesariamente acompañarían a la Ley en su ejecución, los Esquemas Nacionales de Seguridad y de Interoperabilidad.

¿Por qué? Porque es de sentido común y de una previsión encomiable, prescribir que un servicio público que va a utilizar masivamente las Tecnologías de la Información y la Comunicación (TICs) tenga que ser seguro para los ciudadanos y compatible tanto con las tecnología que ellos usan como con las que usan las administraciones.

Los Esquemas Nacionales de Seguridad e Interoperabilidad son la respuesta a la pregunta que cualquier ciudadano se hará al enfrentarse al uso de la administración electrónica: ¿la tramitación que voy a realizar desde mi casa y mi ordenador va a ser igual que si lo hiciera en una ventanilla convencional, va a valer lo mismo?.

El objeto de esta Guía es transmitir conocimientos acerca de la seguridad de la información tal y como se entiende en el Esquema Nacional de Seguridad así como proporcionar unas pautas que ayuden en la tarea de aplicar el Esquema Nacional de Seguridad a aquellos que se tengan que encargar de ello.

3 OBJETIVOS

El objetivo principal de esta Guía es difundir los requisitos planteados por el ENS de una manera práctica. Se pretende por un lado, instruir sobre qué hay que hacer para cumplir con el ENS y por otro dar ideas sobre cómo hacerlo, desde el entendimiento de que cada entidad cuenta con unas características propias que es imposible recoger fielmente en una publicación de estas características.

4 CONTEXTO

Según datos recogidos por el Consejo Superior de Administración Electrónica1, en las Comunidades Autónomas hay un alto grado de implementación de las actuaciones incluidas en la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), como se puede ver en el Gráfico 1.

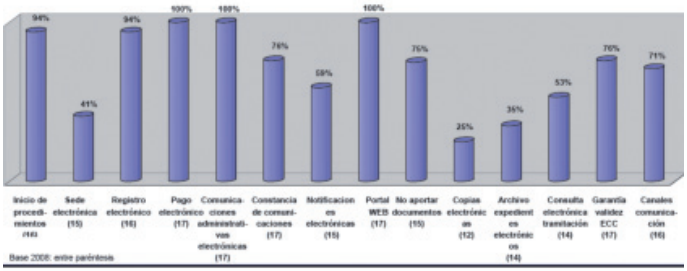

Gráfico 1 -Implementación de la servicios electrónicos en las AAPP.

*1 *Resultados del cuestionario de Administración Electrónica (año 2008), http://www.csae.map.es/csi/pdf/Informe_OAE_2008_definitivo.pdf*

Aunque se puede argumentar que el ENS no ha sido publicado en el mejor contexto económico, está claro para cualquier involucrado en el mundo de las TIC, que era completa y absolutamente necesario contar con un marco de trabajo como el ENS que permitiera a la Administración Pública avanzar en la modernización de sus actividades y estructuras, proporcionando una seguridad imprescindible en el actual contexto tecnológico. Si los ciudadanos cuentan con antivirus (91,7%), cortafuegos (80,0%) y actualizan el sistema operativo y programas (80,9%)2 , no se puede pedir menos a nuestra administración. Y además tiene que estar preparada para que estos ciudadanos concienciados por la seguridad informática le exijan un nivel de seguridad que les transmita confianza y permita un desarrollo masivo de la administración electrónica.

La eficacia y efectividad de la gestión de la Administración Pública pasa por el uso de la tecnología como motor de cambio, y para ello resulta imprescindible que se haga de una manera segura y que permita ser ágiles, conectando Administraciones de distintos ámbitos para prestar más y mejores servicios al ciudadano.

Como se aprecia en el Gráfico 2, el uso de la administración electrónica es cada vez más relevante. Según el Informe REINA3, a nivel global un 55% de personas accedió a páginas de las Administraciones Públicas para obtener información, un 35% descargó formularios y un 22% envió formularios cum-

2 Datos del "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles (2º trimestre de 2010)", INTECO, 2010.
3 Fuente: Informe REINA 2009, Uso de la eAdministración. http://www.csae.map.es/csi/reina2009/index.html.

plimentados vía Internet a la administración. A medida que más servicios se ponen a disposición del ciudadano, es de esperar que estos porcentajes aumenten rápidamente, y con ello, las expectativas y exigencias en cuanto a la seguridad de la información.

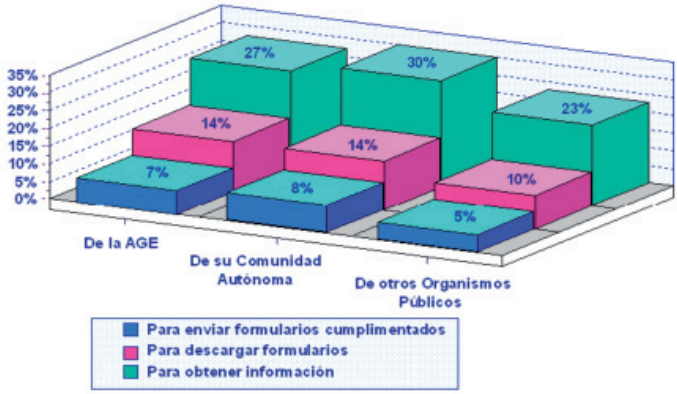

Gráfico 2 - Utilización de los servicios electrónicos.

5 ÁMBITO DE APLICACIÓN

5.1 A QUIÉN APLICA

El Esquema Nacional de Seguridad (ENS), es de obligado cumplimiento para el conjunto de la administración española, entendiendo por tal la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

Esto incluye, además de ministerios, consejerías autonómicas, corporaciones municipales, otras entidades tales como:

- Las Universidades, en cuanto organismos autónomos de la administración.
- Autoridades Portuarias y aeroportuarias.
- A las entidades públicas tipo Institutos de Desarrollo Económico, Servicios de Salud, etc.

La Administración de Justicia no está obligada por la Ley 11/2007, ni por lo tanto por el ENS. Sin embargo cuentan con un programa de actuación, denominado Esquema Judicial de Interoperabilidad y Seguridad (EJIS), suscrito por las Instituciones con responsabilidades en la Administración de Justicia (Ministerio de Justicia, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Comunidades Autónomas con competencias transferidas). El EJIS es un marco de colaboración para colegiar esfuerzos y cuyos objetivos fundamentales son la prestación de los servicios de Administración de Justicia bajo el paradigma de la interoperabilidad, accesibilidad, reusabilidad y seguridad.

No es obligatoria a aquellas administraciones que realicen sus actividades en régimen de derecho privado.

5.2 A QUÉ APLICA

Esta norma aplica a todos los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de medios electrónicos.

Están excluidos los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

Tampoco aplica a las administraciones en las actividades que desarrollen en régimen de derecho privado.

5.3 PLAZOS

Se daban doce meses de plazo tras la entrada en vigor del Esquema Nacional de Seguridad para aplicarlo en los servicios que se prestaban en ese momento.

Cuando no es posible hacerlo por cualquier circunstancia, hay que preparar un plan de adecuación, con las tareas a realizar para la completa aplicación de lo exigido por el ENS a lo largo de un plazo que no puede ser superior a 48 meses desde la entrada en vigor del mismo.

6 INTRODUCCIÓN AL ENS

6.1 PRINCIPIOS BÁSICOS

El objeto último de la seguridad de la información es asegurar que una organización podrá cumplir sus objetivos utilizando sistemas de información. Tal y como estipula el ENS, en las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- Seguridad integral.
- Gestión de riesgos.

- Prevención, reacción y recuperación.
- Líneas de defensa.
- Reevaluación periódica.
- Función diferenciada.

6.1.1 Seguridad integral

Para que sea efectiva, la gestión de la seguridad debe ser un proceso integral, es decir, que hay que considerar tanto los elementos técnicos, como los humanos, los materiales y los organizativos, relacionados con el sistema. En el Esquema Nacional de Seguridad no se admiten actuaciones puntuales.

Parte fundamental en la consecución de una gestión integral de la seguridad es la formación de todo el personal que tenga alguna responsabilidad en los servicios electrónicos que se prestan.

Es importante recordar que los sistemas son gestionados y operados por personas. Aunque se implantaran todas las medidas técnicas aplicables, sería imposible evitar un error humano o un ataque deliberado. La mejor manera de prevenir estos casos es mediante la concienciación y la formación.

6.1.2 Gestión de la seguridad basada en los riesgos

Un programa de seguridad tiene sentido en la medida en la que responde a las necesidades de reducción de riesgos de la entidad.

La herramienta básica para hacerlo es el análisis y gestión de riesgos. El análisis de riesgos detectará los problemas de seguridad y los categorizará mientras que con la gestión se reducirán los riesgos a un nivel aceptable mediante la selección e implantación de medidas de seguridad. Como las circunstancias y los sistemas cambian, el análisis de riesgos debe mantenerse actualizado en todo momento.

6.1.3 Prevención, reacción y recuperación

No todas las medidas de seguridad están enfocadas a los mismos objetivos.

Las medidas de prevención tales como por ejemplo las medidas de protección de los accesos físicos, tienen como fin evitar que se produzcan eventos o incidentes.

Las medidas de detección (implantar antivirus por ejemplo) sirven para identificar eventos potencialmente peligrosos. Deben existir medidas de reacción (eliminación de virus siguiendo con el ejemplo anterior) que atajen el evento, minimizando los daños que hayan podido ocurrir.

Las medidas de recuperación (entre las que se encuentra la realización de copias de seguridad) son las que permiten restablecer la información o los servicios que hayan podido resultar dañados por un incidente de seguridad.

La utilización de todos los tipos de medidas permitirá un enfoque integral de la seguridad tal y como exige el ENS, evitando incidencias y reduciendo el impacto de aquellas que finalmente ocurran.

Otro punto a considerar es la necesidad de conservar los da-

tos en soporte electrónico así como la de mantener disponibles los servicios que los utilizan durante todo el ciclo de vida útil de dichos datos. Esto habitualmente se hará mediante procedimientos orientados a preservar el patrimonio digital.

