FICHA DE BUENA PRÁCTICA

IDENTIFICACIÓN DE LA BUENA PRÁCTICA

Nombre: Adecuación al ENS de los sistemas de información para los servicios de la Sede Electrónica del Ayuntamiento de Alcobendas

Responsable: Dirección General de Informática

Colaboradores (internos y externos): Planificación, Calidad, Organización, Seguridad Ciudadana, AENOR, seguridaddelainformacion.com, Innovación Tecnológica

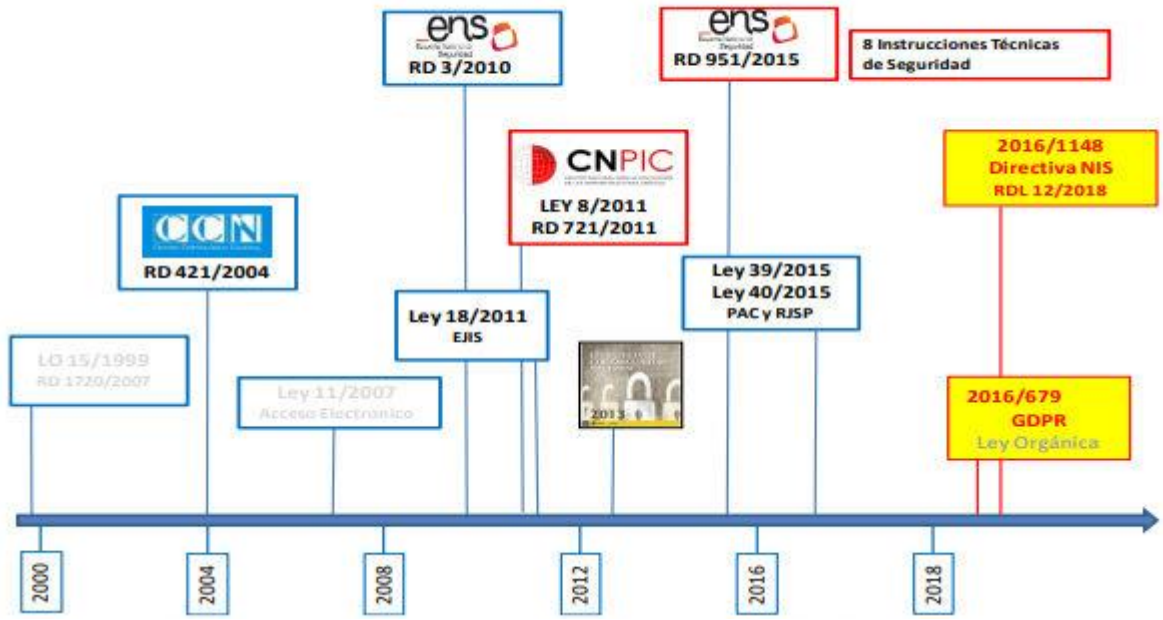
Fecha de inicio: 2017

Conceptos Fundamentales de la Excelencia: Añadir valor para los clientes; Desarrollar la capacidad de la organización; Aprovechar la creatividad y la innovación; Gestionar con agilidad

ENFOQUE

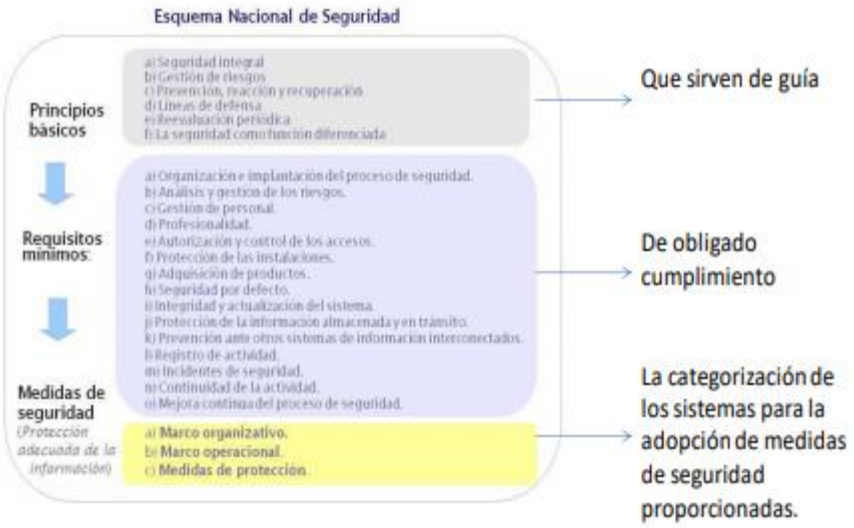
Antecedentes:

