Universidad Zaragoza
1542

Trabajo Fin de Grado

Seguridad de la Información en el Entorno Laboral

Autor:

Carlos Arbizu Milagro

Directora:

María Jesús Lapeña Marcos

Facultad de Economía y Empresa de Zaragoza (GADE)

Año 2014

Información

Autor del Trabajo: Carlos Arbizu Milagro

Director del Trabajo: María Jesús Lapeña Marcos

Título del Trabajo: Seguridad de la información en el entorno laboral

Titulación: Grado en Administración y Dirección de Empresas.

Resumen del contenido

Mediante este trabajo intento resaltar la importancia de un tema de gran interés y actualidad: la seguridad informática. El uso responsable, ético y legal de las TIC conlleva la protección de la información y de los sistemas que la contienen.

Comenzaremos definiendo el concepto de Seguridad de la información y Seguridad Informática, explicando qué es, por qué es tan importante y cómo debemos actuar para garantizar la protección de la información y controlar su flujo de transmisión.

Analizaremos los riesgos a los que está expuesto el sistema informático de la empresa y la información relativa a sus clientes, empleados socios o proveedores…; describiremos cuáles son estos riesgos y cómo desarrollar un buen Sistema de Gestión de Seguridad de la Información (SGSI) que nos permita gestionarlos, minimizarlos y tenerlos bajo control.

Haremos una revisión de la normativa legal en materia de seguridad informática, así como de los distintos tipos de certificaciones (o sellos de calidad) existentes al respecto, indicando las principales empresas que llevan a cabo dichas certificaciones en el territorio español.

Para finalizar, una vez hecha la revisión documental y obtenidos los conocimientos básicos sobre seguridad, utilizaremos lo aprendido en una vertiente más práctica; por una parte, presentamos una guía con recomendaciones básicas en materia de seguridad informática dirigida a empresas; y para finalizar, como aplicación práctica, haremos el análisis práctico de un caso real: analizaremos el estado de la seguridad informática en una empresa real y haremos una valoración de las medidas existentes y una serie de recomendaciones.

Abstract

With this project I try to show the importance of a topic which has so much interest in our days: the computing security. The responsible, ethic and legal use of TIC's involve the protection of the information and besides of the systems where it's saved.

First of all we define the concept of Information Security and Computing Security, explaining what is it, why is so important and how should we act to guarantee the protection of the information and control her transmission.

We will analyze the risks that the computed system of the enterprise is exposed at and the information relative of customers, employees, partners or suppliers…; we will describe which those risks are and how to develop a good System of Management of Information Security (SMIS) which allow us to manage them and also to have them controlled.

We will review the legal normative in subject of information security, the different kinds of certifications (or quality seals) that exists indicating the most important enterprises that use them in Spain.

Finally, once done the documental revision and obtained the basic knowledge of security, we will use it in a more practice vision; we will see a guide with basic recommendations in subject of information security for enterprises; and finally, like a practice application, we will make the practice analyze of a real case: we will analyze the status of the computing security in a real enterprise and we will also make a valuation of the existent measures and recommendations.

Índice

1. Introducción:

1.1. Planteamiento, justificación y objetivos del trabajo

A lo largo de este trabajo quiero **plantear** un tema de gran importancia e interés de la actualidad, que en los últimos años, está alcanzando la relevancia que realmente merece: la **Seguridad Informática y de la información**; y su implicación en la empresa.

Hace no muchos años, el concepto de seguridad de la información era casi desconocido. Había que proteger los equipos de escritorio, los servidores o los dispositivos de comunicaciones, pero no la información. Era suficiente con tener un buen antivirus, un cortafuegos, hacer copias de seguridad de vez en cuando y tener la sala de servidores cerrada con llave. La conexión a Internet de las empresas era poco habitual, el comercio electrónico era una promesa y los ciberataques y la ciberseguridad dos términos totalmente desconocidos.

Las cosas han cambiado mucho en los últimos años. La conexión a Internet es un aspecto imprescindible de cualquier empresa para la comunicación con proveedores, clientes o la propia administración. El comercio electrónico se afianza poco a poco como una poderosa fuente de ingresos para muchas organizaciones.

Los procesos han ganado en productividad y eficiencia con la incorporación de la tecnología; ahora es posible explotar la información de maneras que hace años no se podría imaginar.

Podemos llevar en nuestro bolsillo volúmenes de información jamás pensados. En unos años la tecnología ha irrumpido poco a poco, pero de manera imparable, en todos los ámbitos corporativos. Es inconcebible que hoy en día una empresa, sea grande, pequeña o incluso un autónomo, no esté conectada a Internet o no utilice las TIC en su actividad diaria.

En este nuevo escenario virtual no todos los riesgos que se presentan son comunes y reconocidos por todo el mundo.

Es clara, por tanto, la **justificación** para el estudio y desarrollo de este tema. En la actual sociedad de la información, toda empresa tiene una gran dependencia de las TIC; es por ello que es imprescindible hacer un uso estratégico de las mismas, hay que hacer un buen gobierno de las TIC para ponerlas al servicio del negocio y obtener calidad de los servicios, eficiencia, seguridad, disponibilidad, confidencialidad... Son muchas las amenazas que acechan sobre el sistema informático y muchos los riesgos a los que está sometido: accidentes fortuitos (fuego, inundaciones), errores humanos, ataques programados, software malicioso, accesos no autorizados a la información, pérdida de datos… Las consecuencias pueden ser muy graves: interrupción del servicio, pérdida de imagen, pérdidas económicas, posibles sanciones, imposibilidad de continuar con el

negocio… En definitiva, hay que conocer los riesgos para poder gestionarlos, controlarlos y minimizarlos.

La conexión a Internet e informatización del mundo de la empresa ha traído una horda de curiosos, delincuentes y ciberatacantes deseosos de robar información corporativa, dañar sistemas o aprovechar nuestras infraestructuras en su propio provecho.

El comercio electrónico tiene que abrirse paso entre diferentes técnicas de fraude online, y la movilidad que los dispositivos han traído consigo riesgos de sustracción de información sensible en caso de pérdida de un portátil o un smartphone.

Los nuevos sistemas de procesamiento de información han requerido el desarrollo y aplicación de mecanismos legales de protección de información sensible (como los datos personales).

El abundante número de empleados conectado a la red corporativa, introduce riesgos derivados del simple desconocimiento o de las llamadas "malas prácticas" (contraseñas de acceso muy simples, pinchar en los adjuntos de correos de desconocidos, entrar en Webs de riesgo…).

Este cambio radical no tiene vuelta atrás: ya no podemos volver a los libros de cuentas, a los documentos manuscritos o al correo postal. Y eso implica una gran dependencia. Sin tecnología, no hay empresa.

En definitiva, hemos entrado en una nueva era en la que ya no se gestionan sistemas informáticos. Gestionamos información, y lo hacemos en cualquier lugar de nuestra empresa: desde el Smartphone de un comercial hasta el equipo del director general. Eso ha obligado a que la seguridad se extienda más allá de los límites del departamento de Informática, en dirección hacia toda la empresa: Recursos Humanos, Asesoría legal, Administración, Logística, y en definitiva cualquier departamento de nuestra organización. Si cualquier persona gestiona información, cualquier persona debe aplicar medidas de seguridad.

Por ello, con este trabajo nos proponemos los siguientes **objetivos**:

- Mentalizarnos de la importancia de la seguridad informática; conocer las amenazas existentes y los riesgos derivados y sensibilizar sobre la necesidad de invertir en seguridad.
- Hacer una revisión de la documentación existente en materia de seguridad informática.
- Revisar detalladamente el marco normativo relativo a seguridad informática, tanto las medidas de obligado cumplimiento (ejemplo: ENS, de obligado cumplimiento en la Administración Pública) como las recomendaciones

ofrecidas en referencias nacionales o internacionales de reconocido prestigio (Norma ISO 27001).

- Evaluar/auditar el nivel de seguridad informática en una empresa real, estudiando las medidas técnicas y organizativas existentes para controlar y minimizar los riesgos.
- Elaborar una guía-resumen dirigida a empresa que recoja una serie de pautas a seguir y medidas a implantar para garantizar la seguridad del sistema informático.

1.2. Estructura del trabajo

Para desarrollar este tema, he decidido dividir este documento en 4 partes principales.

En primer lugar, repasaremos todos los conceptos fundamentales referidos a la seguridad informática y motivaremos la necesidad de poner en marcha una serie de medidas técnicas y organizativas que garanticen un buen nivel de seguridad.

A continuación, haremos una revisión de la normativa en materia de seguridad informática: leyes, referencias y estándares nacionales e internacionales que marcan las pautas a seguir para tener sistemas seguros; destacaremos la Norma ISO 27001 y el ENS (Esquema Nacional de Seguridad).

En el siguiente apartado, como aplicación de todo lo anterior, trabajaremos en un caso práctico: una evaluación/auditoría de la seguridad informática en una empresa real; hacemos una revisión de los controles existentes y presentamos los resultados obtenidos, haciendo una valoración de los mismos.

Finalmente, presentaremos una guía-resumen sobre lo que hay que saber y tener en cuenta para hacer un uso seguro de las TIC en la empresa.

Terminamos el trabajo con un apartado de conclusiones y otro con las referencias bibliográficas.

1.3. Transcendencia y aplicaciones.

Este trabajo, tiene varias aplicaciones de campo, tanto para la enseñanza universitaria como para mundo laboral (privado o público), como para la vida cotidiana:

- En el **ámbito universitario**, creo que es un tema que para la titulación que curso, Grado en Administración y Dirección de Empresas, debería de verse más a fondo.

  Solo lo hemos tratado en parte en una asignatura optativa, en Tecnología de la Información y las Comunicaciones, a mi criterio insuficiente para una carrera que pretende formar a futuros empresarios, pudiendo ayudar a los alumnos a llegar más preparados al mercado laboral ante una serie de riesgos que desconocen.

- En el **mundo laboral**, tener los conocimientos que se muestran en estos documentos, puede ayudar a evitar grandes pérdidas a las empresas, por poner un ejemplo: si un empleado de una empresa no tiene los conocimientos básicos de buenas prácticas en el uso de internet, puede usar su correo electrónico para intercambiar datos con cliente, como un número de cuenta, haciendo que alguien con los conocimientos necesarios y carácter malintencionado pueda perjudicar a cliente o empresa.

- Y, por último, en la **vida cotidiana**, igual que en el mundo laboral, nos ayudará a hacer un uso consciente y responsable de las tecnologías de la información y la comunicación, evitando los riesgos que conllevan las habituales malas prácticas.

2. La seguridad de la información y la seguridad informática

2.1. Definición de seguridad informática

La seguridad informática es un concepto integrado dentro de la seguridad de la información, es una parte clave de esta y se refiere a la protección de la información y de los sistemas de la información contra el acceso, uso, divulgación, interrupción o destrucción no autorizada.

Esta a su vez se divide en la protección de datos y en la protección de la información

- En la **Protección de la Información** el objetivo de la protección son los datos mismos y trata de evitar su pérdida y modificación no autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

- En el caso de la **Protección de Datos**, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

(Más información ver anexo 2)

La información es poder y se considera: ***Critica:*** Es indispensable para la operación de la empresa. ***Valiosa:*** Es un activo de la empresa y muy valioso. ***Sensitiva:*** Debe de ser conocida por las personas autorizadas.

2.2. La seguridad de la información

La seguridad de la información se centra en la preservación de las características de confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento dentro de una organización, independientemente de la forma que los datos pueden tener: electrónicos, impresos, audio, video….

- ***Confidencialidad***

  La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. El acceso está restringido sólo a aquellas personas, procesos o aplicaciones que estén autorizados. Es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

- ***Integridad***

  Preservar la integridad significa mantener la exactitud y completitud de la información. Los datos deben mantenerse libres de modificaciones no autorizadas.

  La violación de integridad se presenta cuando una persona, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes. Preservando la integridad se consigue que la información permanezca inalterada a menos que sea modificada por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

- ***Disponibilidad***

  Es la característica, cualidad o condición por la que la información debe encontrarse a disposición de quienes están autorizados para acceder a ella, ya sean personas, procesos o aplicaciones.

  Preservar la disponibilidad supone evitar/controlar interrupciones del servicio debido a cortes de energía, fallos de hardware, actualizaciones del sistema…

Adicionalmente se pueden considerar otras propiedades, como *autenticidad, no repudio, trazabilidad, confiabilidad...*

- ***Autenticidad***

  Hace referencia al aseguramiento de la identidad respecto al origen de la información. El objetivo que se pretende es la comprobación de que dichos datos o información provienen realmente de la fuente que dice ser.

  El problema del control de autenticidad, tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica digital.

  Proporciona seguridad en el caso de transacciones a través de la Red, y protege a los usuarios ante posibles ataques de suplantación de identidad y fraudes.

- ***No repudio***

  Hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación.

  El "no repudio" evita que el emisor o el receptor nieguen la transmisión de un mensaje. Prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

  La firma Electrónica aporta el efecto jurídico del "no repudio"

- ***Trazabilidad***

  Es la propiedad que permite conocer la historia y trayectoria de los datos. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

- ***Confiabilidad***

  Significa que la información debe ser obtenida de fuentes fiables.