6.1.4 Líneas de defensa

El sistema debe contar con sucesivas capa de protección de manera que un incidente no sea capaz de desarrollar todo su potencial dañino en caso de que ocurra. Para ello es necesario que encuentre distintos obstáculos que reduzcan su impacto total en forma de líneas de defensa.

De esta manera, si ocurre un incidente, las capas de medidas de seguridad deben permitir:

- Ganar tiempo para reaccionar, conteniendo el incidente.
- Reducir la amplitud del impacto, evitando que se difunda a todo el sistema.
- Disminuir hasta donde sea posible el impacto total sobre el sistema.

Para que esto sea posible deben aplicarse un conjunto de medidas de carácter organizativo (como las políticas de uso aceptable), físicas (por ejemplo equipos antiincendios) y lógicas (tales como las segregación de redes).

6.1.5.Reevaluación periódica

Como se ha comentado anteriormente, la evaluación de riesgos debe estar actualizada para que cumpla eficazmente con

su función de detectar peligros potenciales para el sistema. En esa dinámica se enmarca asimismo la revisión de las medidas de seguridad, para verificar que siguen siendo las adecuadas a los riesgos detectados y que mantienen su eficacia protegiendo el sistema contra ellos. Esta revisión puede llevar a la conclusión de que hay que añadir más controles, mejorar los existentes o incluso reorganizar por completo el conjunto de controles aplicados.

6.1.6 Función diferenciada

En cualquier marco de trabajo de seguridad es crucial mantener una sana separación de responsabilidades que evite conflictos de interés que puedan ir en detrimento de la seguridad.

El ENS estipula que el las funciones de responsable de la información, responsable del servicio y responsable de la seguridad deben estar separadas.

El responsable de la información es quien conoce el uso que se le debe dar a dicha información por lo que es la persona más apropiada para definir los requisitos de seguridad de la información tratada.

El responsable del servicio es quien conoce la problemática de dicho servicio y las condiciones en la que se puede y debe prestar, por lo que es el indicado para determinar los requisitos de seguridad de los servicios prestados.

Por último, el responsable de seguridad es quien está al tanto de la visión general de los sistemas, datos y riesgos a los que están expuestos, por lo que es la personal que puede tomar con más conocimiento de causa las decisiones para

satisfacer los requisitos de seguridad de la información y de los servicios.

De esta manera se asegura que los distintos requisitos son adecuadamente consensuados, optimizando los resultados.

Los roles y responsabilidades deben estar claramente definidos y documentados en la política de seguridad, así como los mecanismos para la resolución de conflictos.

6.2 REQUISITOS MÍNIMOS DE SEGURIDAD.

Todos los organismos que estén sujetos al cumplimiento del ENS deben contar con una política de seguridad formal, aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.

- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.
-

6.2.1 Organización e implantación del proceso de seguridad

El proceso de seguridad, aunque tenga personas responsables de ciertos aspectos formales o de gestión, es competencia de todo el personal de una entidad. No es posible hacer un esfuerzo integral como demanda el ENS sin involucrar a todo el mundo, ya que cada uno es responsable de la seguridad en las tareas que realiza.

La política de seguridad recogerá los responsables de definir y hacer cumplir la política, así como las líneas a seguir en la entidad, por lo debe ser difundida a toda la organización y conocida por todos.

6.2.2 Análisis y gestión de los riesgos.

Cada organización debe realizar su propio análisis y gestión de riesgos para sus sistemas de información.

El ENS no prescribe ninguna metodología de análisis de riesgos, estableciendo únicamente que debe utilizarse una que esté internacionalmente reconocida. A efectos prácticos esto significa que cualquier metodología que reconozca el European Network and Information Security Agency (ENISA) en su Inventario de Metodologías[4] sería válida en este contexto.

Dado que Magerit se encuentra en este Inventario así como la herramienta asociada Pilar en el Inventario de Herramientas, y la alta difusión de esa metodología en el ámbito de las Administraciones Públicas, es la candidata más apropiada para ser utilizada en la implantación del ENS.

En la gestión de riesgos es importante escoger y aplicar medidas de seguridad proporcionales al riesgo detectado. Es decir, el coste y esfuerzo de las medidas puede ser tan alto como el riesgo que se pretende mitigar, pero no debería ser mayor.

6.2.3 Gestión de personal.

Como se ha comentado anteriormente, un factor crítico de éxito para los esfuerzos en seguridad es la participación del personal.

Todos deben ser concienciados, formados, e informados de sus deberes y obligaciones en materia de seguridad.

---

4 http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-methods

Esto permitirá tomar acciones encaminadas a corregir comportamientos poco adecuados, e incluso exigir responsabilidades a aquellas personas que no cumplan con lo establecido. Para esto es necesario también que los usuarios estén identificados de manera única en el sistema para poder seguir sus acciones.

Tras la formación deben realizarse acciones que verifiquen si se siguen las normas de seguridad establecidas de manera sistemática.

6.2.4 Profesionalidad

El personal que esté dedicado a las tareas de seguridad debe estar cualificado de manera apropiada, dada la sensibilidad y complejidad de algunas de esas tareas. Esto es aplicable a todas las fases del ciclo de vida del proceso de seguridad: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Para ello el personal de las Administraciones Públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios sujetos al ENS.

Lógicamente los mismos requisitos que se exigen internamente deben ser exigidos a cualquier proveedor que preste algún servicio relacionado con seguridad. Los proveedores deberán contar con un nivel de seguridad similar al requerido por la entidad.

6.2.5 Autorización y control de los accesos

El primer paso para asegurar que la información y los sistemas están protegidos es limitar el acceso a los mismos. Debe definirse quienes y en qué medida tendrán acceso a los recursos, de manera que cada uno tenga el acceso necesario para realizar sus tareas, pero no a equipos o datos que no deben estar a su alcance. Además de debe contar con mecanismos de autorización para permitir el acceso y denegarlo y revocarlo cuando sea necesario.

6.2.6 Protección de las instalaciones

Las instalaciones deben protegerse contra daños que puedan afectar a los sistemas que albergan y contra accesos de personas no autorizadas.

En caso de instalaciones en las que se ubiquen sistemas el control de acceso deberá ser como mínimo mediante salas cerradas y con control de llaves.

6.2.7 Adquisición de productos

Los productos de seguridad que se adquieran deberán ser idealmente certificados en seguridad según alguna norma o estándar reconocido internacionalmente. En este contexto, lo habitual será la certificación en Common Criteria.

En cualquier caso, la compra de cualquier producto o servicio relacionado con la administración electrónica debe hacerse tras un completo análisis de los requisitos no solo funcionales sino también de seguridad que debe cumplir.

6.2.8 Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. Para conseguirlo, las pautas a seguir son:

- No proporcionar más funcionalidad que la requerida por las necesidades y objetivos de la entidad.
- En línea con lo anterior, deben eliminarse las funciones que no sean necesarias para el correcto funcionamiento del sistema o para la consecución de los objetivos.
- Los privilegios de operadores, administradores y usuarios deberán ser los mínimos necesarios para que cumpla con sus obligaciones.
- Los accesos deben estar restringidos al personal autorizado, los horarios establecidos y los puntos de accesos aprobados.
- El sistema ha de ser sencillo y seguro de utilizar, de forma que para que ocurra un incidente de seguridad sea necesario que el usuario lo haga de manera consciente.

6.2.9 Integridad y actualización del sistema

Para garantizar la integridad del sistema en todo momento, cualquier cambio tanto físico como lógico debe ser realizado solamente tras su aprobación formal y mediante un procedimiento formal.

Se deben llevar a cabo las actualizaciones de los sistemas de una manera controlada y en función del estado de seguridad requerido en cada momento. Los cambios en las especifica-

ciones de los fabricantes, la aparición de nuevas vulnerabilidades, la emisión de actualizaciones y parches que afecten a los sistemas deben ser analizados para tomar las medidas necesarias para que no se degraden los sistemas ni su nivel de seguridad, gestionando asimismo los riesgos que introducen los cambios que se realizarán.

6.2.10 Protección de la información almacenada y en tránsito

Una parte significativa del ciclo de vida de la información corresponde a su almacenamiento y a su transporte.

La información debe estar protegida en todo momento, por lo que es crítico tener en cuenta los riesgos que conllevan esas fases, especialmente con el uso de medios como ordenadores portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. Estos dispositivos y medios presentan más riesgo de pérdidas o robos que los tradicionales, por lo que se debe tener más cuidado en su uso y manipulación.

Otro aspecto importante es que la información esté correctamente almacenada y conservada, de manera que pueda ser recuperada cuando sea necesario. Para ello es necesario desarrollar procedimientos adecuados, que cubran tanto a la información en soporte electrónico como en papel, si es el origen o la consecuencia directa de la información electrónica a la que se refiere el ENS.

6.2.11 Prevención ante otros sistemas de información interconectados

Actualmente es más habitual encontrarse con sistemas conectados con otros sistemas mediante redes privadas o públicas que sistemas independientes. Conectarse con otros sistemas, en particular a redes públicas de comunicaciones (por ejemplo Internet), conlleva unos riesgos que deben ser evaluados y mitigados antes de llevar adelante la conexión.

6.2.12 Registro de actividad

Registrar las actividades de los usuarios, recogiendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permite identificar a la persona que las ha realizado y tomar medidas al respecto según la gravedad de los hechos

Esto debe realizarse únicamente en la medida que sea necesario para cumplir con los requisitos del ENS y sin incurrir en incumplimientos de la Ley de Protección de Datos de Carácter Personal o en otras leyes y regulaciones relacionadas.

6.2.13 Incidentes de seguridad

El ENS establece que se debe instalar un sistema de detección y reacción frente a código dañino (virus, gusanos, troyanos, etc.).

Gestionar los incidentes de seguridad tiene como objetivo asegurarse de que los eventos y los puntos débiles de la seguridad de la información asociados con los sistemas de información se comunican de forma que sea posible emprender acciones correctivas, se registran, se escalan y se resuel-

ven de la manera más eficaz posible.

Documentando los incidentes y las acciones tomadas para su resolución es posible evaluarlos para identificar incidentes recurrentes o de relevancia. Con esta información se puede estudiar mejorar o añadir controles, en definitiva, se puede mejorar el sistema.