Los cambios en la sociedad, que generan nuevas leyes y normativa que regula la Administración, y la permanente necesidad de innovar en sus servicios y prestaciones a la ciudadanía, hacen necesario un modelo que permita conjugar factores de la calidad en la gestión con la propia confianza y seguridad de las relaciones de la Ciudadanía con la Administración a través de medios digitales.



Esquema de evolución normativa en Administraciones

El RD 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Este Real Decreto establece los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información de las Administraciones públicas.



En este contexto, se debe tener en cuenta que la información y los datos personales se deben custodiar de acuerdo con las especificaciones funcionales del ENS, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar a conocimiento de personas no autorizadas.

En el gráfico siguiente se resumen esquemáticamente estas medidas de seguridad que se deberán tener en cuenta para el proyecto de adecuación al ENS:

Objeto: Adecuación al ENS de los sistemas de información para los servicios de la Sede Electrónica del Ayuntamiento de Alcobendas

Objetivo/s: Adaptación del SGSE al ENS.

DESPLIEGUE

El proceso de implantación de acuerdo con los requisitos del ENS que se ha desarrollado en Alcobendas se puede resumir los siguientes grandes hitos:

- Constitución de un equipo multidisciplinar para el proceso de implantación.
- Planificación inicial del proyecto y sus diferentes fases.
- Aprobación de la Política de Seguridad de la Información, Normativa y Procedimientos del Sistema, y nombramiento del Comité de Seguridad de la Información.
- Categorización del Sistema, donde se identifican los activos esenciales, es decir, los servicios y la información del Ayuntamiento de Alcobendas. **Resultando una CATEGORÍA MEDIA del Sistema de Información de la Sede Electrónica.** Activos de información del Ayuntamiento de Alcobendas utilizados para la categorización de los sistemas de acuerdo con el Esquema Nacional de Seguridad y posteriormente considerados en el análisis de riesgos.

Se ha valorado el impacto que tendría un incidente que afecte a la seguridad de la información y los sistemas. Para determinar ese impacto se tuvo en cuenta las dimensiones de la seguridad:

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

El impacto que tendría un incidente que pudiese ocurrir sobre cada información o cada servicio pueden afectar a una o más de sus dimensiones de seguridad y cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO.

Como consecuencia de la valoración de los servicios y la información, ha resultado una CATEGORÍA MEDIA del Sistema de Información de los procedimientos electrónicos y aplicaciones informáticas.

El Esquema Nacional de Seguridad valora aquellos servicios que son relevantes para el proceso administrativo. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares del organismo. En cualquier caso, los servicios aquí contemplados tienen identidad propia con independencia de los medios que se empleen para su prestación, asumiendo el organismo que los presta unas obligaciones con respecto a los mismos.

- Análisis de Riesgos de los activos de información y los servicios identificados, y los activos secundarios que dan soporte a los mismos. El objeto del análisis y gestión de los riesgos fue determinar el nivel de riesgo de la organización y las prioridades en cuanto al tratamiento de dicho riesgo, es decir, la implantación de medidas para mitigar o suprimir los riesgos.
    - Análisis de Riesgos del ENS, basado en los activos de información identificados, cuyo objeto fue determinar el nivel de riesgo de la organización y las prioridades en cuanto al tratamiento de dicho riesgo.
    - Se realizó un Análisis de Riesgos con la herramienta PILAR, que desarrolla la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que está desarrollada por el Centro Criptológico Nacional (CCN), adscrito al CNI. Los pasos seguidos para desarrollar el análisis de riesgos según el ENS y empleados en Alcobendas son:
        - Identificación y valoración de los activos del sistema.
        - Identificación de las dependencias entre activos.
        - Identificación de las amenazas.
        - Identificación y valoración de las medidas de seguridad que protegen dichas amenazas.
        - Identificación y valoración de los riesgos residuales

Como resultado final, se elabora el Informe de Análisis de Riesgos del ENS, donde se recogen las principales conclusiones de este, incluyendo los activos identificados, la madurez de las medidas de seguridad y el mapa de riesgos.