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. El acceso está restringido sólo a aquellas personas, procesos o aplicaciones que estén autorizados. Es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

2.2.1. La información y su importancia

Como he mencionado antes, la protección de los equipos y redes informáticas, es una parte muy importante de la protección de la información de una empresa. Por lo que debemos hacernos las siguientes preguntas pregunta:

¿Qué tenemos que proteger en un sistema informático?:

Cuando hablamos de protección del sistema informático, no solo nos referimos, a evitar la entrada de virus, sino a la protección del sistema en si con medidas de seguridad preventivas, como establecer un manual interno de seguridad, la formación de los

empleados en el ámbito de la seguridad de la información, la instalación de los mejores sistemas de seguridad informática y de control de los mismos…

Lo que protegemos es la información de valor de la empresa y de los clientes (sean activos intangibles, patentes, información personal de los clientes…), por lo que estableceremos medidas de seguridad en todos los puntos de acceso a esta información, estableciendo un control al flujo de la misma.

¿Por qué nos tenemos que proteger? La respuesta, es bien sencilla:

La repercusión de los delitos informáticos, y de las malas prácticas en este tema dentro de la empresa causan millones de pérdidas al año, tanto en filtración de información relevante, como en estafas económicas, destrucción de datos, etc. Más adelante nos centraremos en ampliar este punto.

Mucha gente cree, que seguridad informática es tener actualizado el antivirus y poner una contraseña de seguridad para limitar el acceso y la verdad, para un *hackers* no tendría ningún problema en conseguir vulnerarlos.

En una empresa grande, con miles de empleados, la seguridad de los sistemas informáticos no puede limitarse única y exclusivamente a una barrera tan simple como es una contraseña, ya que no solo proteges un ordenador, sino todo su contenido que puede ser muy valioso para la empresa. Es decir, debemos proteger tanto el *hardware* como el *software.*

¿Cómo conseguimos proteger nuestros sistemas informáticos? Hay que tener en cuenta diversos factores:

- **Encargado de la seguridad informática:**

  ¿Quién se encarga de dirigir la seguridad informática de la empresa?
  En muchas empresas los encargados de la seguridad son los directivos, en otras el departamento informativo, en otras la empresa de seguridad ajena contratada… La situación no es quien se encargue de ella, sino que lo haga alguien, y que lo haga de una manera correcta, ya que el encargado va a ser el responsable de darles las herramientas y conocimientos necesarios a los empleados para realizar un uso seguro de los equipos.

- **Protección del sistema:**

  Lo principal para proteger los intereses de una empresa en el campo de la seguridad informática, es un buen sistema de seguridad. Esto no solo consiste en la instalación de un antivirus en cada ordenador.

  En primer lugar necesitamos una buena red de comunicaciones interna, y que sea segura a la hora de compartir información, es decir, obtener acceso desde cualquier lugar al correo electrónico o a los sitios Web internos de la compañía, a través de una red privada virtual (VPN).

  Instalación de los antivirus y cortafuegos correspondientes para la detección de software malicioso y de intrusos.

  Establecer un sistema de copias de seguridad al que vaya toda la información que maneja la empresa. Esto permite que la información no se pierda por cualquier fallo del ordenador o humano.

- **Protección de acceso a los equipos informáticos.**

  El peligro no solo viene vía Web, sino que también puede ser ocasionado por un intruso físico. Para ello la empresa debe de contar con algún equipo de seguridad que proteja los equipos, tanto personal de seguridad que vigile las instalaciones como contar con un sistema de filtración de usuarios.

  Contar con un sistema de vigilancia de cámaras de seguridad, y con otro de control de historial de movimientos.

  Las personas que accedan a los equipos deben de estar autorizadas mediante algún tipo de identificación física o digital (identificación por tarjeta, condigo, huella dactilar, etc.) en la entrada del recinto al encardado de la seguridad, y si no es posible por el tipo de oficina que posee la empresa, con una identificación

virtual a la hora de acceder a los equipos, mediante cuentas de usuario individuales.

- **Concienciación del personal.**

  La mejor manera a veces de evitar un fallo de seguridad en el sistema, puede ser la puesta en marcha de mecanismos de concienciación de los empleados.

  Muchas veces, dentro de las oficinas los empleados tienden a tener malas costumbres con respecto a la seguridad de sus equipos informáticos, por el simple hecho de dejarse llevar por la dejadez sobre un tema que muchos desconocen en gran medida, además de no darle la importancia como para esforzarse en realizar las buenas prácticas que conducen a la protección de los equipos de la empresa y de los datos de los mismos.

  Las malas prácticas están a la orden del día en las oficinas, con frecuencia se comparten contraseñas de acceso, o se anotan en un lugar cerca del equipo para no olvidarla, además suelen ser simples y usadas para diversos programas y equipos. En muchas ocasiones no se realizan las convenientes actualizaciones del sistema y del antivirus. Los empleados navegan y descargan datos en páginas de riesgo, o abren correos electrónicos inesperados de remitente desconocido.

  Para evitar este tipo de problemas, las empresas deben de tener una política de concienciación sobre la seguridad informática y que llegue a cada uno de los empleados estableciendo unas pautas para las buenas prácticas de navegación y uso de los sistemas informáticos que permita mantener la seguridad de los datos desde dentro de la empresa.

  La empresa, comentado anteriormente, debe gestionar todos sus datos mediante un sistema interno de copia de seguridad que puedan usas los trabajadores e imponerles la obligatoriedad de usarlo. Y no solo esto, sino además deben instaurar un *Plan de Contingencia* ó de *Recuperación de Negocio*, que permita

seguir con las actividades de la empresa ante cualquier "catástrofe" en la que pueda verse afectada.

2.3. Análisis y gestión de riesgos

Para iniciar este apartado, debemos de tener claros una serie de conceptos que se explican a continuación:

- **Análisis de riesgos**: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización, es decir, proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo que significa la prevención de este suceso. Se recomendaran acciones en base al costo-beneficio de las mismas.

- **Gestión de riesgos**: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Partimos de unos **activos**, que están expuestas a un riesgo (probabilidad de que una determinada **amenaza**, explotando la **vulnerabilidad** de un activo o grupo de activos pueda ocasionar la pérdida de los mismos, es decir un **impacto**).

- **Activos**: Software, hardware, información, servicios, documentación y personas.

- **Amenazas**: Una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Se presentan de forma compleja y, en muchos casos, son difíciles de predecir. Ejemplos: Catástrofes naturales, accidentes, ataques malintencionados, aplicaciones mal diseñadas…

- **Vulnerabilidad**: La situación creada por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático. Debilidad en la seguridad de la información de una organización que potencialmente

permite que una amenaza afecte a un activo.Ejemplos: Falta de control de acceso lógico, falta de formación, deficiente política de contraseñas…

- **Exposición o impacto**: Efecto del riesgo. daño sobre el activo derivado de la materialización de la amenaza. El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros. Ejemplos: Pérdidas directas (económicas, vidas humanas…), incumplimiento de leyes (LOPD), interrupción de los servicios, pérdida de prestigio (imagen), etc.

2.3.1. ¿Qué podemos hacer ante los riesgos?

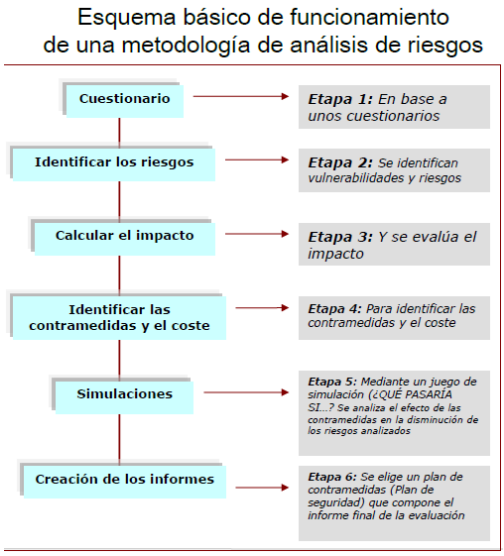
- **Evitarlos**: Analizar los posibles riesgos que pueden a afectar a nuestro negocio y anticiparnos a ellos para esquivarlos o protegernos ante ellos. (No construir un centro donde hay peligro constante de inundaciones)
- **Transferirlos**: Uso de un Centro de Cálculo contratado. (Seguro)
- **Reducirlos**: Establecer métodos que permitan minimizar o incluso acabar con el riesgo cuando un problema tiene lugar. (Sistema de detección y extinción de incendios)
- **Asumirlos**: Estar preparado y tener los medios necesarios para permitir que el negocio siga adelante después de un problema. (Lo que se hace si no se controla el riesgo en absoluto)

Establecer controles o contramedidas que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo más baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

2.3.2. ¿Qué obtenemos de un análisis de riesgos?

Información, para la determinación de los recursos sensibles de la organización, sobre las amenazas del sistema y vulnerabilidades, además de la identificación de posibles

pérdidas (€ y otras no cuantificables), la probabilidad de que las haya y identificación de contramedidas efectivas y herramientas de seguridad para evitar estas amenazas.



2.4. Algunas medidas organizativas y técnicas para garantizar la seguridad.

Según la Ley Orgánica de protección de Datos, estas son las medidas de seguridad que una empresa debe implantar en su Sistema de Gestión de la Seguridad de la Información para preservar las siguientes características:

- **Confidencialidad**: entendido como el acceso autorizado a los datos.
- **Exactitud**: la información no debe sufrir alteraciones no deseadas, en cuanto a su contenido.
- **Disponibilidad**: sólo las personas autorizadas pueden tener acceso a la información.

Las medidas de seguridad son las siguientes:

Documento de Seguridad. Identificación y Autenticación:

1) Existencia de una lista actualizada de usuarios autorizados que tengan acceso autorizado al sistema de información (art.11.1 y 12.3).
2) Procedimientos de identificación y autenticación informáticos:
   a) Contraseñas: procedimiento de creación, asignación, conservación y cambio periódico (art.11.2 y 11.3).

b) Identificación de usuario, de manera inequívoca y personalizada (art.18.1).
c) Limitación de acceso incorrecto reiterado (art.18.2).

Control de Acceso:

1) Los usuarios tendrán únicamente acceso a los datos/recursos de acuerdo a su puesto laboral y tareas definidas en el documento (art.12.1).
2) Deberán implantarse mecanismos que eviten el acceso no autorizado a otros recursos: establecimiento de perfiles de usuario (art.12.2).
3) Control de acceso físico a servidores y CPD (art.19).
4) De cada acceso se guardarán: identificación usuario, fecha y hora, fichero accedido, tipo de acceso y su autorización o denegación, guardando la información que permita identificar registro accedido (art.24.2).
5) Los mecanismos de acceso estarán bajo el control directo del Responsable de Seguridad, sin que pueda permitirse la desactivación (art.24.3).
6) Registro y conservación de accesos lógicos al fichero por un plazo no inferior a 2 años (art.24.4)
7) Para accesos a través de redes de telecomunicaciones, deberán tener las mismas medidas que para accesos en modo local (art.5).

Funciones y obligaciones del personal:

1) Definición en el Documento de Seguridad de las funciones y obligaciones de grupos de usuarios y/o perfiles (art.9.1).
2) Conocimiento por parte del personal de las normas y medidas de seguridad que les son aplicables (art.9.2).
3) Identificación y funciones del/los Responsables de Seguridad (art.15 y 16).
4) Trabajo fuera de ubicación principal debe ser expresamente autorizado (art.6).
5) Listado de personal con acceso a Servidores y/o CPD (art.19).
6) Listado de personal con privilegios administrativos informáticos sobre aplicaciones y ficheros (art.12.4).

Estructura de los Ficheros y del Sistema Informático:

1) Descripción y estructura informática del Fichero (campos ID)

2) Descripción y estructura del Sistema Informático (enumeración de equipos, redes, programas, etc...)

Gestión de Soportes:

1) Identificación, inventariado y almacenamiento (art.13.1).
2) Autorización necesaria para salida de soportes (art.13.2).
3) Cifrado de soportes en caso de operaciones externas de mantenimiento (art.20.4).
4) Medidas y procedimientos para la destrucción de soportes (art.20.3).
5) Registro de Entrada de Soportes (art.20.1).
6) Registro de Salida de Soportes (art.20.2).
7) Distribución de soportes con mecanismos de cifrado de datos (art.26).

Registro de Incidencias:

1) Contenido mínimo: tipo de incidencia, momento en que se produce, efectos producidos, persona que comunica, medidas adoptadas (art.10).
2) Contenido adicional: Procedimiento de restauración de datos, datos restaurados y datos grabados manualmente (art.21.1).

Procedimientos de Copias de Respaldo y Recuperación datos:

1) Deberán garantizar la restauración de los datos al momento anterior a producirse la pérdida (art.14.2).
2) Realización de copias de backup al menos con una frecuencia semanal (art.14.3).
3) Necesaria autorización para la ejecución de procedimientos de restauración de datos (art.21.2).
4) Almacenamiento externo de copias y procedimientos de restauración de datos (art.25).

Actualización y Auditoria:

1) Revisión y actualización del Documento de Seguridad en función de cambios relevantes en la Organización (art.8.3).
2) Auditoria cada 2 años. Conservación de Informe a disposición AEPD (art.17).

3) Revisión periódica de la información de control de los accesos informáticos a ficheros y aplicaciones (art.24.5).

Medidas específicas para datos en soporte papel:

1) Control de acceso a la documentación.
2) Medidas de conservación y almacenamiento.
3) Procedimientos y mecanismos de destrucción que impidan posterior recuperación de la información que contienen.

3. Marco legal y normativo en materia de seguridad informática

En este apartado describimos diferentes normas, estándares y certificaciones en materia de seguridad informática; en primer lugar, la norma **ISO 270001**, norma certificable que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI); también describiremos el **Esquema Nacional de Seguridad** (ENS), que especifica las medidas a implantar para garantizar la seguridad en las operaciones electrónicas con la Administración Pública; finalmente, nombraremos algunos otros referentes en materia de seguridad y, por último, nos referiremos a los organismos de certificación en España, **AENOR y BSI**.