6.2.14 Continuidad de la actividad

Reaccionar a la interrupción de las actividades y proteger los sistemas de información de los efectos de desastres o de fallos importantes, así como garantizar su oportuna reanudación es el objetivo de implantar medidas como las copias de seguridad y mecanismos para asegurar la continuidad como los planes de continuidad.

Estos planes aseguran que la disponibilidad de la información y los servicios se mantienen en un nivel y en un plazo temporal establecidos incluso después de una interrupción o un fallo de los procesos críticos de negocio.

6.2.15 Mejora continua del proceso de seguridad

La mejora continua es uno de los requisitos del ENS, que requiere que el proceso integral de seguridad implantado se actualice y mejore de manera continua, dejando a criterio de los implantadores los métodos para realizarlo, ya que no especifica un método determinado para realizarlo, simplemente que sea un método reconocido internacionalmente.

6.2.16 Cumplimiento de requisitos mínimos

Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, se aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta los siguientes criterios:

- Los activos que constituyen el sistema y su valoración.
- La categoría del sistema.
- Las decisiones que se adopten para gestionar los riesgos identificados.
- Los requisitos que apliquen en cuestión de materia de protección de datos de carácter personal.

Se pueden ampliar estos mínimos a criterio del responsable de seguridad teniendo en cuenta:

- El estado de la tecnología.
- La naturaleza de los servicios prestados y la información manejada.
- El resultado del análisis de riesgos.

6.2.17 Infraestructuras y servicios comunes

Para facilitar el cumplimiento de lo requerido por el ENS, se utilizarán las infraestructuras y servicios comunes reconocidos en las Administraciones Públicas en la medida de lo posible y de acuerdo con las necesidades de cada entidad.

Estos servicios comunes, desarrollados para cualquier admi-

nistración, se agrupan en las siguientes materias:

- Interconexión entre Administraciones (por ejemplo la red SARA)
- Firma Electrónica (por ejemplo @firma, la plataforma de validación de certificados y firmas del Ministerio de la Presidencia).
- Tramitación electrónica.
- Normativa, Regulación y Recomendaciones.
- Servicios integrales.
- Información y difusión.
- Herramientas de apoyo.
- Gestión de Recursos Humanos en la Administración General del Estado.

6.2.18 Guías de seguridad

El Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones para facilitar la implantación del ENS.

El listado completo de estas guías forma parte de la bibliografía de esta Guía (ver sección 10).

6.2.19 Sistemas de información no afectados

Como el alcance del ENS es la administración electrónica, se dará el caso de que habrá sistemas de información a los que no les sea de aplicación el ENS por ser sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.

Cada entidad deberá determinar cuales son estos sistemas.

6.3 COMUNICACIONES ELECTRÓNICAS

6.3.1 Condiciones técnicas de seguridad de las comunicaciones electrónicas.

Las comunicaciones electrónicas son un punto sensible en cuanto a seguridad por su vulnerabilidad a ataques de diversa índole.

El ENS determina que deben controlarse las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, según lo establecido en la Ley 11/2007, de 22 de junio.

Las medidas de seguridad adoptadas serán implementadas de acuerdo con lo establecido en el ENS.

Debe tenerse en cuenta que las comunicaciones tendrán el

valor y la eficacia jurídica que corresponda a su naturaleza, según la legislación aplicable.

6.3.2 Requerimientos técnicos de notificaciones y publicaciones electrónicas

Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos por su impacto en los ciudadanos deben protegerse cuidadosamente. El ENS exige que:

- Se asegure la autenticidad del organismo que lo publique.
- Se asegure la integridad de la información publicada.
- Quede constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.
- Se asegure la autenticidad del destinatario de la publicación o notificación.

6.3.3.Firma electrónica

La firma electrónica es una medida de seguridad muy valiosa para proteger la autenticidad de quien emite una comunicación electrónica.

El uso de la firma electrónica debe documentarse en una política de firma electrónica, así como debe existir una política de certificados, que regulen los procesos de generación, validación y conservación de firmas electrónicas, así como las

características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas.

La firma electrónica se aplicará según lo estipulado en el Anexo II del ENS y el Esquema Nacional de Interoperabilidad.

6.4 AUDITORÍA DE LA SEGURIDAD

El ENS requiere que se lleve a cabo una auditoría cada dos años como mínimo o antes si hay cambios importantes en el sistema de información, que puedan afectar a las medidas de seguridad requeridas.

La auditoría se llevará a cabo siguiendo las pautas de las guías CCN-STIC-802 Guía de Auditoría y CCN-STIC-808 Verificación del Cumplimiento de las Medidas.

Los informes de auditoría detectarán las deficiencias y desviaciones del sistema de seguridad respecto a lo establecido en el ENS y deberán ser analizados para tomar acciones que corrijan esta situación.

6.5 ESTADO DE SEGURIDAD DE LOS SISTEMAS

Regularmente el Comité Sectorial de administración electrónica elaborará un informe en el que se recogerán las principales variables de la seguridad en los sistemas de información a los que se refiere el ENS, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

6.6 RESPUESTA A INCIDENTES DE SEGURIDAD

6.6.1 Capacidad de respuesta

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team). Se denomina CERT a un grupo de trabajo responsable de desarrollar medidas de prevención y de reacción antes incidentes de seguridad en los sistemas de información. Este grupo actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

6.6.2 Prestación de servicios de respuesta a incidentes de seguridad

El CCN-CERT mencionado en el punto anterior prestará a las Administraciones Públicas los siguientes servicios:

- Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad.

- Investigación y divulgación de las mejores prácticas sobre seguridad de la información. En este contexto se han desarrollado las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional y que se pueden consultar en su sitio web[5].

5 *www.ccn-cert.cni.es*

- Formación destinada al personal de la administración especialista en el campo de la seguridad de las tecnologías de la información.

- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas.

El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones Públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal.

6.7 NORMAS DE CONFORMIDAD

6.7.1 Sedes y registros electrónicos

Las sedes y registros electrónicos son el primer punto de contacto del ciudadano con la administración electrónica. De ahí que sea fundamental garantizar su seguridad y la del acceso electrónico de los ciudadanos a las mismas. Son servicios críticos que se protegerán de acuerdo con los requisitos del ENS.

6.7.2 Ciclo de vida de servicios y sistemas

Para que la seguridad sea verdaderamente integral debe estar presente en todo el ciclo de vida de servicios y sistemas, por lo que las especificaciones de seguridad deben incluirse con el resto de especificaciones funcionales, organizativas, etc. cuando se decida planificar un nuevo servicio o sistema.

6.7.3 Mecanismos de control

Sin un mecanismo de control que monitorice y verifique el correcto seguimiento de las directrices de seguridad no es

posible tener un sistema de seguridad que funcione correctamente. Deben establecerse puntos y elementos de control para realizar esta tarea.

6.7.4 Publicación de conformidad

Las entidades sujetas al ENS deben hacer públicas en las correspondientes sedes electrónicas las declaraciones de conformidad con el ENS, y cualquier otro distintivo de seguridad que posean.

6.8 ACTUALIZACIÓN

6.8.1 Actualización permanente

Ya se ha mencionado en otras secciones y se vuelve a insistir aquí en la importancia de mantener actualizado el sistema de seguridad, mejorándolo con el tiempo para responder a los cambios en los servicios de administración electrónica, la evolución tecnológica y nuevos estándares internacionales sobre seguridad y auditoría en los sistemas y tecnologías de la información.

6.8.2 Categorías

Los sistemas se adscribirán a una categoría, en función de la gravedad del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios siguiendo el procedimiento establecido en el Anexo I.

Esta categoría es la que da la medida de hasta qué punto hay que dedicar esfuerzos en seguridad a proteger ese sistema de los riesgos a los que está expuesto.

Las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se valora en función de su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cum-

plimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

6.8.3 Facultades

El responsable de cada información o servicio es quien debe realizar las valoraciones mencionadas en el punto anterior y mantenerlas actualizadas.

El responsable del sistema es quien debe asignar la categoría al mismo.

7 EL PLAN DE ADECUACIÓN

El ENS especifica que si no es posible en plazo y forma la adecuación al mismo, la entidad deberá contar con un plan de adecuación. Los detalles de cómo desarrollarlo se recogen en la GUÍA DE SEGURIDAD (CCN-STIC-806) ESQUEMA NACIONAL DE SEGURIDAD - PLAN DE ADECUACIÓN.

Este plan de adecuación contendrá la siguiente información:

1. La política de seguridad.
2. Información que se maneja, con su valoración.
3. Servicios que se prestan, con su valoración.
4. Datos de carácter personal.
5. Categoría del sistema.
6. Declaración de aplicabilidad de las medidas del Anexo II del ENS.
7. Análisis de riesgos.
8. Insuficiencias del sistema.
9. Plan de mejora seguridad, incluyendo plazos estimados de ejecución.

El Plan de Adecuación lo desarrollará el Responsable de Seguridad cuando lo haya o la persona a la que se asigne esta función de forma temporal.

7.1 LA POLÍTICA DE SEGURIDAD

Idealmente, el organismo dispondrá de una política de seguridad conforme a lo que se pide en el Anexo II del ENS, por lo que sólo será necesario identificarla y anexarla al plan de adecuación. Pero si no es así, el plan tendrá que recoger la planificación de la modificación de la política de seguridad existente o el desarrollo de una nueva que cumpla con todos los requisitos.

7.2 VALORACIÓN DE LA INFORMACIÓN QUE SE MANEJA

Hay que detallar la información que se maneja y valorarla según se establece en el ENS y se describe en la sección 7.1.2 .

En una entidad en la que no haya una política de seguridad clara y definida puede resultar problemático llevar a cabo tanto el inventario de toda la información utilizada en la prestación de los servicios como posteriormente valorarla, ya que no habrá criterios definidos para hacerlo y faltarán algunos propietarios. Si fuera así, el Responsable de Seguridad o la persona designada para llevar a cabo sus funciones tendrá que realizar esta valoración según su leal saber y entender, dejando constancia de los motivos y razonamientos para determinar las valoraciones documentadas.