- **La Declaración de Aplicabilidad,** con las medidas de seguridad seleccionadas del anexo II del ENS, de acuerdo a la categoría correspondiente a los sistemas identificados.

En esta fase del proyecto, tras el análisis de riegos, la declaración de aplicabilidad, etc. es cuando empieza la verdadera implantación de las medidas de seguridad que se deben aplicar así en todas las acciones contempladas en el Plan de mejora.

- **Implantación del Plan de Mejora,** desarrollado para ejecutar las acciones necesarias para que los sistemas del Ayuntamiento de Alcobendas estén completamente adecuados al ENS. Esta implantación ha supuesto medidas y actuaciones como:
    - **Definir y aprobar la composición y funciones del Comité de Seguridad de la Información**
      Establecer los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo. Se determinó qué personas formarían parte del Comité de Seguridad de la Información, detallando su ámbito de responsabilidad y sus posibles relaciones con otros elementos de la organización. Todo ello se aprobó en mayo de 2018 por Decreto de Alcaldía.
    - **Aprobación de la documentación del Sistema de Gestión**
      En el ámbito del ENS se ha realizado una serie de documentación que conforma un Sistema de Gestión de Seguridad de la Información, y que debe ser aprobada de acuerdo a lo definido en la Política de Seguridad de la Información y al ENS.
    - **Concienciación:** Consejos sobre Seguridad de la Información en la Intranet, información en revistas de comunicación interna a la institución, y en prensa a los ciudadanos de Alcobendas, complementada con pop-ups periódicos en el arranque de los ordenadores a nivel Institucional.
    - **Mejora de la capacitación en materia de seguridad tecnológica** con jornadas, seminarios y cursos sobre Concienciación y Sensibilización en materia de Seguridad de la Información. Inclusión anual en el plan de formación Municipal

de cursos en materia de ciberseguridad. Formación específica en seguridad para técnicos TIC y personal con funciones de gestión en ámbitos TIC.

- **Acciones técnicas sobre los sistemas de información,** como puede ser actualización de sistemas operativos en servidores y equipos de personal municipal, actualización de la política de Contraseñas de acceso, securización completa de la web municipal bajo protocolo seguro de comunicación https, sustitución del protocolo de encriptación de las comunicaciones TLS 1.0 por versión superior, entre otras medidas técnicas.

- **Reuniones de seguimiento del proceso de implantación** tanto del equipo de proyecto como del Comité de Seguridad. Una vez desarrollados y aprobados inicialmente los procedimientos, la normativa de seguridad, etc. se fue implantando y controlando su efectividad, así como la idoneidad de lo descrito en los mismos por si eran susceptibles de cambios.
- **Formación**
  De acuerdo con el ENS, todos los miembros del Ayuntamiento debían involucrarse en el proceso de seguridad de la información y conocer y comprender las normas y procedimientos establecidos. La mejor manera de conseguirlo fue la realización de acciones de formación sobre la política, normativa y procedimientos de seguridad de manera que el personal aprendía y asimilaba las indicaciones sobre las normas con las que deben trabajar.

Se realizó una evaluación de los resultados obtenidos en relación a los objetivos perseguidos con las acciones formativas. Se han realizado, y se están realizando, diversas acciones encaminadas a la concienciación y formación en materia de seguridad, así como mejora de los sistemas de información. Entre ellas, podemos destacar:

- Consejos sobre Seguridad de la Información en la intranet y como pop-ups en el arranque de los ordenadores.
- Jornadas, seminarios y cursos sobre Concienciación y Sensibilización en materia de Seguridad de la Información.
- Difusión de la Política de Seguridad de la Información, Normativa y Procedimientos (información accesible en la Intranet Municipal).