3.1. Norma ISO 27001

ISO - International Organization for Standardization: Es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en los distintos países (público, privado…).

ISO desarrolla estándares requeridos por el mercado que representen un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios, consumidores…) acerca de productos, tecnologías, métodos de gestión, etc. Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

ISO garantiza un marco de amplia aceptación mundial a través de los 3000 grupos técnicos y 50.000 expertos que colaboran en el desarrollo de normas.

La norma ISO 27001, es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (Plan-Do-Check-Act; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.). El

establecido en 2005, es el único estándar aceptado internacionalmente para la administración de la seguridad de la información.

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

Con estándar nos referimos a publicación que recoge el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

Su objetivo es ayudar a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores, vendedores, compradores, usuarios y reguladores). En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos.

(Estructura ISO 27001 véase anexo 3)

3.1.1. Sistemas de Gestión de Seguridad Informática. (SGSI)

¿Qué es?

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001 (explicado más adelante).

Consiste en un sistema que establece e implanta unos procesos de gestión que permiten a una organización realizar un producto/servicio conforme a unas especificaciones dadas. Mide y evalúa los resultados obtenidos frente a los objetivos marcados. Incorpora un proceso de revisión para asegurar que los problemas que pueden surgir se detectan y se corrigen, y que permite identificar oportunidades de mejora. Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

¿Para qué sirve?

Aseguran que una organización sea dirigida de un modo eficiente y eficaz. Formalizan y sistematizan la gestión en procedimientos escritos, instrucciones, formularios y registros que aseguren la eficiencia de la organización y su mejora continua.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un SGSI es **garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados** por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

El diseño e implantación de un SGSI depende de las necesidades concretas, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización.

El SGSI **protege los activos de información de una organización**, independientemente del soporte que se encuentren; por ej., correos electrónicos, informes, escritos relevantes, páginas web, imágenes, documentos, hojas de cálculo, faxes, presentaciones, contratos, registros de clientes, información confidencial de trabajadores y colaboradores...

Un SGSI implica que la organización ha estudiado los riesgos a los que está sometida toda su información, ha evaluado qué nivel de riesgo asume, ha implantado controles (no sólo tecnológicos, sino también organizativos) para aquellos riesgos que superan dicho nivel, ha documentado las políticas y procedimientos relacionados y ha entrado en un proceso continuo de revisión y mejora de todo el sistema.

El SGSI da así la garantía a la organización de que los riesgos que afectan a su información son conocidos y gestionados. No se debe olvidar, por tanto, que no hay seguridad total sino seguridad gestionada.

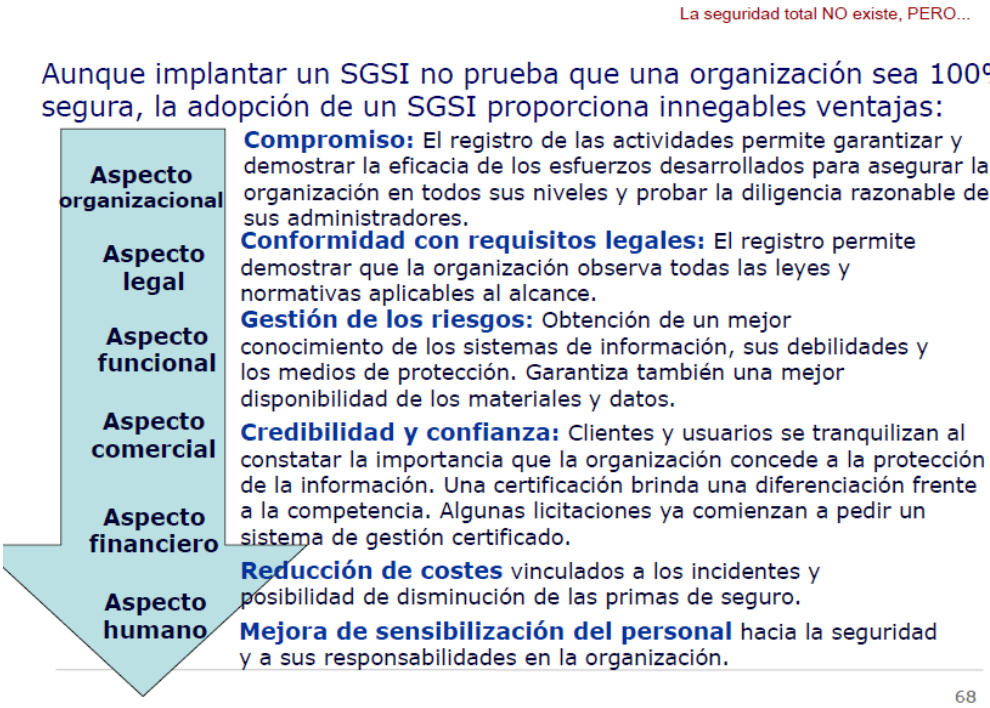
La seguridad no es un producto, es un proceso. No existe un producto comercial que cubra todos los aspectos de seguridad de la información.

La seguridad exige de un plan de gestión del riesgo continuado, políticas adecuadas a cada empresa y una seguridad establecida en base a múltiples y diferentes barreras. Siempre hay que recordar que: "La seguridad no es un producto sino un proceso".

Lo que SGSI aporta a la empresa, una minimización de los riesgos, asegura la continuidad adecuada de las actividades de negocio hasta en los casos más extremos, adapta la seguridad a los cambios continuos que se producen en la organización y en su entorno y nos acerca a la seguridad total (aunque nunca lleguemos a ella) mediante una mejora continua.

Es más apropiado hablar en términos de riesgo asumible en lugar de seguridad total.

El gasto en seguridad no será mayor que los impactos potenciales de los riesgos que pretende evitar.



SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.

En el contexto aquí tratado, se entiende por **Información** todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo,

fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

Adicionalmente, preservar también autenticidad, responsabilidad, no repudio, y confiabilidad.

¿Por qué es tan importante tener un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero

también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

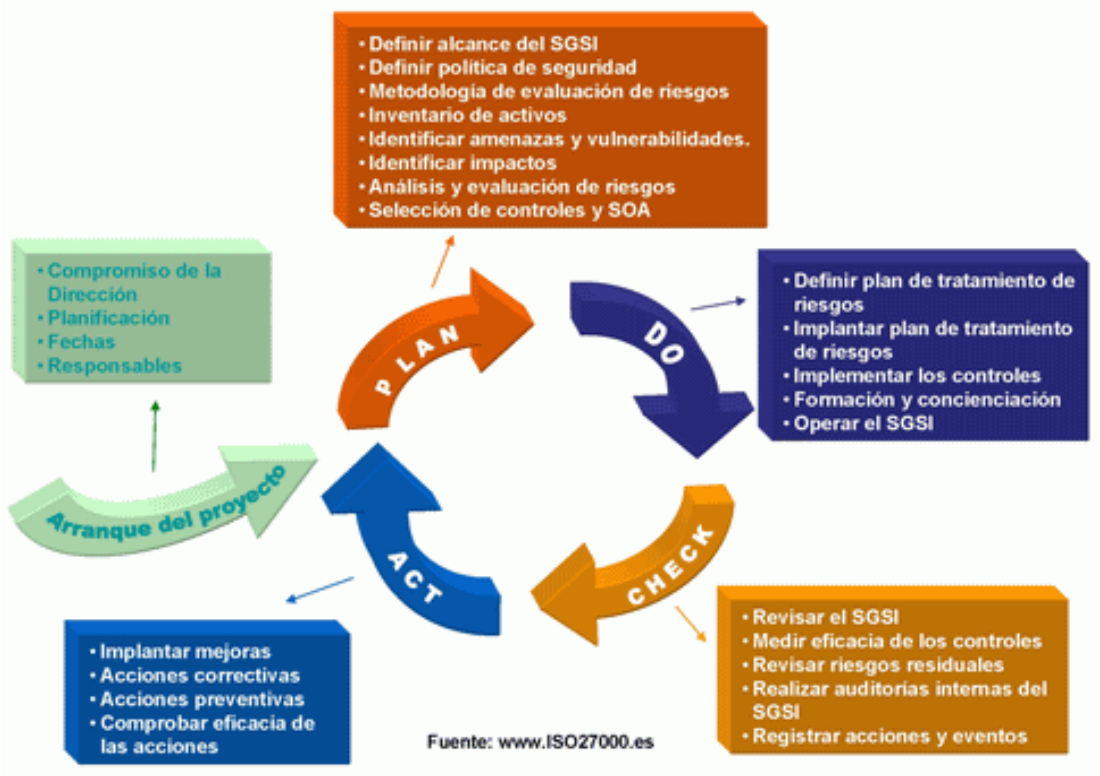
El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

(Estructura y documentación de SGSI según ISO27001 véase anexo 4)

¿Cómo establecemos un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo **PDCA**, tradicional en los sistemas de gestión de la calidad.



El modelo sigue una serie de etapas en las que cada una se realizan diversas funciones que conducen a la siguiente etapa. Esto hace que se genere un ciclo continuo que permite a la empresa establecer un modelo de calidad, en este caso respecto a la seguridad de la información.

Las etapas son las siguientes:

PLAN = Establecer con planificación

Establecer las actividades del proceso, necesarias para obtener el resultado esperado. Al basar las acciones para el resultado esperado, la exactitud y cumplimiento de las especificaciones a lograr se convierten también en un elemento a mejorar, aunque sería mejor ya no tener que mejorar, o sea, hacerlo bien a la primera. Cuando sea posible conviene realizar pruebas según sea requerido, para probar los resultados.

- Recopilar datos para profundizar en el conocimiento del proceso.
- Detallar las especificaciones de los resultados esperados
- Definir las actividades necesarias para lograr el producto o servicio, verificando los requisitos especificados

DO = Implementar y utilizar el SGSI

Es ejecutar el plan estratégico lo que contempla: organizar, dirigir, asignar recursos y supervisar la ejecución.

CHECK = Monitorizar y Revisar

Pasado un periodo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los requisitos especificados inicialmente, para saber si se han cumplido y en su caso, evaluar si se ha producido la mejora.

Monitorear la implementación y evaluar el plan de ejecución documentando las conclusiones.

ACT = Mantener y Mejorar

Con base a las conclusiones del paso anterior elegir una opción:

- Si se han detectado errores parciales en el paso anterior, realizar un nuevo ciclo PDCA con nuevas mejoras.
- Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos
- Si se han detectado errores insalvables, abandonar las modificaciones de los procesos

- Ofrecer una Retro-alimentación y/o mejora en la Planificación.

(Véase anexo 5, para una explicación más detallada del PDCA)

3.2. Esquema Nacional de Seguridad (ENS)

3.2.1. ¿En qué consiste y que misión tiene?

El Real Decreto 3/2010, de 8 de enero, BOE de 29 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, previsto en el artículo 42 de la Ley 11/2007 (LAECSP).

Establece la política de seguridad en la utilización de medios electrónicos por las Administraciones Públicas.

Está constituido por unos principios básicos y unos requisitos mínimos que obligan a definir unas medidas de seguridad para asegurar una protección adecuada de la información.

El Esquema se centra en la aplicación de un conjunto de MEDIDAS DE SEGURIDAD (75 controles en total) decididas en base a un Análisis de Riesgos sobre los activos y Sistemas de información relacionados con la Administración Electrónica.

Se hace una categorización de los niveles de seguridad según las dimensiones de seguridad de cada uno de los sistemas de información que forman parte del alcance. Los niveles BÁSICO, MEDIO y ALTO recuerdan mucho al Reglamento de Medidas de seguridad de la LOPD pero a diferencia de la legislación sobre protección de datos personales, éstos se calculan aquí según el impacto en la organización (estilo ISO 27001).

El Real Decreto también legisla sobre la Auditoría del propio Esquema, uniendo en estos aspectos la posibilidad de realizar un enfoque práctico y global junto con la normativa de protección de datos personales e incluso con la certificación de un SGSI sobre ISO 27001.

Todos los órganos superiores de la Administraciones Públicas deberán disponer de su política de seguridad que garantice el acceso, integridad, disponibilidad, autenticidad,

confidencialidad, trazabilidad, conservación y no repudio (explicados anteriormente en este documento) de los datos, informaciones y servicios utilizados en medios electrónicos.

Se entiende por seguridad de las redes y de la información 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 trasmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

(Para más información sobre el ENS, como elementos básicos, estructura y categorías de los sistemas véase Anexo 6)

3.3. Otras normas y referencias nacionales e internacionales

A continuación veremos algunos ejemplo de certificaciones en seguridad de la información menos conocidas, las individuales, es decir, aquellas certificaciones a las cuales los profesionales acuden para tener una "marca" de calidad y demostrar sus conocimientos y dominios en el campo de la seguridad de la información.

Estas certificaciones son usadas por las empresas para buscar trabajadores que tienen los conocimientos necesarios para ayudarles a mejorar en el campo de la seguridad de la información y de la seguridad informática.

CISSP (Certified Information Systems Security Professional)

Es una certificación de alto nivel profesional otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc), con el objetivo de ayudar a las empresas a **reconocer a los profesionales con formación en el área de seguridad de la información.**

Certified Information Systems Auditor (CISA)

Certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA) (Information Systems Audit and Control Association). Los candidatos deben cumplir con los requisitos establecidos por la ISACA.