Esta valoración es meramente provisional para los efectos del plan y deberá realizarse una valoración formal en un plazo adecuado, documentándose estas tareas en el plan.

7.3 VALORACIÓN DE LOS SERVICIOS QUE SE PRESTAN

De manera análoga a lo indicado en la sección anterior para la información, debe realizarse la valoración de los servicios.

Para ello debe enumerarse los servicios que se prestan y valorarlos como de detalla en la sección 7.1.2.

Cuando no hay política de seguridad por la que regirse para hacer esta valoración, faltan responsables de los servicios o la valoración de la información no está aprobada formalmente, se realizará una valoración provisional, especificando su plazo de validez, pasado el cual deberá haberse realizado una valoración formal.

7.4 DATOS DE CARÁCTER PERSONAL

Cuando el sistema maneja datos de carácter personal, deberá incluirse la relación detallada de dichos datos en el plan de adecuación. Para ello es suficiente hacer referencia al Documento de Seguridad requerido por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal existente en la entidad.

7.5 CATEGORÍA DEL SISTEMA

Con las valoraciones disponibles de la información y los servicios, el Responsable de Seguridad establecer la categoría del sistema, siguiendo los criterios y pasos recogidos en el Anexo I del ENS.

Una estrategia eficaz para reducir la utilización de recursos

es segregar los sistemas en sub-sistemas, si es posible. De esta manera se aplicarán las medidas de seguridad exigidas para niveles altos específicamente a aquellos segmentos del sistema que lo requieran y no al sistema completo, que requeriría mucho más esfuerzo.

7.6 DECLARACIÓN DE APLICABILIDAD

El Responsable de Seguridad, a la vista del nivel del sistema y de los requisitos planteados para la protección de los datos de carácter personal, documentará la lista de las medidas aplicables al sistema, como se describe en la sección 7.2.2.

7.7 ANÁLISIS DE RIESGOS

Otro de los puntos a incluir en el Plan de Adecuación es un análisis de riesgos, según lo descrito en el Anexo II del ENS para la categoría establecida para el sistema.

En este análisis de riesgos se valorarán las salvaguardas presentes en la fecha de aprobación del plan de adecuación, de manera que se cuente con un mapa de riesgos actuales.

7.8 INSUFICIENCIAS DEL SISTEMA

Hay que identificar y documentar las carencias en el actual sistema de gestión de seguridad de la información, que pueden detectarse en varios aspectos:

- Desviaciones de lo exigido en el Anexo II para valorar el sistema y seleccionar medidas de seguridad.

- Incumplimientos de los requisitos exigidos por el RD 1720/2007 para los datos de carácter personal tratados por el sistema.

- Existencia de riesgos que no son aceptables por el organismo.

Los riesgos residuales (los que quedan tras la aplicación de las medidas de seguridad seleccionadas) deben ser aceptados por los responsables de la información y servicios afectados. Puede darse el caso de que no todos los responsables estén designados o que la aceptación del riesgo no sea formal, el Responsable de Seguridad tomará la decisión a su mejor criterio, indicando por qué y cómo ha llegado a esas decisiones de aceptación o no del riesgo residual.

7.9 PLAN DE MEJORA DE LA SEGURIDAD

Partiendo de la información recopilada, y teniendo en cuenta las carencias detectadas se elaborará un plan de mejora de la seguridad que detallará las acciones que se van a tomar para subsanarlas.

Además para cada una de las acciones que se tomarán se documentará:

- Las insuficiencias que subsana.

- El plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación.

- Los principales hitos del proyecto.

- Una estimación del coste que supondrá.

7.10 INTERCONEXIÓN DE SISTEMAS

Cuando se da el caso de que un sistema maneja información de terceros o presta servicios a terceros, es necesario que la valoración de la información y los servicios sea aportada por dicho tercero.

Si por el motivo que sea no es posible que el tercero suministre esta valoración, el Responsable de Seguridad establecerá unos valores en base a su experiencia y conocimiento, y los documentará como "compromiso de prestación de servicios". Si más adelante los responsables de este sistema modifican las exigencias en materia de seguridad, se recurrirá a la realización de un "Plan de adecuación incremental" que recoja las acciones necesarias para cumplir con los nuevos requisitos.

Cuando el caso es el de un sistema que utiliza sistemas de terceros para manejar información o para prestar servicios, la valoración se realizará internamente y se le exigirá al tercero que colabora que la incorpore a su plan de seguridad. Si el prestatario está sujeto al cumplimiento del Esquema Nacional de Seguridad, incorporará estos requisitos a su propio plan de adecuación o a su propia declaración de conformidad.

IMPLANTACIÓN DEL ENS 8

Para llevar a cabo de manera eficiente y eficaz el diseño, desarrollo e implantación del Esquema Nacional de Seguridad, se desarrollaran las siguientes actividades:

- Definir una política de seguridad.
- Definir el conjunto de recursos técnicos, organizativos, humanos y procedimentales sujetos al ENS.
- Catalogación de los tipos de información según su criticidad (estructura de tipos y niveles).
- Definir y asignar responsables de velar por el cumplimiento de la política de seguridad de la organización.

- Realizar el análisis y gestión de los riesgos del sistema y mantenerlo actualizado.

- Seleccionar las medidas de protección en función de los tipos y niveles de la información.

- Definir la Normativa de Seguridad. Documentos que detallen como y quien hace las distintas tareas y como se identifican y resuelven los comportamientos anómalos. Entre ellos estarán:

    - Definición de los sistemas de registro, control y resolución de incidencias.

    - Definición y desarrollo de un plan de continuidad de servicio.

    - Definición y desarrollo de un plan de pruebas y monitorización del sistema.

    - Definición de las medidas de protección adecuadas para los riesgos detectados.

- Definir y describir los Procesos de Autorización, formalizando autorizaciones que cubran todos los elementos de los sistemas de información: Instalaciones, equipos, aplicaciones, medios de comunicación, accesos, soportes, etc.

- Formar a todos los funcionarios sobre la política, normativa y procedimientos de seguridad.

- Evaluar la eficacia de las medidas adoptadas.

- Mantener el sistema actualizado.

- Realización de una Auditoría bienal de Seguridad que revise la política de seguridad y el sistema de seguridad establecidos.

8.1 PLANIFICACIÓN

Se asume que en la implantación del ENS se va a utilizar la metodología de análisis de riesgos MAGERIT y la herramienta basada en ella, Pilar, aunque el ENS no es preceptivo al respecto, especificando únicamente que debe ser utilizada una metodología de Análisis de Riesgos reconocida internacionalmente.

En la práctica esto significa que se puede utilizar para los fines del ENS cualquiera de las recogidas por ENISA en su catálogo6. Sin embargo debido a la amplia difusión de la metodología MAGERIT en el ámbito de las AAPP y a su libre disposición por parte de las mismas, hace de esta metodología y su herramienta la opción más eficaz y económica para el propósito de este tipo de proyectos.

8.1.1 Política

La política de seguridad tiene que ser formal y aprobada por el titular del órgano superior correspondiente, es decir los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico. En el caso de los municipios, se prevé que podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter

6 Inventory of Risk Management / Risk Assessment Methods, ENISA, http://rm-inv.enisa.europa.eu/rm_ra_methods.html

representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan.

Para poder desarrollarla en primer lugar debe designarse a los integrantes que van a conformar el Comité de Seguridad. Así mismo se asignaran el/los responsable(s) de seguridad encargados de velar por el cumplimiento de las futuras medidas de seguridad a implantar en la Entidad. Tras esto se recoge información sobre los recursos técnicos de la entidad, la infraestructura existente, los controles de seguridad existentes, las Normas de Seguridad implantadas, las responsabilidades asignadas, etc. Con esta información se definirá la política de seguridad, que debe ser revisada por el Comité, aprobada por el órgano superior de la entidad y publicada. Puede hacerse dentro de la Intranet ó por correo electrónico o se lo brinda en formato papel la política de seguridad a todos los funcionarios de la entidad.

La política debe cubrir los requisitos mínimos establecidos por el ENS:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.

- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Sin embargo debe tenerse en cuenta que el nivel de cumplimiento de estos requisitos depende de los riesgos de los sistemas a los que apliquen. Por ello podría darse el caso de que una política aplicable a un sistema con un riesgo o una criticidad muy baja, no cuente con todos los puntos anteriores o solo de una manera muy genérica.

8.1.2 Categorización de los sistemas de información

Para realizar la categorización de los sistemas se debe partir de un inventario de los servicios de administración electrónica que se prestan a los ciudadanos y de la información que se maneja para la prestación de dichos servicios.

El conjunto formado por servicio/s + información es lo que en el ENS se considera un sistema. Una entidad puede contar con uno o varios sistemas, dependiendo de su tamaño, del número de servicios o de la criticidad de los mismos.

Una vez definidos los servicios y la información se deben valorar en función de la importancia que cada uno de los criterios de valoración, según se ha definido en la guía CCN-STIC-803, ESQUEMA NACIONAL DE SEGURIDAD, VALORACIÓN DE LOS SISTEMAS. Estos criterios son:

D: Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo no estuviera disponible cuando se necesita?.

I: Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo fuera alterado por alguien sin autorización?.

C: Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. La pregunta a responder para valorar un activo en este criterio será: ¿Qué importancia tendría que al activo fuera revelado a personas no autorizadas?.

T: Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. La valoración de este criterio responde a la pregunta de ¿qué importancia tendría no poder identificar a quien haya ejecutado una acción?.

A: Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. La pregunta aquí sería,

¿qué importancia tendría que el remitente o el destinatario de un activo no fuera el que dice ser?.

Para valorar los activos en cada uno de estos criterios se utiliza una escala de tres puntos; bajo, medio y alto, según lo establecido en la mencionada guía.

Como establece el ENS, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio. Consecuentemente, la categoría del Sistema viene dada por el valor máximo de los parámetros.