Retos y dificultades:

En proyectos de esta envergadura y con un impacto tan importante en la organización, determinadas decisiones estratégicas y políticas pueden a veces ralentizar o dificultar el proceso si no hay una verdadera implicación, por lo que se debe planificar este tipo de proyectos teniendo muy en cuenta estas variables. En nuestro caso la implicación fue máxima a todos los niveles.

Este tipo de proyectos exigen cambios en la operativa de los empleados, en la propia Organización y a todos los niveles (Ej.: Políticas de contraseñas, doble factor de autenticación, etc.) y resulta vital realizar una buena gestión del cambio y concienciación sobre su necesidad, de forma previa, continua y firme. Estas acciones nos han facilitado el despliegue de las medidas técnicas. Su adecuación e implantación no deben paralizar a la Organización, a los servicios o a nuevos proyectos, pues de otro modo no resultarían eficaces.

En determinadas ocasiones algunos de los requisitos marcados en el ENS, suponen unas importantes inversiones (tiempo, económicos, contratación de nuevo personal y formación del existente, diseños…) para poner en marcha las medidas de seguridad en la información o compensatorias en el proceso de adaptación al ENS. Si el desaliento aparece en el proyecto

debemos recordar que nuestra meta ha de ser la mejora de la seguridad de forma continua, no la propia certificación. El esfuerzo continuado ha posibilitado que se obtuviese la certificación.

Durante este proceso de implantación del SGSI y adaptación al ENS, se han puesto de manifiesto algunos aspectos que han sido determinantes para poder lograr la adaptación:

- Se han identificado aspectos comunes en otros proyectos, como RGPD, gestión de riegos corporativa o planes directores. (Ej. Análisis de gestión de riesgos). La reutilización del conocimiento es clave. Como también lo es la planificación y estrategia, actuando como habilitadores para conseguir los objetivos. Calendarizar las actuaciones permiten reservar los recursos económicos, de tiempo, disponibilidad, personas y no perder el foco, aunque se produzcan desviaciones en la planificación.
- Destacar también como algunas actuaciones ya se venían desarrollando; ya se estaba dando cumplimiento a algunos de los requisitos marcados en el ENS, por lo que solamente ha sido necesario sistematizarlas, crear procedimientos formales o instrucciones para asegurar su continuidad y aplicación sistemáticas.
- Importancia de trabajo en equipo, resaltando que donde unas áreas y/o personas no llegan…otras áreas y personas puede aportar y crear sinergias fundamentales para el desarrollo del proyecto.
- La importancia de contar con ayudas externas, resultandos destacables tanto la labor de una buena consultoría especializada que pueda orientar en fases determinadas y concretas del proyecto, como las propias guías, manuales y otros documentos del CCN (Centro Criptológico Nacional), INCIBE, FEMP y otros organismos e instituciones.

Continuidad del proyecto

La gestión de la seguridad de la información es un proceso continuo que requiere ser verificado de forma sistemática y continua con el objeto de detectar brechas y cualquier tipo de incidentes de seguridad, así como detectar medidas, normas y/o elementos que hayan podido quedar obsoletos y que provoquen que no se esté realizando una efectiva gestión de los riesgos en la organización. Por eso, aunque se ha conseguido una mejora sustancial en la implementación de las medidas de seguridad refrendada por la certificación, el Ayuntamiento es consciente de continuar con la mejora continua de la seguridad, pues las medidas de hoy no garantizan el estado de seguridad del mañana.

Cada novedad tecnológica u operativa conlleva sus riesgos, y es nuestra labor evaluar continuamente los riesgos y adoptar medidas para reducir y/o eliminarlos.

Por ello resulta necesaria una monitorización y supervisión del Sistema de Gestión de Seguridad de la Información. El sistema se debe mantener actualizado de acuerdo a los nuevos enfoques, tendencias, nuevas tecnologías y cumplimientos legales que se requieran en el Ayuntamiento de Alcobendas.