CISM (Certified Information Security Management)

Certificación para administradores de seguridad de la información respaldada por la ISACA (Information Systems Audit and Control Association). Está enfocada en la gerencia y ha sido obtenida por siete mil personas desde su introducción, en 2004. A diferencia de otras certificaciones de seguridad, CISM define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

Criterios de Evaluación de Seguridad en Tecnologías de la Información (CESTI)

Conjunto de criterios para evaluar la seguridad informática de productos y sistemas.

El producto o sistema sometido a evaluación, denominado objetivo de evaluación (OE) es sometido a un examen detallado de sus características de seguridad, que culmina con extensas pruebas de funcionamiento y tests de penetración. El grado de examen depende del nivel de confianza deseado para el OE. Para proporcionar diferentes grados de confianza, los CESTI definen los llamados niveles de evaluación, desde E0 a E6. Los niveles más altos de evaluación exigen exámenes y tests más detallados del OE.

ITIL

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes

del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

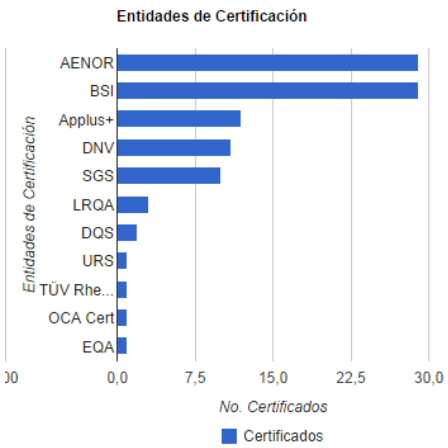
COBIT

Objetivos de Control para la Información y Tecnología Relacionada (COBIT) es un marco creado por ISACA para tecnología de la información (IT) de gestión y gobierno de TI . Es un conjunto de herramientas de soporte que permite administradores para cerrar la brecha entre las necesidades de control, cuestiones técnicas y riesgos de negocio.

COBIT tiene como objetivo "investigar, desarrollar, publicar y promover un, conjunto autorizado, hasta al día internacional de aceptación general de control de tecnología de la información objetivos para el uso del día a día a los gerentes de empresas, profesionales de TI y profesionales de aseguramiento".

3.4. Empresas principales de certificación en España

Hay varias entidades encargadas de gestionar las certificaciones en España pero nos vamos a centrar en dos: AENOR y BSI. Son las de más relevancia y las que más certificaciones llevan al año en el territorio español. En 2013 realizaron 29 cada una como se puede apreciar en la gráfica:



AENOR

La Asociación Española de Normalización y Certificación (AENOR) es una entidad española de normalización y certificación en todos los sectores industriales y de

servicios. AENOR abarca mucho mas pero en este apartado nos vamos a centrar en el ámbito de la seguridad de la información e informativa.

En su vertiente de normalización, tiene encomendada esta tarea por la Administración española y es el representante de España en ISO. En su vertiente de certificación, opera en el mercado como cualquier otra entidad privada de certificación y no tiene concedida ninguna exclusividad.

En materia de seguridad AENOR tiene como misión:

- Garantizar la protección eficaz de la información empresarial.
- Garantizar la seguridad de los sistemas de información y de los procesos informáticos se está convirtiendo en uno de los principales objetivos de cualquier organización. Los virus, los ataques de intrusión, los fraudes informáticos, la falta de protección o cualquier otro riesgo no controlado pueden ocasionar pérdidas importantes y repercutir directamente en la calidad del servicio.

La certificación concedida por AENOR permite a las compañías calcular y analizar sus riesgos identificando amenazas y por lo tanto prevenir, eliminar o reducir eficazmente el riesgo mediante la implantación de los controles adecuados.

La certificación del Sistema de Gestión de Seguridad de la Información de AENOR, de acuerdo a UNE-ISO/IEC 27001, contribuye a fomentar las actividades de protección de la información en las organizaciones, mejorando su imagen y generando confianza frente a terceros.

Por otra parte, el interés de las empresas españolas por esta certificación ha hecho que entremos en el top ten mundial por el número de certificados de SGSI, y que AENOR sea el líder en esta certificación.

Este esquema de certificación es aplicable a cualquier tipo de organización independientemente del sector en el que actúe.

El Sistema de Gestión de la Seguridad de la Información integra el ciclo de mejora continua PDCA, compartiéndolo con el resto de Sistemas de Gestión ISO. Esto posibilita la integración del SGSI con cualquier otro sistema de gestión.

Una vez superado el proceso de Auditoría, si el sistema implantado se adecúa a los requisitos de la norma UNE-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI) la empresa obtiene:

- El Certificado AENOR de Sistemas de Gestión de Seguridad de la Información.
- La licencia de uso de la marca Seguridad de la Información, de AENOR.
- El Certificado IQNet, pasaporte para un acceso internacional de su certificación. Con él, su certificado AENOR quedará reconocido por las entidades de certificación líderes en el ámbito internacional.
- La licencia de uso de la marca IQNet.

Más de 300 es el número de certificados de SGSI emitidos por AENOR. Entre las organizaciones certificadas hay administraciones públicas y múltiples organizaciones de todo tipo de sectores de actividad (sanitario, tecnológico, telecomunicaciones, seguros, banca, servicios, bufetes de abogados, constructoras, transportes, etc.)

Logo de la certificación ISO 27001:

BSI

La British Standards Institution, cuyas siglas corresponden a **BSI**, es una multinacional cuyo fin se basa en la creación de normas para la estandarización de procesos. BSI es un organismo colaborador de ISO y proveedor de estas normas, son destacables la ISO 9001, ISO 14001 e ISO 27001. Entre sus actividades principales se incluyen la certificación, auditoría y formación en las normas.

BSI fue fundada por el Comité de Ingeniería de normas de Londres en 1901. Poco a poco extendió su actividad de normalización a otros ámbitos y adoptó el nombre de British Standards Institution, tras recibir la aprobación por Royal Charter en 1929. En 1998, tras una revisión del Royal Charter, BSI comenzó a diversificarse. De este modo se estableció su nombre comercial haciendo referencia a su presencia Internacional: BSI Group.

Actividades de BSI

Actualmente BSI tiene presencia en Asia, Europa y América. La organización lleva en España desde 1998 y ha centrado sus actividades en:

1. **Auditoría**
2. **Certificación**
3. **Formación**

1- Las **auditorías** proporcionadas desde BSI España se dividen en:

- Auditorías de segunda parte:

  Se trata de auditorías realizadas en nombre de un cliente determinado que solicita los servicios de BSI, bien porque tenga esa necesidad ya que la propia organización solicitante no pueda proporcionarla por si misma o bien porque necesiten una tercera parte neutral y experta que medie entre la organización solicitante y sus proveedores.

- Auditorias de tercera parte

  Se trata de las auditorías que BSI realiza de manera independiente. BSI España dispone de un equipo de auditores repartidos por toda la geografía española que basan su labor diaria en el concepto de "Auditoría constructiva".

2- BSI España **certifica** en las siguientes normas:

Desempeño:

- Calidad ISO 9001
- Servicio de Gestión TI ISO/IEC 20000
- Automoción ISO/TS 16949
- Aeroespacial AS9100
- Telecomunicaciones TL 9000
- Gas & Petróleo ISO 29001
- Satisfacción de cliente ISO 10002

Sostenibilidad:

- Medio Ambiente ISO 14001
- Verificación de Memorias de Sostenibilidad GRI / AA 1000 AS
- Verificación de la Huella de Carbono PAS 2050
- Responsabilidad Social SA 8000
- Desarrollo sostenible BS 8900

Riesgo:

- Seguridad Laboral OHSAS 18001
- **Seguridad de la Información ISO/IEC 27001**
- Continuidad de Negocio BS 25999
- Seguridad Alimentaria ISO 22000

presas.

en el mercado. Así, respondiendo a este criterio existen cursos para las siguientes normas:

- Calidad: ISO 9001:2008
- Medio Ambiente: ISO 14001
- Continuidad de Negocio: BS 25999
- Seguridad y Salud Laboral: OHSAS 18001
- **Seguridad de la Información: ISO 27001: 2005**
- Tecnologías de la Información: ISO/IEC 20000:2005
- Sistemas de Gestión integrados: PAS 99
- Automoción: ISO/TS 16949:2002
- Seguridad Alimentaria: ISO 22000

Existen tres tipos de cursos para cada norma:

- **Cursos de Introducción**

  En ellos los alumnos no necesitan tener ningún conocimiento previo de la norma.
- **Cursos de Implantación**

  En los que es aconsejable un conocimiento previo de la norma.
- **Cursos de Auditor Interno**
- **Cursos de Auditor Jefe**

Los cursos se imparten en centros formativos situados en los centros de formación de BSI en Madrid, Barcelona, Valencia, Bilbao y Marbella. (También existe la modalidad de formación in-company).

Logo certificación ISO 27001:

4. Caso Práctico: Banco “Seguro”

A continuación voy a aplicar lo estudiado hasta ahora a un ejemplo práctico. Voy a usar una empresa real, el “Banco Seguro” (le he cambiado el nombre con la intención de “anonimizarlo”, así como de todas las menciones relacionadas que este banco en el resto del documento), para mostrar la política de seguridad de la información e informática de una entidad financiera.

En este apartado veremos la política de seguridad del “Banco Seguro”, en un ámbito global, desde la protección de sus oficinas y entidades, hasta los sistemas de seguridad informáticos y de protección de la información.

Analizaremos porque no tiene la certificación ISO 27001, explicaremos el porqué, y daremos los pasos necesarios para que la obtenga.

4.1. Política de seguridad del Banco Seguro.

He optado por estudiar este tipo de empresa porque en su entorno laboral se maneja información, tanto de clientes como de la propia entidad, que es de gran valor tanto para el propietario de la misma, como para gente ajena a ella que se puede beneficiar de ella.

En concreto he optado por el Banco Seguro porque es mi entidad bancaria permitiéndome obtener información de primera mano.

Para comenzar vamos a analizar las **medidas de seguridad que son comunes** en todos los bancos y las **medidas de seguridad informática y de la información** que tiene el **Banco Seguro**.

4.1.1. Medidas de Seguridad obligatorias

Para empezar vamos a repasar las medidas de seguridad obligatorias en bancos, cajas y entidades de crédito y por tanto, también en el “Seguro”, en lo que se refiera a la **protección de los activos físicos** (dinero, divisas y demás material de valor que guarden en sus sucursales), ya que no todo lo que se protege es información.

El apartado tercero de la Orden Ministerial de 23 de abril de 1997, por la que se concretan determinados aspectos en materia de medidas de seguridad, establece las medidas de seguridad específicas en entidades de crédito, disponiendo que:

1. "En los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instaladas con carácter obligatorio las medidas de seguridad especificadas en los apartados b), c) y f) del artículo 120.1 y en el artículo 122.1 del Reglamento de Seguridad Privada".

   Por tanto, todos los bancos, cajas de ahorro y entidades de crédito, cualquiera que sea la población de la localidad donde se ubiquen, deberán contar obligatoriamente con las siguientes medidas de seguridad:

   - Dispositivos electrónicos con capacidad para detectar el ataque a cualquier elemento de seguridad física donde se custodien efectivos o valores. (Art. 120.1.b).
   - Pulsadores u otros medios de accionamiento fácil de las señales de alarma. (Art. 120.1.c)
   - Carteles u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad, con referencia expresa al sistema de apertura automática retardada y, en su caso, al sistema permanente de captación de imágenes. (Art. 120.1.f)
   - Caja fuerte protegida con los dispositivos de bloqueo y apertura automática retardada, Cuando su peso sea inferior a 2000 kilos, estarán, además, ancladas, de manera fija, en estructuras de hormigón armado, al suelo o al muro. (Art.122.1).

2. Además de tales medidas de seguridad, los citados establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, en los que concurran las circunstancias del número 3 de este apartado tercero (poblaciones con 10.000 habitantes o más y el número de robos con intimidación "conocido", producidos en las entidades de crédito existentes en dichas localidades, en los dos años naturales anteriores a la fecha de entrada en vigor de esta Orden, según la estadística elaborada por la Secretaría de Estado de Seguridad) deberán contar con una de las tres que se citan a continuación:

- El recinto de caja a que se refiere el artículo 120.1.d) del Reglamento de Seguridad Privada, con el nivel de blindaje que se determina en el apartado sexto de esta 'Orden. Se entiende por recinto de caja el destinado a disponer de las cajas auxiliares en su interior.
- El control de accesos previsto en el artículo 120.1.e) del Reglamento de Seguridad Privada, con el nivel de blindaje que se determina en el apartado sexto de la presente Orden.
- Dispensadores de efectivo adecuados a lo dispuesto en el artículo 122.3 del citado Reglamento y en el apartado decimotercero de esta Orden, cuando su instalación sustituya a todas las cajas auxiliares. De mantenerse alguna caja auxiliar, será preciso que ésta se encuentre dentro del recinto de caja.

3. En todo caso, deberán contar con una de las tres medidas indicadas, y con la regulada en el artículo 120.1.a), del Reglamento de Seguridad Privada, las oficinas que no estando afectadas por lo dispuesto en el artículo 120.2, párrafo primero, de dicho Reglamento (localidades con población inferior a 10.000 habitantes y no cuenten con más de 10 empleados), se ubiquen en:

   - Capitales de provincia.
   - Localidades de provincias, cuyo número de robos con intimidación en entidades de crédito, supere la media de 100, en los dos años a que se refiere el número 3 de este apartado cuarto, las cuales se relacionan en el Anexo número 1.
   - Localidades con una población superior a los 50.000 habitantes y que se relacionan en el Anexo número 2.