8.1.3 Análisis de Riesgos

Para realizar un análisis de Riesgos se debe partir de un inventario de los activos involucrados en la prestación de los servicios de administración electrónica. Habitualmente se consideran los siguientes tipos de activos:

- Hardware, equipos necesarios para la prestación de los servicios identificados.
- Software, aplicaciones utilizadas en la prestación de los servicios identificados.
- Personal, personal involucrado en la prestación de los servicios identificados.
- Instalaciones, ubicaciones, edificios u oficinas utilizadas durante la prestación de los servicios identificados.

Estos activos reciben la valoración de los servicios e información que dependen de ellos.

Tras la valoración, deben considerarse:

- las amenazas que pueden afectar a esos activos.
- la frecuencia de ocurrencia de esas amenazas.

Con estos datos, se obtendrá un informe de las diferentes amenazas, vulnerabilidades e impactos que podrían producirse en los sistemas de información de la entidad. Es decir, se consigue una valoración del riesgo inicial, es decir del riesgo latente de los activos si no estuvieran protegidos.

La siguiente tarea del análisis de riesgos será la valoración de la madurez de las medidas de seguridad que se hayan implantadas actualmente para proteger los activos. Hay cinco niveles:

Nivel	Significado	Descripción
n.a.	No es aplicable	
L0	Inexistente	En el nivel L0 de madurez no hay nada.
L1	Inicial / ad hoc	Las medidas de seguridad existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las entidades exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de la alta calidad.
L2	Reproducible, pero intuitivo	La eficacia de las medidas de seguridad depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción a los hechos. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.

Nivel	Significado	Descripción
L3	Proceso definido	Se despliegan y se gestionan las medidas de seguridad. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es consecuencia del trabajo consciente y riguroso.
L4	Gestionado y medible	Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las medidas de seguridad. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5	Optimizado	El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

Habrá que realizar un análisis diferencial con el fin de determinar qué controles, de los existentes en el ENS ya se en encuentran implantados en la entidad. Con los controles ya implantados y aquellos que el ENS prescribe para el nivel del sistema que se está analizando, se obtiene el valor de riesgos actual. Este mapa de riesgos identifica los activos que requieren de algún tipo de actuación para delimitar sustancialmente el riesgo, pudiendo ser necesario aplicar algún control más para minimizar el riesgo de los activos cruciales para cumplir con el nivel de seguridad deseado. Hay que tener en cuenta que cuanto mayor sea la madurez de la medida implantada, mayor será su eficacia en la reducción del riesgo.

8.1.4 Metodologías. Magerit

La metodología Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del "Ministerio de Administraciones Públicas", cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada.

En primer lugar, el análisis de riesgos permite conocer el sistema: sus activos, su valor, y las amenazas a las que está expuesto. Tras este análisis, el tratamiento de riesgos se centra en seleccionar medidas de seguridad para conjurar las amenazas. Por último, la gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

Para el Análisis de riesgos se identifican los Activos de la entidad. Estos activos están expuestos a una serie de Amenazas que, cuando ocurren, degradan el valor del activo, causando un cierto Impacto.

La metodología propone una serie de Amenazas que afectan directa o indirectamente al Activo según su tipo. Si estimamos la probabilidad de la amenaza, podemos concluir el

Riesgo en el sistema, o la pérdida a la cual está expuesto.

La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza.

Para la gestión de riesgos se seleccionan las salvaguardas para hacer frente a las amenazas, así como el nivel al que están aplicadas o el nivel objetivo que se pretende alcanzar.

Las salvaguardas mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores residuales, que deberán ser asumidos por la Entidad o mitigados de nuevo hasta un nivel aceptable.

8.2 IMPLANTACIÓN

8.2.1 Selección de medidas de seguridad

La selección de las medidas de seguridad debe realizarse con las pautas marcadas en el ENS.

Una vez que se ha determinado la categoría de un sistema, se deben seleccionar aquellas medidas que según el Anexo I corresponden a ese nivel de sistema. Es decir, para un sistema de nivel bajo se seleccionarán las medidas identificadas en el Anexo I para este nivel. Para el nivel medio, las identificadas expresamente para este nivel así como las del nivel anterior.

Para un sistema de nivel alto, aplicarán todas las medidas de seguridad recogidas en el Anexo I, y con el grado de exigencia especificado para el mismo.

Los sistemas de nivel Alto deberán cumplir con todas las medidas de seguridad.

Las medidas de seguridad que estipula el ENS son:

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
				ORG	MARCO ORGANIZATIVO
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				OP	MARCO OPERACIONAL
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento /Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
I C A T	aplica	=	=	op.acc.4	Gestión de derecho de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				MP	MEDIDAS DE PROTECCIÓN
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos

Dim. afectadas	Bajo	Medio	Alto	Tipo de medida	Medida de seguridad
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (back Up)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

Además, deben escogerse controles que mitiguen los riesgos detectados en el análisis de riesgos, de manera que no queden huecos de seguridad que impidan cumplir con el requisito de contar con un sistema de gestión de seguridad integral.

8.2.2 Declaración de Aplicabilidad

El conjunto de medidas seleccionadas debe documentarse en una Declaración de Aplicabilidad, firmada por el responsable de la seguridad del sistema.

En caso de que haya particularidades en la aplicación de alguna medida concreta, se darán las explicaciones necesarias para clarificarlo. Estas diferencias pueden venir dadas por características particulares del sistema o bien por requerimientos del tratamiento de datos de carácter personal.

Si una medida requerida por el nivel del sistema no se considera aplicable, debe justificarse por qué no se aplica.

Si se da el caso de que se utilicen otras medidas distintas de las propuestas por el ENS, de debe justificar asimismo por qué se ha decidido utilizarlas y a qué medidas sustituyen.

8.2.3 Desarrollo de normativa

Una vez que se ha decidido qué se va a hacer en materia de seguridad, es necesario determinar cómo se va a llevar a cabo.

Para ello se deben elaborar, por un lado, una normativa de seguridad para detallar cuales son los usos correctos e incorrectos de los equipos, servicios e instalaciones, así como las responsabilidades del personal con respecto al cumplimiento o violación de estas normas, y por otro lado, los procedimientos que indique cómo llevar a cabo las tareas, las responsabilidades en la ejecución de estas tareas y el control de dicha ejecución.

La normativa de seguridad servirá para implantar y mantener las medidas de seguridad escogidas por la entidad. Según se vayan desarrollando procedimientos, se deben poner en funcionamiento y controlar la efectividad de la implantación así como la idoneidad de lo descrito en los procedimientos.

8.2.4 Declaración de Conformidad

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad. Entre estos distintivos se incluirán certificaciones de accesibilidad, interoperabilidad, menciones de calidad de cualquiera de las Administraciones Públicas (estatal, autonómica y local), de organizaciones internacionales o de organismos privados.

Los órganos y entidades de derecho público darán publicidad a la conformidad de sus sistemas respecto al cumplimiento del Esquema Nacional de Seguridad, de acuerdo con lo dispuesto en el Capítulo VIII del Real Decreto 3/2010, de 8 de enero, mediante declaraciones escritas, publicadas en las correspondientes sedes electrónicas y situadas en lugar de fácil acceso para los usuarios.

En el primer cuerpo se identificará el declarante. El órgano o entidad de derecho público titular del sistema, que se declara conforme, se identificará de forma inequívoca en la declaración escrita, señalando grupos operativos, departamentos o administración a la que pertenece, o los datos que fuesen necesarios para proporcionar la identificación indubitada del organismo público a que se refiere, mediante la denominación con la que aparece en la norma que aprueba la estructura orgánica a la que está adscrito.

En el segundo se indicará el contenido de la declaración. El contenido de la declaración de conformidad ha de describir de forma inequívoca el objeto de la misma, identificar de forma fidedigna el sistema o sistemas, y servicios a los que se refiere, e indicar que ha superado el plan de adecuación para lograrlo, en su caso.

Si no se cumple con el ENS, debe declararse el plan de adecuación, que se identificará de acuerdo con lo establecido en la Guía CCN-STIC 806.

En el tercero, se señalará en base a qué se declara la conformidad y con qué finalidad.

Ha de ir firmada por el titular del organismo emisor de la declaración de conformidad, que ha de ser identificado con su nombre completo y cargo que ostenta.

8.2.5 Formación

La formación es un punto en el que se insiste bastante a lo largo del ENS. Es fundamental contar con personal concienciado y formado a todos los niveles para el éxito de un programa de seguridad de la información. Por ello se recomienda poner en marcha jornadas informativas para todo el personal de la entidad al objeto de transmitirles las nuevas formas de trabajo así como para explicarles el porqué y el cómo de la adopción del ENS.

Estas jornadas deberían personalizarse para las distintas necesidades que presentará cada uno de los grupos de trabajo y planificarse adecuadamente.

Es recomendable realizar evaluaciones de la formación impartida, para verificar que han sido comprendidos y asumidos los conceptos y métodos expuestos.

8.3 VERIFICACIÓN Y VALIDACIÓN

Las medidas de seguridad implantadas deben contar con algún método de control que garantice que son apropiados y suficientes en todo momento, y no se degrade su eficacia con el tiempo o queden obsoletas.

Métodos de control apropiados pueden ser:

- Autoevaluaciones llevadas a cabo por el Responsable de Seguridad, en las que se chequeen:
    - La validez y vigencia de la Política y la Normativa de Seguridad.
    - La vigencia de la categorización de los sistemas y el

análisis de riesgos.

- La validez y vigencia de los controles aplicados.

- La eficacia de los controles.
  Los resultados de estos chequeos deben documentarse y firmarse.

- Auditorías internas, llevadas a cabo por un auditor interno cualificado e independiente, que compruebe las medidas implantadas y la documentación de soporte cumple con los requisitos del ENS.

- Auditorías externas, llevadas a cabo por un auditor externo debidamente cualificado, que verifique el cumplimiento del ENS en la entidad.

Si los sistemas son de nivel bajo, una autoevaluación periódica es suficiente, pero si son de nivel medio o alto están sujetos como mínimo a una auditoría cada dos años en la que ser revisarán la política de seguridad y su cumplimiento, así como el conjunto de riesgos, normativas, procedimientos y controles establecidos.