Por otra parte, se deben seguir elaborando planes de auditoría y de formación para mantener a todos los miembros del Ayuntamiento sensibilizados con el proceso de seguridad de la información implantado.

El Esquema Nacional de Seguridad establece la necesidad de realizar una auditoría completa del sistema al menos cada dos años. No obstante, será conveniente realizar auditorías con una mayor frecuencia, al menos hasta que se haya logrado un buen ajuste y una buena asimilación de los procesos dentro de la organización.

Por todo ello, se sigue trabajando en:

- Planes de formación y concienciación del SGSI/ENS para todo el personal del Ayuntamiento de Alcobendas.
- Coordinación de auditorías internas del SGSI/ENS para comprobar la correcta y adecuada implantación del SGSI/ENS.
- Evaluación actualizada de riesgos y el RGPD.
- Auditorías de Seguridad de la Información.
- Gestión de incidencias (no conformidades), observaciones y oportunidades de mejora derivadas de los resultados de las auditorías, con el objeto de determinar y aplicar las acciones necesarias para corregir las desviaciones detectadas y lograr/mantener la mejora continua.
- Implantación progresiva y alineamiento con las herramientas y servicios que proporciona el CCN-CERTç
- Recopilar muestras de distintos indicadores y métricas para cumplimentar la encuesta anual del estado de la seguridad (INES) y conocer el estado de distintas medidas de seguridad.

Ventajas:

La experiencia de este proceso de implantación y certificación ha sido enriquecedora, muy positiva y, sin duda, ha servido tanto a los participantes del equipo de proyecto como al resto de la Organización, para crecer y mejorar en el camino de la gestión de sistemas en general y en particular en lo relativo a la gestión de la seguridad e información.

El trabajo realizado ha conllevado al entendimiento de la seguridad como un proceso de mejora continua., aspecto que, si bien era conocido por el equipo de trabajo, quizá no se había interiorizado en toda su dimensión.

Toda certificación conlleva una preparación que exige solventar dificultades, minimizar incertidumbres a través de nuevos conocimientos y preparar aquello que por una causa u otra no se ha tenido tiempo de materializar. Simplemente su preparación ya permite una mejora sustancial, además de visualizar la importancia de la seguridad en un mundo cada vez más complejo y digital. Superarlo es la recompensa a un equipo de trabajo que ha perseverado en su consecución y ha permitido mejorar sus capacidades y por ende la de los servicios que prestan.

EVALUACIÓN

Indicadores (cuantitativos y cualitativos) asociados a los objetivos

RESULTADOS

- Primer municipio de más de 100.00 habitantes en conseguir la certificación, integrándolo armónicamente con el resto de sistemas de información, de gestión y con el trabajo de equipos multidisciplinares, involucrando activamente a los responsables de seguridad de la ciudad, entendiendo la seguridad informática (TIC) como un eslabón adicional de seguridad para la gestión de la ciudad.

- Premio mejor proyecto de adecuación al ENS. CNIS 2019

- Buena práctica del club de Innovación:

https://www.clubdeinnovacion.es/proyecto-adecuacion-al-ens-los-sistemas-informacion-los-servicios-la-sede-electronica-del-ayuntamiento-alcobendas/

ENLACES DE INTERÉS

Esquema Nacional de Seguridad:
http://colabora-ayto.alcobendas.org/ENS/SitePages/Inicio.aspx

Publicación:
http://colabora-ayto.alcobendas.org/BancoConocimiento/Lists/Listado%20Publicaciones/DispForm.aspx?ID=8&Source=http%3A%2F%2Fcolabora%2Dayto%2Ealcobendas%2Eorg%2FBancoConocimiento%2FLists%2FListado%2520Publicaciones%2FAllItems%2Easpx&ContentTypeId=0x01007EFEB0D234F0B04D9017117B80E298EA

PERSONA DE CONTACTO

Nombre:	Sergio Rafael Caballero Benito
Puesto:	Director General de Informática
Dirección:	Plaza Mayor 1 – 28100 Alcobendas (Madrid)
Teléfono:	91 659 76 00
Mail:	scaballero@aytoalcobendas.org

Fecha de edición: 13/06/2019