De todo lo que antecede, puede concluirse que las medidas de seguridad que la normativa de seguridad privada exige, en general, para los Bancos, Cajas de Ahorro y demás Entidades de Crédito son:

- Equipos o sistemas de captación y registro de imágenes.
- Dispositivos electrónicos capaces de detectar cualquier ataque a los elementos de seguridad física.
- Pulsadores de accionamiento de señales de alarma. Recinto de caja.

- Control individualizado de accesos.
- Dispensadores de efectivo.
- Carteles anunciadores de las medidas de seguridad.
- Caja Fuerte.
- Conexión a Central de Alarmas.

Las características de estas medidas de seguridad, tal y como se expone en los párrafos anteriores, se encuentran recogidas en el Capítulo II del Reglamento de Seguridad Privada, concretamente en los artículos 119, 120 y 122 y en la Orden Ministerial de 23 de abril de 1997 por la que se concretan determinados aspectos en materia de medidas de seguridad, apartado tercero de su Capítulo II. De las medidas de seguridad enumeradas, **son exigibles a todos** los Bancos, Cajas de Ahorros y Entidades de Crédito las siguientes:

- Dispositivos electrónicos capaces de detectar cualquier ataque a los elementos de seguridad física.
- Pulsadores de accionamiento de señales de alarma. Carteles anunciadores de las medidas de seguridad.
- Caja Fuerte.
- Conexión a Central de Alarmas.

4.1.2. Medidas de Seguridad de la Información

En este apartado, voy a explicar las medidas de seguridad aplicadas en el Banco Seguro para proteger la información de sus clientes y de la propia entidad bancaria.

Esta información ha sido obtenida de la propia página web del banco, así como de una investigación de campo entrevistando a personal del “Seguro”, que han facilitado información sobre tipo de formación recibida para proporcionar el mejor servicio y salvaguardar la información de los clientes y del mismo banco.

Para los clientes. BSOnline

En la Banco Seguro, como la gran mayoría de las entidades financieras, proporciona gran parte de sus servicio vía web, por lo que dispone de un servicio de Banca Online con un gran número de sistemas de seguridad.

Este sistema permite a sus clientes, tanto empresas como particulares, realizar la mayoría de las gestiones que necesiten, mediante cualquier dispositivo móvil, tablet ú ordenador.

El sistema de Banca Online del "Seguro", cuanta con el cumplimiento de todas las leyes pertinentes para la protección de los intereses del consumidor, así como con la ley de la protección de datos incorporando la tecnología de seguridad más actualizada hasta el momento, así como medidas complementarias:

Protocolo SSL EV de cifrado 128 bits. "*Servidor seguro"*

Esta tecnología permite que los datos introducidos en pantalla y que viajan a través de la red estén cifrados mediante un algoritmo, con claves variables en cada conexión. Estas claves son realmente el elemento esencial de lo que constituye la seguridad de un "servidor seguro".

Cifrado de los mensajes

Seguro está dentro en un "servidor seguro" y tiene incorporadas estas claves de 128 bits utilizando la última versión de certificados disponible, denominados certificados de validación extendida o **certificados SSL EV**. Dichos certificados incorporan mecanismos adicionales de seguridad que incorporan tecnologías de prevención del fraude, informando sobre el nivel de seguridad de la página visitada. Las últimas versiones de los navegadores, como por ejemplo Internet Explorer en su versión 7 o superior, o Firefox a partir de la versión 3, soportan estos tipos de certificados, indicando la autenticidad de la página web visitada, sombreando la barra de direcciones en color verde.

Adicionalmente, junto a la figura del candado de seguridad, se muestra información de la Sociedad Jurídica propietaria de la página web accedida (en nuestro caso Banco de Seguro). Pulsando sobre esta área se pueden obtener detalles adicionales acerca del certificado utilizado.

(Si por el contrario la barra de direcciones aparece sombreada en color rojo, desconfíe de dicha página, ya que ésta podría ser fraudulenta; y si utiliza versiones de navegadores que no soporten dichas funcionalidades, la barra de direcciones no aparecerá sombreada.)

El código de acceso

El código de acceso el cliente introduce en Banco Seguro, ha de superar una serie de controles: un número máximo de equivocaciones por día, o acumulado de varios días, provocará que el código de acceso se cancele automáticamente. En ese caso, para reactivarla, el usuario tendría que solicitarlo por escrito o bien personalmente en su agencia de Banco Seguro.

Aquellas operaciones que precisan mayor seguridad (transferencias, órdenes de bolsa, etc.) solicitan una **segunda clave**. Esta segunda clave corresponde a una de las que constan en la tarjeta de claves de BS Online. Esta **tarjeta de claves** es distinta y personalizada para cada cliente. Cada operación de este tipo le solicita una clave distinta de forma aleatoria. La tarjeta de claves es un elemento absolutamente importante de la seguridad, la propia entidad bancaria aconseja a sus clientes conservarla siempre en su poder y comunicar inmediatamente su pérdida o extravío al servicio del banco.

En el momento de su conexión a BS Online, se indica el **día y hora de la anterior conexión**, para que el cliente pueda verifique que realmente fue así. Esta facilidad le permite comprobar que sólo el propio usuario conoce sus claves de seguridad y por tanto sólo el accede al servicio.

Limitación en el importe

En algunas de las operaciones se **limita el importe por operación** (y su acumulado en un período) y a partir de determinado importe, la oficina tiene conocimiento inmediato de su realización, por lo que de observar algo anormal, realizará las verificaciones que crea convenientes.

Además el cliente tiene la opción de establecer unos perímetros de seguridad para el uso de la banca electrónica, limitando algunas operaciones o ciertas cuantías.

Política Seguridad Clientes:

- Desconfíe de aquellos mensajes de correo electrónico que provengan de sitios desconocidos o que contengan información incoherente.
- Nunca entregue su identificador y contraseña u otros datos personales cuando éstos le sean requeridos por mensajes SMS, fax, un mensaje de correo electrónico, o por un enlace contenido en el mismo, que no apunte a una dirección segura (https:).
- Recuerde que su código de acceso es personal e intransferible. Se recomienda cambiarlo periódicamente para evitar el acceso por parte de terceros. Además, recuerde memorizarlo y evite su anotación.
- Guardar con cautela la tarjeta de claves o la Tarjeta de Identificación Digital, sin permitir su acceso a terceros. Estas tarjetas son la llave que permite la realización de operaciones.
- Evite la visualización o el acceso de su tarjeta de claves por parte de terceros y no realice copias de la misma. Si utiliza una Tarjeta de Identificación Digital, recuerde retirarla del lector cuando haya dejado de utilizarla; asimismo, cambie periódicamente el PIN de su tarjeta, recuerde memorizarlo y evite su anotación.
- Utilice un sistema antivirus y antispyware, actualizándolo con frecuencia, preferiblemente de forma automática.
- Actualice su navegador y sistema operativo con las mejoras de seguridad que aportan los fabricantes y siempre siguiendo sus indicaciones.
- Si dispone de conexión permanente (del tipo ADSL, cable o similar) es conveniente instalar un firewall (cortafuegos) personal.

- Tome precauciones adicionales cuando utilice ordenadores públicos o compartidos.
- Si detecta o sospecha algún problema de seguridad, contacte inmediatamente con el Banco.
- Compruebe si la fecha y hora del último acceso que se le informa al entrar en los servicios de Banca a Distancia coincide realmente con la última vez que los utilizó.

Para los empleados. Canal BS (Intranet y Extranet)

La información obtenida en este apartado ha sido conseguida directamente de los propios empleados del banco Seguro, que tuvieron la amabilidad de explicarme, dentro de lo que se les permite, como funciona red de equipos informáticos y su canal de trasmisión de información interna, conocido como Canal BS.

Para la creación de este sistema el Seguro, en el año 2000 (fecha aproximada), el banco ya contaba con su propio equipo informático, que con las pautas que les dio la directiva, se encargaron de la elaboración del sistema y su programación.

En la actualidad sigue habiendo un departamento informático, que se ha encargado del mantenimiento, desarrollo y actualización del Canal BS, pero antes es necesario conocer cómo funciona su red de equipos informáticos.

Red de equipos informáticos del Banco Seguro

Para la instalación, mantenimiento y programación de los equipos de las diversas oficinas y sucursales, se delega en empresas locales de las mismas, subcontratando personal cualificado de estas. Digo “subcontratados” porque aunque trabajen para otra empresa, tienen un contrato con al banco para hacer que los equipos estén perfectamente durante toda su vida útil. Para ello han de pasar un cursillo de formación implantado por la propia entidad bancaria.

Los informáticos siguen unas pautas para la instalación del hardware y software exigido por el departamento de informática. Todos los ordenadores son iguales en función de la tarea que tiene que desempeñar el empleado que los va a usar.

Para asegurar que no hay ningún fallo en el sistema, los ordenadores son supervisados, mediante auditorías internas periódicas, por los informáticos del banco. Cuentan con los mejores antivirus y cortafuegos del mercado y están conectados a una red de vigilancia 24 h.

Como medidas de seguridad adicionales cada oficina cuenta con un sistema de bloqueo de los equipos, que permite al director de cada sucursal desactivar los ordenadores durante un periodo de tiempo. Este sistema de seguridad es el mismo que la caja fuerte del banco, es decir no se puede acceder a los ordenadores ni a la cámara fuera de horario laboral, ya que hay una secuencia temporal que solo se puede alterar con un debido periodo de antelación y con la clave de usuario del director de la oficina y del encargado de la seguridad de la misma.

Canal BS

Desde el año 2000 (fecha aproximada) el Banco Seguro implanto un sistema de comunicación y gestión interna, que permite comunicarse a los empleados y realizar las gestiones facilitándoles el trabajo.

Antes a esta época todas las operaciones a distancia se realizaban vía fax o vía telefónica, y la implantación de esta red facilito mucho el trabajo a los empleados y hizo que las gestiones internas fueran más seguras.

Este sistema ha ido evolucionando, pasando de ser un programa de comunicación de correo electrónico con clave personal de seguridad, a en la actualidad ser una aplicación que permite a los empleados del Banco Seguro comunicarse y realizar su trabajo desde cualquiera de las oficinas.

Las principales cualidades de esta red son la agilidad con la que permite realizar su labor a los empleados, pero sobre todo la seguridad:

- Es un sistema controlado permanentemente, en el que cada empleado cuando acceder a él deja un rastro.

- Solo se puede entrar desde un ordenador de una oficina del banco Seguro (intranet), aunque el banco tiene una aplicación de este sistema llamado extranet que permite a algunos empleados, en función de su trabajo en el banco (por ejemplo los comerciales), acceder desde terminales externos a esta red.

- Cada empleado tiene una clave y una contraseña propia
- En función de la labor de cada uno y de su puesto en la entidad, tiene un acceso personalizado que le limita a su campo de trabajo, a no ser que solicite una autorización y se le conceda el acceso.

- El sistema no funciona fuera del horario laboral

Desde su implantación hasta la actualidad los empleados se han sometido a diversos cursillos internos, unos para aprender a manejar el sistema y para adaptarse a los cambios de este a lo largo de los años; y otros para tener conocimiento de buenas prácticas con la banca online y los sistemas de gestión informáticos.

Estas son las pautas que da el Banco Seguroda a sus empleados en sus cursos internos y que a su vez recomienda a sus clientes para un uso seguro del BS Online:

- Navegar únicamente por sitios conocidos de los que tengamos referencias y que nos inspiren confianza, puesto que algunos virus y programas maliciosos se encuentran ocultos en páginas de Internet de dudosa confianza.

- No utilizar ficheros o programas de los que se desconoce el origen.

- No abrir mensajes de correo electrónico de origen desconocido.

- Ser precavidos con mensajes de correo electrónico que provengan de personas conocidas y que tengan un título sin sentido o inesperado. Antes de abrir estos mensajes contactar con el presunto emisor y constatar que realmente él ha enviado dicho mensaje ya que podría tratarse de un mensaje enviado por un virus.

- Disponer de un programa antivirus reconocido y mantener permanentemente actualizadas sus tablas de detección de virus. No es suficiente con disponer de la última versión del programa antivirus. Para que este sea efectivo con los últimos virus aparecidos, deberemos mantener actualizadas sus tablas.

- No abrir directamente los ficheros anexos en mensajes de correo. Es más seguro guardarlos primero en el ordenador y abrirlos desde fuera del programa de correo electrónico.

4.2. Evaluación de adaptación a ISO27001

A pesar de las evidentes medidas de seguridad que posee el Banco Seguro tanto en sus oficinas, como en sus sistemas informáticos, aun no poseen la certificación ISO 27001. Desconozco el motivo de porque esto es así, ya que las personas entrevistadas no pertenecen a la junta directiva y no saben qué planes tienen sobre si a la entidad financiera le interesa tener este sello de calidad.

En mi opinión, se están preparando para solicitar en un futuro no muy próximo este certificado. Es evidente la buenas prácticas del Seguro en materia de protección de la información como ha quedado reflejado en el apartado anterior, pero la realidad es solo una entidad financiera en España ha conseguido esta certificación, Bankia, lo que me hace reflexionar en el motivo de esta situación.