8.4 MEJORA CONTINUA

El modelo básico cuando hablamos de mejora continua es el círculo de Deming (PDCA, Planificar, Desarrollar, Comprobar y Actuar), que incorporan las normas ISO de gestión de sistemas, por lo que está probada su aplicabilidad en este ámbito. La idea básica de este modelo es que se aprenda de los errores y poco a poco se vaya mejorando la gestión de los sistemas, que de esta manera serán cada vez más eficaces y eficientes. El modelo permite definir indicadores y métricas

comparables y medibles en el tiempo para verificar el cumplimiento de los objetivos y la mejora del sistema.

En este caso se cuenta por un lado con los resultados de las acciones de verificación y validación, que reportarán interesantes hallazgos. Esta información será la base sobre la que se pueden decidir acciones de mejora para el sistema.

Asimismo la gestión de incidencias es una fuente importante de información sobre aspectos que deben ser mejorados, ya que eliminando la causa raíz de los incidentes se habrá evitado que vuelvan a ocurrir eventos iguales o semejantes.

Formalizar en un plan las acciones de mejora que se emprendan servirá para justificar el cumplimiento de este aspecto del ENS.

CASO PRÁCTICO 9

9.1 CONTEXTO

El Ayuntamiento de Villanueva lleva varios años empeñado en modernizar el Municipio, y el equipo que gestiona el consistorio siempre ha tenido claro que las Tecnologías de la Información y la Comunicación eran las herramientas para conseguirlo.

Existe un grupo de Informática, formado por un responsable de Sistemas, Luís y un técnico, Cristina. Varias tareas están subcontratadas.

El grupo cuenta con una pequeña oficina en el Ayuntamiento, donde trabajan Luís y Cristina, así como un cuarto en el sótano en el que han ubicado el CPD.

Hace dos años lanzaron la página Web del Ayuntamiento. Esta primera página era informativa, pero ya tenía un Buzón del Ciudadano, una dirección de correo electrónico para que los ciudadanos expresaran sus quejas, sugerencias e incluso llegó alguna que otra felicitación.

Hace un año se pusieron en marcha los dos primeros servicios, peticiones de licencias de obra y certificados de empadronamiento.

Para ello se compró un nuevo servidor que albergara inicialmente estos dos servicios y tuviera capacidad para los que vinieran más adelante.

Las aplicaciones utilizadas son desarrollos a medida:

- VillanuevaGestión, para la gestión de expedientes municipales, entre ellos la concesión de licencias de obra.

- VillanuevaPadrón, para la gestión del padrón municipal (altas, bajas y modificaciones).

El mapa de red es como sigue.

9.2 POLÍTICA DE SEGURIDAD

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día dos de Enero de 2011 por la Corporación Municipal de Villanueva.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

El Ayuntamiento depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información

tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La entidad es consciente de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

PREVENCIÓN

La entidad evita, o al menos intenta prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la entidad:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se monitoriza la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

RESPUESTA
La entidad ha establecido mecanismos para responder eficazmente a los incidentes de seguridad.

Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

SE han establecido protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

RECUPERACIÓN
Para garantizar la disponibilidad de los servicios críticos, la entidad ha desarrollado planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE
Esta política se aplica a todos los sistemas TIC de El Ayuntamiento y a todos los miembros de la organización, sin excepciones.

MISIÓN
Ofrecer al ciudadano un servicio de Administración Municipal, a través de medios electrónicos, potenciando el uso de las Nuevas Tecnologías en el Ayuntamiento y en la ciudadanía.

Los principales objetivos que se persiguen son:

- Fomentar la relación electrónica del ciudadano con el Ayuntamiento.

- Reducir tiempos de espera de atención al ciudadano.

- Acortar tiempos de espera en la resolución de trámites solicitados por el ciudadano.

- Desarrollar un sistema de gestión de información documental que facilite un rápido acceso del personal del servicio a la información solicitada por el ciudadano.

MARCO NORMATIVO
Esta política se enmarca en la siguiente legislación:

1. RD 3/2010 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. BOE de 29 de enero de 2010.

2. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal.

4. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

5. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

6. Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

7. Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

8. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

9. Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

ORGANIZACIÓN DE LA SEGURIDAD

El Comité de Seguridad TIC estará formado por el concejal responsable de la administración electrónica, el Departamento de Sistemas y los Responsables de los Servicios Electrónicos.

El Secretario del Comité de Seguridad TIC será el Responsable del Departamento de Sistemas que se encargará de convocar las reuniones del Comité y levantar acta de las mismas.

El Comité de Seguridad TIC reportará a la Corporación Municipal.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Coordinar y aprobar las acciones en materia de seguridad de la información.

- Impulsar la cultura en seguridad de la información.

- Participar en la categorización de los sistemas y el análisis de riesgos.

- Revisar la documentación relacionada con la seguridad del sistema.

- Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.

Las responsabilidades del Responsable de Seguridad de la Información son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.

- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.

- Gestionar la formación y concienciación en materia de seguridad TIC.

- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.

- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

- Las responsabilidades del Responsable del Sistema son:

- Gestionar el Sistema durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.

- Definir los criterios de uso y los servicios disponibles en el Sistema.

- Definir las políticas de acceso de usuarios al Sistema.

- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.

- Realizar el análisis y gestión de riesgos en el Sistema.

- Elaborar y aprobar la documentación de seguridad del Sistema.

- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.

- Implantar y controlar las medidas específicas de seguridad del Sistema.

- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

- Suspensión el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves

de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por la Corporación Municipal a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta política de seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Corporación Municipal y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

El Ayuntamiento trata datos de carácter personal. El Documento de seguridad que encuentra bajo la custodia del Responsable de Seguridad recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de El Ayuntamiento se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá al menos una vez al año o cuando cambien la información manejada, los servicios prestados, suceda un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política de seguridad de la Información complementa las políticas de seguridad del Ayuntamiento de Villanueva en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet para su consulta.

OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Villanueva tienen la obligación de conocer y cumplir esta política de seguridad de

la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros del Ayuntamiento de Villanueva atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del Ayuntamiento de Villanueva, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

TERCERAS PARTES

Cuando del Ayuntamiento de Villanueva preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta política de seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Villanueva utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos

específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

9.3. CATEGORIZACIÓN DEL SISTEMA

El sistema se ha categorizado valorando los parámetros de confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad, según los criterios que se han definido.

9.3.1 Confidencialidad

Valor	Escala
Alto	Porque la información debe conocerla un número muy reducido de personas. Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque su revelación causaría un grave daño, de difícil o imposible reparación. Porque su revelación supondría el incumplimiento grave de una norma. Porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas masivas (alteración seria del orden público).

Valor	Escala
Medio	Porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita. Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque su revelación causaría un daño importante aunque subsanable. Porque su revelación supondría el incumplimiento material o formal de una norma. Porque su revelación causaría pérdidas económicas importantes. Porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas públicas (alteración del orden público).
Bajo	Porque la información no deben conocerla personas ajenas a la organización. Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque su revelación causaría algún perjuicio. Porque su revelación supondría el incumplimiento leve de una norma. Porque su revelación supondría pérdidas económicas apreciables. Porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en múltiples protestas individuales.
Sin valorar	Información de carácter público, accesible por cualquier persona.

9.3.2 Integridad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden,... Porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación. Porque su manipulación o modificación no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque su manipulación o modificación no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en protestas masivas (alteración seria del orden público).
Medio	Por disposición legal o administrativa: ley, decreto, orden,... Porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable. Porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma. Porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes. Porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público).

Valor	Escala
Bajo	Por disposición legal o administrativa: ley, decreto, orden,... Porque su manipulación o modificación no autorizada causaría algún perjuicio. Porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma. Porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables. Porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales.

9.3.3 Autenticidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden,... Porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación. Porque su la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque su la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración seria del orden público).

Valor	Escala
Medio	Por disposición legal o administrativa: ley, decreto, orden,... Porque su la falsedad en su origen o en su destinatario: causaría un daño importante aunque subsanable. Porque su la falsedad en su origen o en su destinatario supondría el incumplimiento material o formal de una norma. Porque su la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes. Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público).
Bajo	Por disposición legal o administrativa: ley, decreto, orden,... Porque su la falsedad en su origen o en su destinatario causaría algún perjuicio. Porque su la falsedad en su origen o en su destinatario supondría el incumplimiento leve de una norma. Porque su la falsedad en su origen o en su destinatario supondría pérdidas económicas apreciables. Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque su la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales.
Sin valorar	Cuando el origen es irrelevante o ampliamente conocido por otros medios. Cuando el destinatario es irrelevante, por ejemplo por tratarse de información de difusión anónima.

9.3.4 Trazabilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden,... Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error grave. Porque la incapacidad para rastrear un acceso a la información impediría la capacidad para perseguir delitos. Porque la incapacidad para rastrear un acceso a la información facilitaría enormemente la comisión de delitos graves.
Medio	Por disposición legal o administrativa: ley, decreto, orden,... Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad de subsanar un error grave. Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error importante. Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad para perseguir delitos. Porque la incapacidad para rastrear un acceso a la información facilitaría la comisión de delitos.
Bajo	Por disposición legal o administrativa: ley, decreto, orden,... Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores. Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
Sin valorar	Cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios. Cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios.

9.3.5 Disponibilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible reparación. Porque la indisponibilidad de la información supondría el incumplimiento grave de una norma. Porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público). Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es inferior a 4 horas.
Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque la indisponibilidad de la información causaría un daño importante aunque subsanable. Porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma. Porque la indisponibilidad de la información causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas públicas (alteración del orden público). Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es de entre 4 y 24 horas (un día).

Valor	Escala
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,... Porque la indisponibilidad de la información causaría algún perjuicio. Porque la indisponibilidad de la información supondría el incumplimiento leve de una norma. Porque la indisponibilidad de la información supondría pérdidas económicas apreciables. Porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque la indisponibilidad de la información podría desembocar en múltiples protestas individuales. Cuando el RTO se sitúa entre 1 y 5 días (una semana).
Sin valorar	Cuando la información es prescindible por tiempo indefinido. Cuando el RTO es superior a 5 días laborables (una semana).

9.4 CATEGORÍA DEL SISTEMA

Se detallan a continuación las valoraciones de cada uno de los activos fundamentales, que son los correspondientes a Servicios (de administración electrónica) e Información.

Como establece el ENS, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio. Consecuentemente, la categoría del Sistema viene dada por el valor máximo en cada parámetro.

ID	ACTIVO	C	I	A	T	D
	SERVICIOS					
S01	Portal web	Sin valorar	B	B	B	M
S02	Gestión de Expedientes	M	M	M	M	B

ID	ACTIVO	C	I	A	T	D
S03	Padrón	M	M	M	M	B
	INFORMACIÓN					
I01	Información web	B	B	B	B	M
I02	Expedientes	M	M	M	M	M
I03	Licencias	B	M	M	M	B
I04	Datos del Padrón	M	M	M	M	B
	SISTEMA	M	M	M	M	M

La categoría del Sistema es Media, por lo que a estos activos se les aplicará como mínimo aquellas medidas de seguridad estipuladas para este nivel en el Anexo II, Medidas de Seguridad, del ENS.

9.5 VALORACIÓN DE LOS ÁCTIVOS

Se valoran aquí el resto de los activos, que no pertenecen a las categorías anteriores y que tienen dependencias con ellos.

Para ello en primer lugar se han identificado las dependencias entre los activos de tipo hardware, software, personal e instalaciones con los activos de tipo servicios e información.

ID	ACTIVO	Portal web	Gestión de Expedientes	Padrón	Información web	Expedientes	Licencias	Datos del Padrón
	HARDWARE							
HW01	Servidor Web	x	x	x	x			

ID	ACTIVO	Portal web	Gestión de Expedientes	Padrón	Información web	Expedientes	Licencias	Datos del Padrón
HW02	Servidor e-administración					X	X	x
HW03	Red DMZ					x	x	x
HW04	Red Lan	x	x	x	x			
HW05	Equipos de usuario	x	x	x	x	x	x	x
HW06	Periféricos		x	x		x	x	x
	SOFTWARE							
SW01	Aplicación Web	x			x			
SW02	VillanuevaGestión		x			x	x	
SW03	VillanuevaPadrón			x				x
	PERSONAL							
P01	Personal del Ayuntamiento	x	x	x	x	x	x	x
P02	Personal subcontratado	x	x	x	x	x	x	x
	INSTALACIONES							
IN01	CPD	x	x	x	x	x	x	x
IN02	Oficinas del Ayuntamiento	x	x	x	x	x	x	x

La valoración de los activos de tipo hardware, software, personal e instalaciones según especifica el ENS, es la heredada de los activos de tipo servicios e información. Por lo tanto su valoración teniendo en cuenta las dependencias identificadas es la siguiente:

ID	ACTIVO	C	I	A	T	D
	HARDWARE					
HW01	Servidor Web	M	M	M	M	M
HW02	Servidor e-administración	M	M	M	M	M
HW03	Red DMZ	M	M	M	M	M
HW04	Red Lan	M	M	M	M	M
HW05	Equipos de usuario	M	M	M	M	M
HW06	Periféricos	M	M	M	M	M
	SOFTWARE					
SW01	Aplicación Web	M	M	M	M	M
SW02	VillanuevaGestión	M	M	M	M	M
SW03	VillanuevaPadrón	M	M	M	M	M
	PERSONAL					
P01	Personal del Ayuntamiento	M	M	M	M	M
P02	Personal subcontratado	M	M	M	M	M
	INSTALACIONES					
IN01	CPD	M	M	M	M	M
IN02	Oficinas del Ayuntamiento	M	M	M	M	M

9.6 ANÁLISIS DE RIESGOS

Se ha llevado a cabo un análisis de riesgos detallado, utilizando la herramienta Pilar y los activos y valoraciones detallados anteriormente.

PILAR estima los riesgos según una escala simple de seis valores:

{5}	crítico
{4}	muy alto
{3}	alto
{2}	medio
{1}	bajo
{0}	insignificante

PILAR presenta los niveles de criticidad con un decimal, de forma que se puede relativizar el riesgo relativo dentro de un mismo nivel.

Los resultados para el riesgo potencial, el que habría sin aplicar medidas de seguridad, y el actual, con las medidas de seguridad aplicadas, se muestran a continuación.

9.6.1 Riesgo potencial

Activo	[D]	[I]	[C]	[A]	[T]
[S] Servicios	{5.1}	{4.5}	{4.5}	{5.1}	{4.2}
[S01] Portal web	{5.1}	{4.5}	{4.5}	{5.1}	{4.2}
[S02] Gestión de expedientes	{5.1}	{4.5}	{4.5}	{5.1}	{4.2}
[S03] Padrón	{5.1}	{4.5}	{4.5}	{5.1}	{4.2}
[I] Información	{5.1}	{3.9}	{4.5}	{4.5}	{2.8}
[I01] Información web	{5.1}	{3.9}	{4.5}	{4.5}	{2.8}
[I02] Expedientes	{5.1}	{3.9}	{4.5}	{4.5}	{2.8}
[I03] Licencias	{5.1}	{3.9}	{4.5}	{4.5}	{2.8}
[I04] Datos del padrón	{5.1}	{3.9}	{4.5}	{4.5}	{2.8}
[HW] Hardware	{4.4}	{2.4}	{3.6}	{3.6}	{3.3}
[HW01] Servidor Web	{4.4}	{2.1}	{3.4}	{3.4}	{3.3}
[HW02] Servidor de e-administración	{4.4}	{2.1}	{3.4}	{3.4}	{3.3}
[HW03] Red DMZ	{4.2}	{2.4}	{3.6}	{3.6}	{3.3}
[HW 04] Red Lan	{4.2}	{2.4}	{3.6}	{3.6}	{3.3}
[HW05] Equipos de usuario	{4.4}	{2.1}	{3.4}	{3.4}	{3.0}
[HW06] Periféricos	{4.4}	{2.1}	{3.4}	{3.4}	{3.0}
[SW] Software	{4.2}	{4.4}	{4.4}	{4.4}	{4.4}
[SW01] Aplicación web	{4.2}	{4.4}	{4.4}	{4.4}	{4.4}
[SW02] VillanuevaGestión	{4.2}	{4.4}	{4.4}	{4.4}	{4.4}
[SW03] VillanuevaPadrón	{4.2}	{4.4}	{4.4}	{4.4}	{4.4}
[P] Personal	{2.5}	{2.0}	{2.1}	{2.1}	{1.5}
[P01] Personal del Ayuntamiento	{2.5}	{2.0}	{2.1}	{2.1}	{1.5}
[P02] Personal subcontratado	{2.5}	{2.0}	{2.1}	{2.1}	{1.5}
[L] Instalaciones	{3.3}	{2.8}	{2.8}	{2.8}	{2.8}
[IN01] CPD	{3.3}	{2.8}	{2.8}	{2.8}	{2.8}
[IN02] Oficinas del Ayuntamiento	{3.3}	{2.8}	{2.8}	{2.8}	{2.8}

9.6.2 Riesgo actual

Activo	[D]	[I]	[C]	[A]	[T]
[S] Servicios	{3.5}	{3.6}	{3.6}	{4.1}	{3.3}
[S01] Portal web	{3.5}	{3.6}	{3.6}	{4.1}	{3.3}
[S02] Gestión de expedientes	{3.5}	{3.6}	{3.6}	{4.1}	{3.3}
[S03] Padrón	{3.5}	{3.6}	{3.6}	{4.1}	{3.3}
[I] Información	{3.3}	{2.6}	{2.5}	{1.6}	{1.8}
[I01] Información web	{3.3}	{2.6}	{2.5}	{1.6}	{1.8}
[I02] Expedientes	{3.3}	{2.6}	{2.5}	{1.6}	{1.8}
[I03] Licencias	{3.3}	{2.6}	{2.5}	{1.6}	{1.8}
[I04] Datos del padrón	{3.3}	{2.6}	{2.5}	{1.6}	{1.8}
[HW] Hardware	{3.3}	{0.7}	{2.0}	{1.2}	{2.6}
[HW01] Servidor Web	{3.3}	{0.7}	{2.0}	{1.1}	{2.6}
[HW02] Servidor de e-administración	{3.3}	{0.7}	{2.0}	{1.1}	{2.6}
[HW03] Red DMZ	{1.8}	{0.0}	{1.3}	{1.2}	{0.7}
[HW 04] Red Lan	{1.8}	{0.0}	{1.3}	{1.2}	{0.7}
[HW05] Equipos de usuario	{3.3}	{0.7}	{2.0}	{1.1}	{1.7}
[HW06] Periféricos	{3.3}	{0.7}	{2.0}	{1.1}	{1.7}
[SW] Software	{1.5}	{2.4}	{2.4}	{2.4}	{2.4}
[SW01] Aplicación web	{1.5}	{2.4}	{2.4}	{2.4}	{2.4}
[SW02] VillanuevaGestión	{1.5}	{2.4}	{2.4}	{2.4}	{2.4}
[SW03] VillanuevaPadrón	{1.5}	{2.4}	{2.4}	{2.4}	{2.4}
[P] Personal	{1.1}	{1.1}	{1.1}	{1.1}	{1.1}
[P01] Personal del Ayuntamiento	{1.1}	{1.1}	{1.1}	{1.1}	{1.1}
[P02] Personal subcontratado	{1.1}	{1.1}	{1.1}	{1.1}	{1.1}
[L] Instalaciones	{2.7}	{2.4}	{2.4}	{2.4}	{2.4}
[IN01] CPD	{2.7}	{2.4}	{2.4}	{2.4}	{2.4}
[IN02] Oficinas del Ayuntamiento	{2.7}	{2.4}	{2.4}	{2.4}	{2.4}

No se aprecian riesgos con la suficiente entidad para con-

siderar necesario aplicar más controles que los requeridos por el ENS a excepción del Plan de Continuidad, que se ha considerado importante desarrollar para evitar daños a la reputación del Ayuntamiento.