La realidad es que el **UNE-ISO/IEC 27001** es un certificado muy reciente. Su creación tiene lugar en 2005 cuando sustituyo a su antecesor de un año de vida **el UNE 71502**

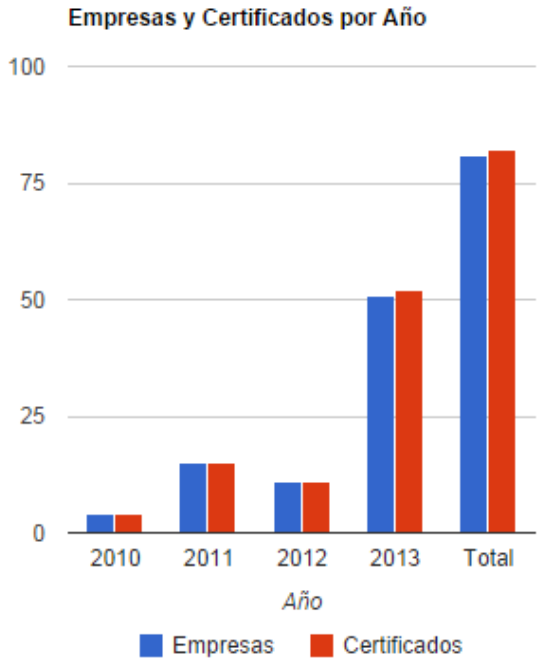
(Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)).

Esto es debido a que como he explicado en apartados anteriores, la sociedad ha sufrido un cambio muy brusco en los sistemas de información. Retomando el ejemplo usado en el primer apartado de este documento, hemos pasado en 20 años de llamarnos por teléfono fijo y mandarnos fax, a una sociedad globalizada, donde toda la información está conectada.

Con esto quiero decir que la idea de protección de la información, para algunas empresas ha cambiado mucho, ya que, lógicamente, aun se están amoldando a las nuevas tecnologías (dispositivos móviles y aplicaciones), y a las nuevas redes de información (redes sociales), para proporcionar sus servicios.

La conclusión que saco de todo esto, es que la sociedad está cambiando muy rápido en este aspecto y con ello las empresas, quedando reflejado que la gran mayoría de ellas están en desarrollo de estas tecnologías, y por supuesto en los certificados de calidad a los que nos referimos en este documento.

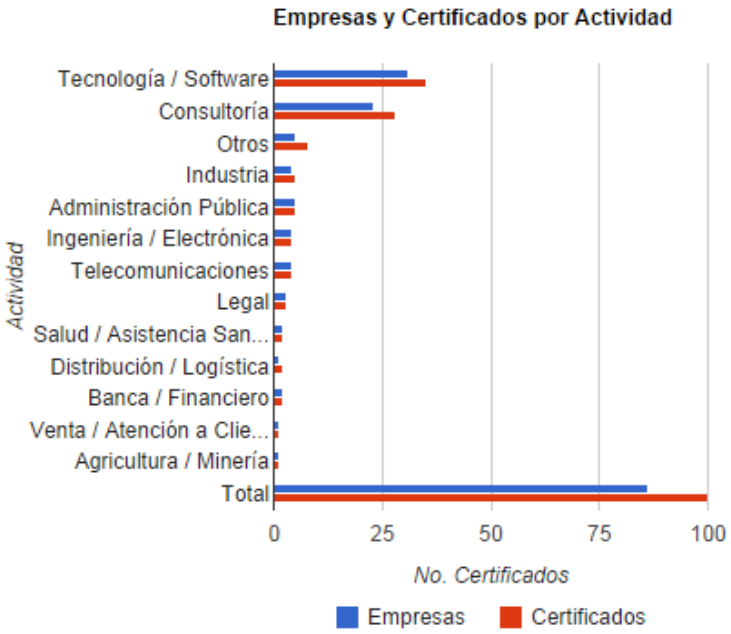
Esta teoría se puede ver reflejada en la siguiente grafica:



En 2010 se concedieron 4 certificaciones ISO 27001 a 4 empresas. Se puede apreciar la evolución donde ya en 2013 se concedieron 52 certificaciones a 51 empresas.

La situación de porque el “Seguro” y ninguna entidad bancaria salvo Bankia, poseen este certificado, se ve jusficada en que no han necesitado este sistema de certificación

como lo han podido necesitar otras empresas de otros sectores. En la siguiente grafica podemos apreciar esta afirmación:



Como era de esperar, Empresas de software informático y las consultorías son las empresas más interesadas en tener un buen SGSI y el certificado ISO 27001, debido, evidentemente al valor de la información que manejan en estos sectores y a que son empresas, que viven de sus equipos informáticos

Los bancos, a pesar de manejar información de gran relevancia y valor tienen algo que no tienen las otras empresas: se crearon para proteger los bienes. La sociedad asocia un banco como un lugar donde pueden proteger sus bienes más preciados, sean tangibles o intangibles. De ahí que no hayan necesitado hasta la fecha un sello de calidad para demostrar la seguridad de sus servicios. **Son empresas consideradas seguras de por sí.**

Eso sí, ahora la gran mayoría de las entidades financieras disponen de un sistema de Banca Online en constante desarrollo. Se han creado aplicaciones para los Smartphones que permiten controlar y gestionar tu cuenta desde cualquier parte.

Lo curioso es que este desarrollo tecnológico en los bancos está teniendo lugar ahora, lo que me hace aventurarme a decir que entre este año y el próximo, las entidades bancarias comenzaran a requerir el certificado ISO 27001 (y entre ellas el “Seguro”)

porque con estos nuevos avances, en mi opinión, va a ser necesario ya que al cliente le trasmitirá una seguridad que antes no tenía.

Entre lo que he averiguado del Banco Seguro este tiempo, destaca que ha sido uno de los bancos que más ha crecido en la última década. Lo ha conseguido tomando las decisiones acertadas y con una buena gestión. Esto, unido a la estructura que posee actualmente en sus sistemas informáticos y su red de información, me hace intuir que se está preparando para solicitar la certificación ISO 27001.

4.3. Recomendaciones: Pasos para lograr la certificación ISO27001.

En este apartado, voy a ponerme en el papel de la directiva del Banco Seguro y dar los **pasos** necesarios para llegar a conseguir la certificación ISO 27001 en Seguridad de la información.

Sé por la información recogida en apartados previos a este, que este banco ya tiene un sistema muy avanzado de Seguridad Informática y de la Información, por lo tanto posiblemente solo solicitaría una auditoría a una empresa de certificación.

Vamos a suponer que la directiva del Banco Seguro quiere ir sobre seguro y quiere dar todos los pasos hasta llegar a la certificación. Para ello nos vamos a basar en este esquema que muestra los controles que establece el ISO27001.

1. **Elegir una empresa de Certificación**

Por prestigio y por los servicios que nos proporciona vamos a elegir una de las dos empresas de Certificación analizadas en este documento: **BSI**

Elijo BSI porque nos proporciona los servicios de Formar, Auditar y Certificar en Sistemas de Seguridad de la Información ISO/IEC 27001.

Como ya hemos mencionado es una de las empresas de certificación de más prestigio que operan en España por lo que creo que sería una decisión acertada.

2. **Creación de un SGSI y de un Política de Seguridad**

Mediante la información obtenida de la Norma ISO 27001 y junto la ayuda de BSI, la junta directiva del Banco Seguro, deberán establecer un SGSI y a su vez crear un departamento informático en el que delegar a la hora de crear la política de seguridad informática.

Como ya hemos dicho, el "Seguro" ya tiene una buen Sistema de Gestión de la Seguridad de la Información y una buena política de seguridad, lo que voy a explicar los pasos que se deberían haber dado si empezara de cero y aparte decir cómo creo que se podría mejorar el que tiene actualmente para que pase la auditoría:

El encargado de la creación del SGSI debe ser la **junta directiva**. Como hemos mencionado, BSI concede sistemas de asesoramiento y formación por lo que como empresa contratada podría intervenir en su creación. Pasos:

Definir una política de seguridad que:

- Incluya el marco general y los objetivos de seguridad de la información de la organización.
  Protección de la integridad de los activos del banco, así como la información de valor de la misma empresa o de los clientes.
- Considere requerimientos legales relativos a la seguridad de la información
  En este caso la Norma ISO 27001

- defina con claridad los riesgos y amenazas a los que se enfrenta la empresa.

  Robo de activos monetarios y derivados en el interior de las sucursales y sustracción de información privada de los clientes que ponga en peligro la integridad de sus bienes.

- establezca los criterios con los que se va a evaluar el riesgo.
- esté aprobada por la dirección.

Se crearan una serie de **medidas de seguridad para la protección de los activos** físicos e informáticos que se aplicara a todas las aéreas de banco:

- Instalación de un sistema de video vigilancia en todas las sucursales.
- Acceso a diversas áreas con lector de huella digital y sistemas de contraseña.
- Cierre de seguridad de la cámara de cada sucursal, así como de los equipos cuando no se está en horario laboral
- …

El departamento de informática sería el encargado de crear una **red central de información** segura en función de la norma ISO 27001. En este caso el Banco Seguro ya lo tiene y ha hecho un buen trabajo con el BSOnline, el Canal BS y el Sistema de Red Central de Seguridad (ya explicados anteriormente).
A su vez serán los responsables de la elección de los equipos informáticos que habrá en las oficinas, así como los programas de seguridad instalados en ellos (antivirus, cortafuegos o sistemas de bloqueo de acceso)

Cambios a realizar:

- Creo que el sistema **tarjeta de claves** o **la Tarjeta de Identificación Digital** para el BSOnline es un error.

  Es un sistema en el que para acceder necesitas una clave que puede variar entre 80 aleatoriamente. Tiene esa tarjeta con todas las claves y cuando intentas hacer una trasferencia u otra operación similar te pide una de ellas aleatoriamente (por ejemplo, la clave 34).

Para realizar una operación de este tipo primero debes de meterte dentro de tu cuenta de BSOnline con un nombre y clave de usuario personal, pero aun así, un despiste dejándote la cuenta activada en tu teléfono por ejemplo, ya puede suponer una situación de riesgo en caso de robo.

- La **política de acceso al Canal BS** según la labor en el banco creo que es errónea.

  En mi opinión creo que puede dificultar el trabajo, ya que si un empleado del banco necesita acceso a determinada información que no está asociada a su campo, puede generar deficiencias en su labor y perjudicar tanto al banco como a los clientes.

  En su lugar insistiría con una política de concienciación más intensiva en buenas prácticas, para que no haya problemas a la hora de acceder a la información de determinadas aéreas de la empresa, ya que además el manejo de la información está controlado por el servidor central en todo momento siendo un método de control suficientemente bueno según mi criterio.

3. Organización de la seguridad de la información

Toda la política de seguridad ha de estar reflejada en un **manual de seguridad**. En él se recogerán todos los riesgos a los que se pueden enfrentar los empleados del banco y los propios clientes, así como las pautas a seguir ante dichos riesgos y los sistemas de prevención de los mismos.

Se establecerá quien es el responsable de esta seguridad, es este caso nos encontramos con dos situaciones:

- La seguridad de las instalaciones (cada oficina, y cada entidad bancaria) y de los activos físicos que se encuentran en su interior, el responsable será la empresa de vigilancia contratada.
- La seguridad de la información y de acceso a los sistemas informáticos y sus contenidos, recaerá sobre la junta directiva y el departamento informático, creadores de las políticas de seguridad y de la red central.

4. Gestión de los Activos de Información

En el Manual de Seguridad, se establecerán unas directrices a seguir por los empleados a la hora de manejar la información personal y de la empresa. Estas normas permitirán que no se vulnere ninguno de los pilares básicos de la seguridad de la información (disponibilidad, confidencialidad, integridad y no repudio):

- Manejo responsable de la información de la empresa y de los clientes, usando redes de comunicación seguras (BSOnline y CanalBS).
- Uso correcto del material informático, no accediendo a web de seguridad dudosa y no abriendo correos de procedencia desconocida o sospechosa.
- En caso de operar desde fuera de una oficina, utilizar un equipo informático con las medidas de seguridad básicas, como antivirus actualizado y conexión a una red con cortafuegos, evitando las redes públicas.
- …

5. Seguridad Ligada al personal

BSI sería la encargada de dar cursos de formación y concienciación en seguridad informática, a todos los miembros de la plantilla, en los que se aseguren una corre Este punto se puede dar de dos maneras:

- **Formación individual**: a todos los miembros de la plantilla, sin excepción (empleados, directiva, asesores…)

- **Formación de personal de auditoría interna**: Serian empleados del propio banco que se les formaría para poder realizar auditorías internas en la empresa, y así conseguir mantener el nivel en todo momento; y también para dar los cursillos de formación y concienciación a sus propios compañeros.

En mi opinión la segunda opción es la mejor, ya que tiene en nomina a alguien que conoce la empresa que va a asegurarse que tus sistemas de seguridad informativa y

los conocimientos de los empleados sobre la seguridad de la información, están siempre al día.

6. Seguridad física del entorno

Como hemos mencionado antes, se deberán incluir en el manual de seguridad unos sistemas de protección física del entorno laboral:

- Sistemas de video vigilancia en las oficinas y sucursales
- Sistema de acceso a ciertas áreas relevantes mediante huella digital o contraseña.
- Bloqueo de seguridad automático de los equipos y las puertas fuera de los horarios laboral.
- …

7. Gestión de las Operaciones y Comunicaciones.

En el Manual de seguridad se detallaran los criterios para la gestión de las operaciones y comunicaciones:

- Se trabajara siempre mediante la red de comunicaciones del banco, se en oficina o fuera de ella (Extranet).
- La red central de Seguridad controlara los movimientos de las gestiones y comunicaciones.
- La red central de Seguridad realizara copias de seguridad, de toda la información que entre en los servidores del banco.
- Para operaciones de alto riesgo o de mucha importancia la propia red, mediante un sistema de filtrado, exigirá al empleado la solicitud de la operación, para que quede registrada, controlada y revisada. Una vez solicitada la operación, si es segura y viable, se le dará luz verde para su realización.
- …

8. Control de acceso

Como hemos mencionado antes en el Banco Seguro, hay acceso limitado a ciertas áreas según la labor que desempeña cada empleado. Esta medida de control la suprimiría para agilizar las labores de los empleados e impartiría las siguientes (algunas ya mencionadas en anteriores apartados):

- Cuenta de Usuario personal con contraseña de máxima seguridad (más de 8 dígitos, con letras mayúsculas minúsculas, números y signos.) para empleados y clientes en la banca Online (CanalBS y BSOnline).
- Puntos de control de acceso a determinadas áreas físicas de las instalaciones, mediante sistema de huella digital y contraseña numérica.
- Registro de todas las operaciones mediante la red informática central.
- Sistema de filtración de operaciones de alto riesgo o de gran importancia, que obliguen al empleado a solicitas su gestión.
- …

9. Adquisición, desarrollo y mantenimiento de los Sistemas de Información

Como ya hemos explicado anteriormente, la adquisición de los equipos informáticos y la creación de la red de comunicaciones interna (CanalBS y BSOnline) es responsabilidad del departamento informático, con la supervisión y aprobación de la junta directiva, y con la colaboración en este caso de la empresa contratada BSI.

Una vez creado, será BSI quien mediante una auditoría interna, vea los puntos fuertes y débiles del Sistema de Información y del Sistema de Seguridad de la Información, para posteriormente notificárselo al Banco Seguro y que este resuelva las deficiencias.

Posteriormente, con los cambios constantes a lo largo del tiempo de los sistemas de información y de la tecnología, será necesario realizar una periódica actualización de los equipos y de las redes de información.

BSI, será la encargada de realizar el seguimiento de la empresa mediante auditorias periódicas que le permitan al Banco Seguro realizar los cambios necesarios que sean necesarios a lo largo del tiempo (cada tres meses o anuales).

10. Gestión de Incidentes de Seguridad

En caso de fallos de seguridad el Banco Seguro deberá de estar preparado para solventarlos rápidamente.
Si suponemos que las medidas de seguridad "preventivas" no han funcionado el banco tiene que estar preparado a la hora de tener una brecha en su sistema de seguridad de la información. Hay dos mecanismos de gestión de los incidentes en estos casos:

- Realización de contratos previos a la relación con los clientes eximiendo de "parte de la culpa" al banco, en caso de pérdidas de activos financieros o de información de valor relevante para los clientes.

  En estos contratos han de quedar claras todas las medidas de seguridad tomadas por el banco. Además han de quedar reflejadas todas las medidas que toma la entidad para cumplir con la LOPD.

  Esto evitaría acciones legales, de los afectados contra la entidad bancaria, haciéndoles conocer los riesgos a los que se exponen a la hora de realizar la relación contractual.

- Contratación de seguros, que permitan la recuperación parcial o total del montante económico de las pérdidas o daños ocasionados, en el caso de una sustracción de activos o información valiosa.

11. Creación de un plan de continuidad del negocio.

La junta directiva tendrá que tener un plan que le permita en caso de que haya un fallo en la seguridad no perder todos sus activos y perder el negocio.

En el caso que nos atañe, un banco nunca tiene todos sus activos monetarios y de valor en una única cámara. En caso de robo en una sucursal, solo se puede perder el total del valor de los activos que contiene la cámara de esa sucursal, pero al tratarse de un banco con cientos de sucursales, el daño nunca será tan grave como para evitar la continuidad del negocio. Pero, ¿ante una brecha en su sistema de seguridad informática, que plan tiene?

¿Podría un hackers, poniéndonos en una situación hipotética (y poniéndonos un poco peliculeros) acceder al sistema central de seguridad del banco y consigue transferir todos los activos financieros a una cuenta en un paraíso fiscal?

No, el Banco Seguro tiene un sistema de bloqueo de los equipos y de las redes, que en caso de un acceso no permitido o de detectar alguna intrusión el sistema se bloquea. Esta información ha sido obtenida de trabajadores del Banco Seguro y al parecer hace no mucho tuvieron un intruso en el sistema y este reacciono bloqueándose, impidiendo el acceso de todos los empleados hasta que el equipo informático acabo con la amenaza y restableció el sistema.

En mi opinión es un muy buen sistema de seguridad, y más bien es un sistema que asegura la continuidad del negocio.

12. Auditoria y Certificación

Una vez, realizadas las medidas, gestiones y normas pertinentes mencionadas en los puntos anteriores y establecido un SGSI adecuado, conocido por todos los miembros de la empresa; es hora que los auditores de BSI vengan a realizar las auditorias de certificación del ISO27001.

Realizaran una auditoria de seguridad interna, otra perimetral y un test de intrusión (explicados en el punto 4.2)

Al tratarse de una empresa con Web y banca electrónica, deberá someterse a una Auditoria Web.

Con estas auditorías la empresa de certificación BSI, comprueba que se han aplicado todas las medidas y requisitos que exige la ISO 27001.

Una vez superado lo el proceso y notificadas las incidencias para que se corrijan, se realizara una última auditoría pasados tres meses, garantizando de esta manera que el banco sigue con cumpliendo con la Norma, lo que le permitirá definitivamente tener el Sello de calidad ISO270001 en Seguridad de la Información de BSI.

5. Guía práctica para empresas

En general, al implementar medidas de seguridad es habitual centrarse en los aspectos más técnicos y no prestar atención a aspectos más formales como desarrollar una política de seguridad.

No basta sólo con escribir un documento, éste debe seguir unos pasos y debe implicar a otras personas que están fuera del ámbito estricto de actuación de la seguridad de la información.

A continuación veremos una las etapas que deben seguir las empresas a la hora de establecer una política de seguridad.

5.1. Elaboración, difusión y cumplimiento de una política de seguridad

Podemos distinguir diferentes etapas que deben seguirse en el desarrollo de una buena política de seguridad desde su creación hasta su implantación en la organización.

Fundamentalmente distinguimos tres etapas en la creación de una Política de Seguridad:

- Fase de desarrollo, en la que se crea, revisa y aprueba la Política.
- Fase de difusión, en la que se comunica, concienciа a los usuarios y/o afectados y se revisa su cumplimiento.
- Fase de mantenimiento, en la que se monitoriza su correcta funcionalidad y se llevan a cabo revisiones periódicas de la misma.

Al establecer una Política de Seguridad podemos hablar de un ciclo de mejora continua, en constante evolución. Una Política de Seguridad obsoleta no es útil… más bien todo lo contrario.

Fase de desarrollo

Esta primera fase supone un esfuerzo de investigación y redacción de la política. Es importante que en la misma seamos capaces de dar respuesta a las siguientes preguntas:

¿Por qué necesitamos una Política de Seguridad?

¿A quién afectará la Política de Seguridad?

¿Quiénes serán los responsables de aplicar y garantizar la Política?

¿Es factible su implementación en nuestra empresa?

Debemos hacer un gran esfuerzo en investigar y formalizar los requerimientos de acuerdo a marcos de buenas prácticas específicos por ejemplo, la norma ISO 27001 y extraer de ellas, aquellas que sean aplicables a las necesidades de nuestra empresa.

Una vez creada la política, se procederá a su revisión. En este punto, es importante contar con el apoyo de una persona que no haya participado en la fase de creación. Sus comentarios y notas servirán para hacer más entendible la política y para corregir posibles desviaciones de la realidad del negocio.

Una vez llevadas a cabo las modificaciones se procederá a la aprobación de la misma, para lo que debemos contar con el apoyo de la Dirección a través de la firma de la política. Indudablemente la Política de Seguridad debe ser decisión de los más altos cargos de la empresa.

Fase de difusión

Una de las principales situaciones a las que se enfrentan las empresas a la hora de proteger la información son las llamadas "malas prácticas" por parte de los empleados.

Entendemos por "malas prácticas" a los hábitos de los empleados que conllevan un riesgo de filtraciones o perdidas de información. Por nombrar unos ejemplos: el uso de los equipos para entrar a páginas de baja seguridad, la apertura de correos de desconocidos sin relación con su función laboral, uso de redes públicas para realizar gestiones de la empresa fuera del horario laboral…

Para evitar estas situaciones, es fundamental que una vez aprobada la política, se defina un plan de comunicación que establezca que recursos son necesarios para conseguir la máxima visibilidad posible de la política. Se puede concienciar a los usuarios de muchas formas diferentes: cursos, presentaciones, circulares, correos electrónicos, boletines, etc.…

Es muy importante contar con un plan de sensibilización de los usuarios y de forma continuada concienciar a los usuarios para ser capaces de garantizar que la política es conocida por todos los interesados y así evitar las malas prácticas

Fase de mantenimiento

Cuando la política es conocida por todos y ya ha sido plenamente implantada en la organización ha llegado el momento de comentar a observar si los esfuerzos que se han realizado para cumplir la política han sido correctos. Esto puede realizarse mediante la auditoría de la política o de un modo más sencillo, inspeccionando, analizando y revisando toda la información que de la política se haya desprendido (resultado de las jornadas de concienciación, estudio de la respuesta a los incidentes de seguridad, observaciones de los empleados, etc.…).

Es muy importante contar con un plan de sensibilización de los usuarios y de forma continuada concienciar a los usuarios para ser capaces de garantizar que la política es conocida por todos los interesados.

Aspectos fundamentales en una política de seguridad:

- **Seguridad física de los equipos**: Sistemas de acceso limitado, sistemas de alarma y video vigilancia, protección del recinto con las mejores mediadas de seguridad…
- **Protección de los archivos**: Protección perimetral con un sistema firewall adecuado, creación de una red y normativa de copia de seguridad de los documentos, acceso limitado a la información por cuenta de usuario y contraseña personal… **(Véase apartado 2.4 de este documento)**
- Elaboración de una **manual de seguridad** donde aparezcan las medidas de seguridad aplicadas y las normas y guía de buenas prácticas para empleados.
- **Creación de un plan de contingencia**: Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. El plan de contingencias sigue el conocido ciclo de

vida iterativo PDCA **(Véase Anexo 5)** Nace de un análisis de riesgo donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio.

5.2. Auditoria informática

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

La **auditoría informática** es el proceso de analizar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, realiza eficazmente las funciones de la organización, utiliza eficientemente los recursos y cumple normativas.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinar si los mismos son adecuados si cumplen unos determinados objetivos y establecer, si procede, los cambios que se deberían realizar para mejorar las posibles deficiencias.

El **objetivo** general de una Auditoria Informática de Sistemas de Información es evaluar la eficiencia y eficacia con que se está operando para que se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- **Auditoría de seguridad interna:** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno

- **Auditoría de seguridad perimetral:** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- **Test de intrusión:** El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense:** El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis postmortem.
- **Auditoría de páginas web:** Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- **Auditoría de código de aplicaciones:** Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los softwares y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

6. Conclusiones:

Después de realizar este estudio sobre la seguridad de la información y la seguridad informativa en el mundo laboral puedo llegar a las siguientes conclusiones:

La sociedad española se encuentra en un momento de cambio en los mecanismos de trasmisión de información. Si hacemos memoria, hace 4 años nadie tenia whatsapp, o hace 8 nadie tenia facebook, o hace 5 años nadie podía pagar una factura desde su teléfono móvil.

Lo que pretendo decir es que esta tecnología es muy reciente, demasiado para que la sociedad (hablo de la española), haya entrado a valorar lo peligrosa que puede ser en algunos aspectos de la vida.

Creo que nos encontramos en un punto en el que la sociedad está empezando a reflexionar sobre ello y a reaccionar, pero en el campo que nos importa, el de la empresa también. Esta afirmación queda reflejada en el creciente número de certificaciones en ISO27001 concedidas en los últimos años.

Esta situación hace que me plante la pregunta: ¿Es necesario tener los conocimientos aplicados en este documento?

La respuesta es sí. Cada vez el mundo está más informatizado y con ello nosotros, tanto los particulares como las empresas, son vulnerables antes riesgos que desconocen, y que por supuesto de los que no saben cómo protegerse.

La elaboración de un Sistema de Gestión de la Seguridad de la Información, hoy en día es más importante para un grupo de sectores de empresas que para otros, por el tipo de negocio al que dedican su actividad. Sin embargo la creciente importancia de las TIC en el mundo de la empresa y la globalización de la información, hace en mi opinión fundamental tener una adecuada política de seguridad, que asegure la continuidad del negocio en caso de un ataque o algún tipo de incidente relacionado con sus sistemas de gestión de la información.

Después de esto creo que mi afirmación inicial sobre la trascendencia que debería tener este proyecto es correcta, y me reafirmo en ella. Creo que todo el mundo debería de tener unos conocimientos básicos sobre seguridad informática y de la información, pero sobre todo la gente del mundo de la empresa: estudiantes, trabajadores, empresarios...; ya que son los encomendados de manejar información que puede ser de gran valor, no solo para ellos, sino también clientes y de la propia empresa.

Si una joyería tiene un sistema de alarma y complejos elementos de alta seguridad para proteger sus joyas y activos monetarios... ¿no debe cualquier empresa actual, completamente informatizada, proteger sus activos intangibles y toda su información (de gran valor) con los mejores sistemas de seguridad de la información?

7. Bibliografía

www.iso27000.es

www.agpd.es

www.lopd.org

http://protejete.wordpress.com/

www.websecurity.es

www.inteco.es

Apuntes de FECEM (La TIC´s en la empresa)

http://www.aenor.es/

http://www.bsigroup.es/

www.bancsabadell.com

www.bankia.es

www.bancosantander.es

Apuntes UM (Seguridad Informática)

www.hispasec.com

Sánchez Fernández de Valderrama, José Luis *Teoría y Práctica de la Auditoría.* 4ªEdicion. Editorial Pirámide. Facultad de ciencias económicas y empresariales.

http://www.microsoft.com/

9. Anexos

Anexo 1

Encuesta sobre buenos hábitos en la seguridad informática y de la información.

A todos los encuestados primeros se les paso por unas preguntas de corte para ver si estaban dentro del tipo de personas necesarias para la encuesta. Queríamos un individuo con conocimientos de informática, y que use a diario cualquier equipo informativo o red informática, en su vida cotidiana o laboral. Las preguntas de corte fueron las siguientes:

1. ¿Maneja usted a diario equipos informáticos para su vida cotidiana o laboral?
2. ¿Tiene cuenta de correo electrónico o es usuario de alguna red social?
3. ¿Alguna vez ha hecho alguna gestión vía web, como una compra, uso de banca electrónica…?

Una vez respondidas estas tres preguntas, si las tres respuestas eran afirmativas, el individuo pasaba al cuestionario sobre buenos hábitos en la seguridad informática y de la información:

Sobre contraseñas web

1. ¿En sus cuentas de correo electrónico, Facebook, eBay… ¿Sus contraseñas son de más de 8 dígitos y con números, mayúsculas, minúsculas y símbolos sin sentido?
2. ¿Tiene más de una contraseña diferente?
3. ¿Renueva con frecuencia (entre uno y dos años) sus contraseñas?
4. ¿Sabe usted de memoria todas las contraseñas evitando anotarlas en algún sitio?

Sobre gestiones vía web

5. ¿Evita usar una red pública para realizar compras por internet, usar la banca electrónica…?
6. ¿Cuándo realiza un compra en alguna web, verifica que se trata de un sitio web seguro (que aparezca en la barra de búsqueda http//:… en verde)

Otros:

7. ¿Tiene un correo electrónico diferente en el trabajo y en su vida contidiana?
8. ¿Tiene instalado un sistema firewall en su red privada?
9. ¿Actualiza el antivirus cuando su equipo se lo recomienda?
10. ¿Desconecta su red WIFI y sus equipos cuando no está en su casa)

Para darle sentido a esta encuesta y hacer una valoración, cada respuesta afirmativa se considera un buen hábito, por lo que al encuestado se le otorga 1 punto, y cada respuesta negativa, 0 puntos. Del total de las preguntas se realizara una valoración sobre 10.

Sujeto	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	
1	1	1	0	1	1	1	0	1	1	1	8
2	0	1	0	1	1	1	0	0	1	0	5
3	0	0	0	1	1	0	1	0	1	0	4
4	0	0	0	0	1	1	0	0	0	0	2
5	0	0	0	1	1	0	0	0	1	0	3
6	0	1	0	1	0	0	1	1	1	1	6
7	0	0	1	1	1	0	1	0	1	0	5
8	0	0	0	1	1	1	0	0	1	0	4
9	1	0	0	1	1	0	0	1	1	0	5
10	0	1	0	1	1	1	0	0	0	0	4
11	1	0	0	1	0	1	1	0	1	0	5
12	1	0	0	1	1	1	1	0	1	0	6
13	0	0	0	0	1	1	0	1	1	1	5
14	0	0	0	1	0	1	1	0	0	0	3
15	0	1	0	1	1	0	0	1	1	0	5
16	0	0	0	1	1	0	0	1	1	0	4
17	0	1	0	1	1	1	1	1	0	1	7
18	1	0	0	1	0	1	1	0	1	1	6
19	0	0	1	1	1	0	1	0	1	0	5
20	0	1	0	0	1	0	0	0	1	0	3
21	0	0	0	1	1	0	0	0	1	1	4
22	1	0	0	1	1	0	0	0	0	0	3
23	0	0	0	1	1	1	1	0	1	0	5
24	0	1	0	1	1	1	1	0	1	0	6
25	0	0	0	1	1	1	1	1	0	1	6
26	0	0	0	0	1	0	0	0	1	1	3
27	1	0	0	1	1	0	0	0	1	0	4
28	1	0	0	1	1	1	0	0	1	1	6
29	1	0	0	1	1	1	1	0	0	0	5
30	1	0	0	1	0	1	1	1	1	1	7
									Media=		4.59

Como podemos observar, una vez realizada la encuesta y una media aritmética entre todos los encuestados, con un **4,59** no "aprueban" en buenos hábitos en la seguridad informática y de la información.

Anexo 2

Seguridad de la Información y Protección de Datos

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos.

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

Para ilustrar un poco la diferencia entre los dos, se recomiendo hacer el siguiente ejercicio.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otros consecuencias negativas para la institución.

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en si mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, si o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

Si revisamos otra vez los resultados del ejercicio con el banco y en particular los elementos que clasificamos como "Información Confidencial", nos podemos preguntar, ¿de qué manera nos podría perjudicar un supuesto mal manejo de nuestros datos personales, por parte del banco, con la consecuencia de que terminen en manos ajenas? Pues, no hay una respuesta clara en este momento sin conocer cuál es la amenaza, es decir quién tuviera un interés en esta información y con qué propósito.

Anexo 3

Estructura del ISO 27001:

0. **Introducción**: Generalidades e introducción al método PDCA
1. **Campo de aplicación**: objetivo, aplicación y tratamiento de exclusiones
2. **Normas para consulta**: otras normas que sirven de referencia
3. **Términos y definiciones**: términos más usados en la norma
4. **Sistema de gestión de la seguridad de la información**: cómo establecer, implementar, monitorizar, revisar, mantener y mejorar el SGSI; requerimientos de documentación y su control.
5. **Responsabilidad de la dirección**: en cuanto a compromiso con el SGSI, provisión de recursos y formación y concienciación del personal.
6. **Auditorías internas del SGSI**: cómo realizar las auditorías internas de control
7. **Revisión del SGSI por la dirección**: cómo gestionar el proceso de revisión constante del SGSI.
8. **Mejora del SGSI**: mejora continua, acciones correctoras y acciones preventivas
9. **Objetivos de control y controles (Resumen de controles)**: anexo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
10. **Relación con los principios de la OCDE**: correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
11. **Correspondencia con otra normas**: tabla de correspondencia de puntos con ISO 9001 y 14001
12. **Bibliografía**: normas y publicaciones de referencia.

Esta norma está orientada a aspectos netamente organizativos. Organizar la seguridad de la información. Propone una secuencia de acciones referentes a establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI (Sistema de Gestión de la Seguridad de la Información).

Anexo 4

Estructura y documentación de un SGSI

Trasladando el modelo ISO 9001 a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, mostramos la documentación del sistema como una pirámide:

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

ISO 27001 indica que un SGSI debe estar formado por los siguientes **documentos** (en cualquier formato o tipo de medio):

- *Alcance del SGSI*: Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- ***Política y objetivos de seguridad***: Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- ***Procedimientos y mecanismos de control que soportan al SGSI***: Aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- ***Enfoque de evaluación de riesgos***: Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- ***Informe de evaluación de riesgos***: Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- ***Plan de tratamiento de riesgos***: Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- ***Procedimientos documentados***: Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la

información, así como para la medida de la eficacia de los controles implantados.

- ***Registros***: Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- ***Declaración de aplicabilidad***: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Acciones de gestión sobre los documentos generados

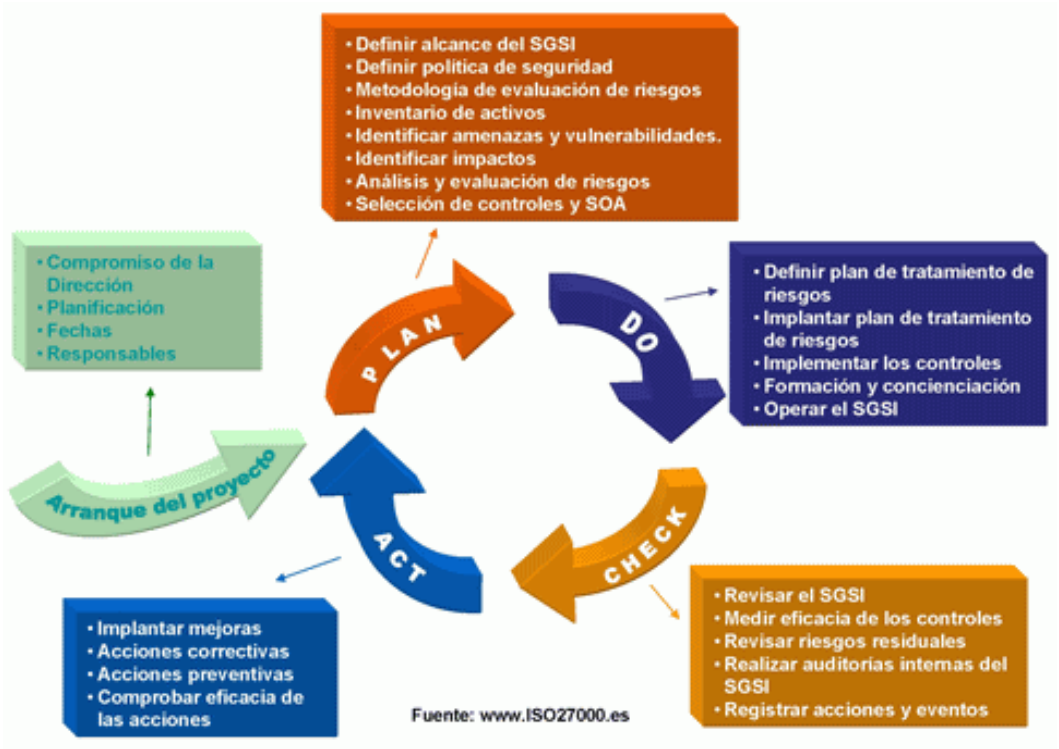
Se debe establecer, documentar, implantar y mantener procedimientos para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA (Plan – Do – Check – Act), tradicional en los sistemas de gestión de la calidad y se aplica a toda la estructura de procesos del SGSI.

Anexo 5

Modelo PDCA para SGSI



0. Arranque del proyecto

- Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
- Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

1. **Planificar**

- Definir alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir política de seguridad que:
    - incluya el marco general y los objetivos de seguridad de la información de la organización.
    - considere requerimientos legales o contractuales relativos a la seguridad de la información.
    - esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
    - establezca los criterios con los que se va a evaluar el riesgo.
    - esté aprobada por la dirección.
- Definir el enfoque de evaluación de riesgos: apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.
- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
- Identificar amenazas y vulnerabilidades.
- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Análisis y evaluación de los riesgos:
    - evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
    - evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
    - estimar los niveles de riesgo.

    - determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Identificar y evaluar opciones para el tratamiento del riesgo
    - aplicar controles adecuados;
    - aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
    - evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
    - transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI.
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability). Tiene que incluir:
    - los objetivos de control y controles seleccionados y los motivos para su elección.
    - los objetivos de control y controles que actualmente ya están implantados.

2. **Implementar y Operar**

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

3. **Monitorizar y revisar el SGSI**

- Ejecutar procedimientos y controles de monitorización y revisión.
    - detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
    - identificar brechas e incidentes de seguridad.
    - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
    - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
    - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la eficacia del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente la evaluación de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar regularmente auditorías internas.
- Revisar regularmente el SGSI por parte de la Dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI.

4. Mantener y mejorar el sistema.

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de ***Act*** lleva de nuevo a la fase de ***Plan*** para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

Anexo 6

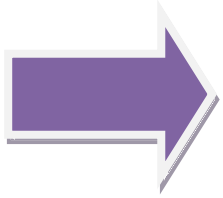
¿Qué objetivos tiene el Esquema Nacional de seguridad?:

- Crear las condiciones necesarias para la confianza en el uso de medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitan a los ciudadanos y a las Administraciones el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007.
- Guiar la actuación de las Administraciones Públicas en materia de seguridad de las TI.
- Aportar un lenguaje común para la interacción de las Administraciones Públicas entre sí y con los ciudadanos.

Estructura del ENS

Principios básicos:

a) Seguridad integral
b) Gestión de riesgos
c) Prevención, reacción y recuperación
d) Líneas de defensa
e) Reevaluación periódica
f) La seguridad como función diferenciada



Requisitos mínimos:

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de riesgos
c) Gestión de personal
d) Profesionalidad
e) Autorización y control de los accesos
f) Protección de las instalaciones
g) Adquisición de productos
h) Seguridad por defecto
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de actividad
m) Incidentes de seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

Medidas de seguridad (pag +1):

a) Marco Organizativo
b) Marco Operacional
c) Medidas de protección

Medidas de Seguridad:

a) *Marco organizativo* (Medidas relacionadas con la organización global de la seguridad):

- Política de seguridad
- Normativa de seguridad

- Procedimientos de seguridad
- Proceso de autorización

b) *Marco operacional* (Medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin):

- Planificación
- Control de acceso
- Explotación
- Servicios externos
- Continuidad del servicio
- Monitorización del sistema

c) *Medidas de protección* (Medidas centradas en proteger activos concretos con el nivel requerido en cada dimensión de seguridad):

- Protección de las instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos
- Protección de las comunicaciones
- Protección de los soportes de información
- Protección de las aplicaciones informáticas
- Protección de la información
- Protección de los servicios