9.7 DECLARACIÓN DE APLICABILIDAD

Teniendo en cuenta que la categoría del sistema del Ayuntamiento de Villanueva es media y los resultados del análisis de riesgos llevado a cabo, se ha determinado que las medidas aplicables son las siguientes:

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Aplicado/ No Aplicado
	ORG	MARCO ORGANIZATIVO	
categoría	org.1	Política de seguridad	Aplicado
categoría	org.2	Normativa de seguridad	Aplicado
categoría	org.3	Procedimientos de seguridad	Aplicado
categoría	org.4	Proceso de autorización	Aplicado
	OP	MARCO OPERACIONAL	
	op.pl	Planificación	
categoría	op.pl.1	Análisis de riesgos	Aplicado
categoría	op.pl.2	Arquitectura de seguridad	Aplicado
categoría	op.pl.3	Adquisición de nuevos componentes	Aplicado
D	op.pl.4	Dimensionamiento / Gestión de capacidades	Aplicado
	op.acc	Control de acceso	
A T	op.acc.1	Identificación	Aplicado
I C A T	op.acc.2	Requisitos de acceso	Aplicado

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Aplicado/ No Aplicado
I C A T	op.acc.3	Segregación de funciones y tareas	Aplicado
I C A T	op.acc.4	Segregación de funciones y tareas	Aplicado
I C A T	op.acc.5	Mecanismo de autenticación	Aplicado
I C A T	op.acc.6	Acceso local (local logon)	Aplicado
I C A T	op.acc.7	Acceso remoto (remote login)	Aplicado
	op.exp	Explotación	
categoría	op.exp.1	Inventario de activos	Aplicado
categoría	op.exp.2	Configuración de seguridad	Aplicado
categoría	op.exp.3	Gestión de la configuración	Aplicado
categoría	op.exp.4	Mantenimiento	Aplicado
categoría	op.exp.5	Gestión de cambios	Aplicado
categoría	op.exp.6	Protección frente a código dañino	Aplicado
categoría	op.exp.7	Gestión de incidencias	Aplicado
T	op.exp.8	Registro de la actividad de los usuarios	No aplicado
categoría	op.exp.9	Registro de la gestión de incidencias	Aplicado
T	op.exp.10	Protección de los registros de actividad	No aplicado
categoría	op.exp.11	Protección de claves criptográficas	Aplicado
	op.ext	Servicios externos	
categoría	op.ext.1	Contratación y acuerdos de nivel de servicio	Aplicado
categoría	op.ext.2	Gestión diaria	Aplicado

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Aplicado/ No Aplicado
D	op.ext.9	Medios alternativos	No aplicado
	op.cont	Continuidad del servicio	
D	op.cont.1	Análisis de impacto	Aplicado
D	op.cont.2	Plan de continuidad	Aplicado
D	op.cont.3	Pruebas periódicas	No aplicado
	Op.mon	Monitorización del sistema	
categoría	op.mon.1	Detección de intrusión	No aplicado
categoría	op.mon.2	Sistema de métricas	No aplicado
	MP	MEDIDAS DE PROTECCIÓN	
	mp.if	Protección de las instalaciones e infraestructuras	
categoría	mp.if.1	Áreas separadas y con control de acceso	Aplicado
categoría	mp.if.2	Identificación de las personas	Aplicado
categoría	mp.if.3	Acondicionamiento de los locales	Aplicado
D	mp.if.4	Energía eléctrica	Aplicado
D	mp.if.5	Protección frente a incendios	Aplicado
D	mp.if.6	Protección frente a inundaciones	Aplicado
categoría	mp.if.7	Registro de entrada y salida de equipamiento	Aplicado
D	mp.if.9	Instalaciones alternativas	No aplicado

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Aplicado/ No Aplicado
	mp.per	Gestión del personal	
categoría	mp.per.1	Caracterización del puesto de trabajo	Aplicado
categoría	mp.per.2	Deberes y obligaciones	Aplicado
categoría	mp.per.3	Concienciación	Aplicado
categoría	mp.per.4	Formación	Aplicado
D	mp.per.9	Personal alternativo	No aplicado
	mp.eq	Protección de los equipos	
categoría	mp.eq.1	Puesto de trabajo despejado	Aplicado
A	mp.eq.2	Bloqueo de puesto de trabajo	Aplicado
categoría	mp.eq.3	Protección de equipos portátiles	Aplicado
D	mp.eq.9	Medios alternativos	Aplicado
	mp.com	Protección de las comunicaciones	
categoría	mp.com.1	Perímetro seguro	Aplicado
C	mp.com.2	Protección de la confidencialidad	Aplicado
I A	mp.com.3	Protección de la autenticidad y de la integridad	Aplicado
categoría	mp.com.4	Segregación de redes	No aplicado
D	mp.com.9	Medios alternativos	No aplicado
	mp.si	Protección de los soportes de información	
C	mp.si.1	Etiquetado	Aplicado
I C	mp.si.2	Criptografía	Aplicado

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Aplicado/ No Aplicado
categoría	mp.si.3	Custodia	Aplicado
categoría	mp.si.4	Transporte	Aplicado
C	mp.si.5	Borrado y destrucción	Aplicado
	mp.sw	Protección de las aplicaciones informáticas	
categoría	mp.sw.1	Desarrollo	Aplicado
categoría	mp.sw.2	Aceptación y puesta en servicio	Aplicado
	mp.info	Protección de la información	
categoría	mp.info.1	Datos de carácter personal	Aplicado
C	mp.info.2	Calificación de la información	Aplicado
C	mp.info.3	Cifrado	No aplicado
I A	mp.info.4	Firma electrónica	Aplicado
T	mp.info.5	Sellos de tiempo	No aplicado
C	mp.info.6	Limpieza de documentos	Aplicado
D	mp.info.9	Copias de seguridad (back Up)	Aplicado
	mp.s	Protección de los servicios	
categoría	mp.s.1	Protección del correo electrónico	Aplicado
categoría	mp.s.2	Protección de servicios y aplicaciones web	Aplicado
D	mp.s.8	Protección frente a la denegación de servicio	Aplicado
D	mp.s.9	Medios alternativos	No aplicado

9.8 NORMATIVA

Las normas que rigen la seguridad de la información en el Ayuntamiento de Villanueva son:

1. Control de documentación.
2. Procedimiento de autorización.
3. Gestión de compras.
4. Gestión de la capacidad.
5. Gestión de accesos lógicos.
6. Gestión de activos.
7. Gestión de cambios.
8. Gestión de incidencias.
9. Gestión de criptografía.
10. Gestión de servicios externos.
11. Gestión de la continuidad.
12. Gestión de la seguridad física.
13. Gestión del personal.
14. Protección de los equipos.
15. Protección de las comunicaciones.
16. Protección de la información y los soportes.
17. Protección de servicios y aplicaciones.

9.9 DECLARACIÓN DE CONFORMIDAD

DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Nombre del declarante: Excelentísimo Ayuntamiento de Villanueva

Dirección postal: Plaza del Ayuntamiento s/n

Dirección electrónica: ayuntamiento@villanueva.es

En cumplimiento de lo dispuesto en el artículo 41 del Real

Decreto 372010, de 8 de enero, declara bajo su exclusiva responsabilidad la conformidad del Sistema para la Gestión de Expedientes del Ayuntamiento al que se refiere este documento, con el Esquema Nacional de Seguridad regulado en el citado real decreto.

Información adicional:

1) Las sedes y registros electrónicos, así como el acceso electrónico de los ciudadanos a los mismos y a los servicios que estos proporcionan, cumplen las exigencias de seguridad del Esquema Nacional de Seguridad.

2) Las especificaciones de seguridad están incluidas en el ciclo de vida de los servicios y sistemas, acompañadas del correspondiente procedimiento de control.

3) El mecanismo de control establecido por el Ayuntamiento de Villanueva que efectúa la declaración de garantía de cumplimiento del ENS, consiste en:

- Revisión anual de la política de seguridad.
- Auditorías bienales de seguridad para comprobar el correcto funcionamiento de las medidas de seguridad.

En Villanueva a 10 de Enero de 2011

Persona que lo firma: José García Fernández

Cargo que ostenta: Excelentísimo Sr. Alcalde

Firma:

Activo. Componente o funcionalidad de un sistema de infor-

10 TÉRMINOS Y DEFINICIONES

mación susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos con-

sistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que se consideran críticos.

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Proceso de seguridad. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Servicios acreditados. Servicios prestados por un sistema

con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza

11 BIBLIOGRAFÍA

DOCUMENTO	ENLACE
Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE número 150 de 23/6/2007.	http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf
RD 3/2010 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. BOE de 29 de enero de 2010.	http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf
RD 4/2010 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica. BOE de 29 de enero de 2010.	http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE número 298 de 14/12/1999.	http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf
Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.	http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf
2001/264/CE Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0066:ES:PDF
CCN-STIC-201 Organización y Gestión para la Seguridad de las TIC.	https://www.ccn-cert.cni.es

CCN-STIC-402 Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.	https://www.ccn-cert.cni.es
CCN-STIC-801 Responsables y Funciones. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-802 Guía de Auditoría. Junio 2010.	https://www.ccn-cert.cni.es
CCN-STIC-803 Valoración de los Sistemas. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-804 Guía de Implantación. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-805 Política de Seguridad. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-806 Plan de Adecuación. 2010	https://www.ccn-cert.cni.es
CCN-STIC-807 Criptología de Empleo. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-808 Verificación del Cumplimiento de las Medidas. 2010.	https://www.ccn-cert.cni.es
CCN-STIC-809 Declaración de Conformidad. 2010.	https://www.ccn-cert.cni.es
CNSS Inst. 4009 National Information Assurance (IA) Glossary. April 2010.	http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.	http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
ISO Guide 73 Risk management — Vocabulary. 2009.	
SP 800-12 An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. October 1995.	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

www.ametic.es

AMETIC

Príncipe de Vergara 74-4ª
28006 Madrid
T 91 590 23 00

Orense 62
28020 Madrid
Telf: 91 417 08 90

E ametic@ametic.es
W www.ametic.es

Proyecto de difusión del Esquema Nacional de Seguridad (TSI-020100-2010-332). Cofinanciado por el Ministerio de Industria, Turismo y Comercio, dentro del Plan Nacional de Investigación Científica, desarrollo e Innovación Tecnológica 2008-2011:

Con la colaboración de: