CONSEJO SUPERIOR DE INFORMÁTICA Y PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA – MINISTERIO DE ADMINISTRACIONES PÚBLICAS

CRITERIOS DE SEGURIDAD
Versión 2.2. (Aprobada por Sesión plenaria de la CIABSI de 24 de junio de 2004)

http://www.csi.map.es/csi/pg5c10.htm

Este documento expone los requisitos, criterios y recomendaciones relativos a la implantación de un conjunto proporcionado de medidas de seguridad, tanto organizativas como técnicas, en el diseño, desarrollo y explotación de las aplicaciones cuyo resultado sea utilizado para el ejercicio de potestades.

Al objeto de conseguir la protección adecuada contra la pérdida de autenticidad, confidencialidad, integridad y disponibilidad, es preciso crear un entorno seguro para los datos, la información, las aplicaciones y los sistemas que los sustentan, que permitirá, entre otras cosas:

-identificar y autorizar el acceso a los sistemas de información

-identificar fidedignamente a remitente y destinatario de las comunicaciones electrónicas

-controlar los accesos para restringir el uso a personas no autorizadas a la par que evitar hipotéticas manipulaciones por su parte

-mantener la integridad de la información previniendo alteraciones o pérdidas de los datos e informaciones

-prevenir la interceptación, alteración y acceso no autorizado a la información…

A través de 19 capítulos se van tratando todos lo extremos necesarios para tales fines:

1. **Gestión global de la seguridad de la información**
2. **Política de seguridad**
3. **Organización y planificación de la seguridad**
4. **Análisis y gestión de riesgos**
5. **Identificación y clasificación de activos a proteger**
6. **Salvaguardas ligadas al personal**
7. **Seguridad física**
8. **Autenticación**

9. **Confidencialidad**
10. **Integridad**
11. **Disponibilidad**
12. **Control de acceso**
13. **Acceso a través de redes**
14. **Firma electrónica**
15. **Protección de soportes de información y copias de respaldo**
16. **Desarrollo y explotación de sistemas**
17. **Gestión y registro de incidencias**
18. **Plan de contingencias**
19. **Auditoría y control de la seguridad**

En cada uno de ellos se analizan los siguientes aspectos:

- **Requisitos** legales que obligan a aplicar distintas medidas de seguridad, en particular en relación con la validez de los procedimientos administrativos y con los datos de carácter personal.

- **Criterios** mínimos que se deben adoptar para satisfacer los requisitos anteriores, a partir de los cuales se pueden añadir protecciones adicionales.

- **Recomendaciones** que completan los criterios.

- **Niveles de seguridad** definidos por el RD 994/1999, de 11 de junio, de Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal

- **Ampliación técnica**: aporta referencias web, bibliográficas, normativas… para profundizar en los conceptos que subyacen a las medidas de seguridad.

Adicionalmente, en algunos capítulos se incluyen unas **consideraciones** que matizan el contenido del capítulo, así como un apartado denominado **conceptos** con definición o explicación de términos, y otro denominado **ejemplo de solución**, en el que se incluyen orientaciones más concretas.

1. Gestión global de la seguridad de la información

Enmarcando la gestión de seguridad de cada aplicación en un contexto global, se enumeran aquellos procesos generales estrictamente necesarios para garantizar dicha seguridad. La planificación de la seguridad es la consecuencia funcional del análisis y gestión de riesgos, premisa fundamental que realizar utilizando preferiblemente la metodología MAGERIT (metodología de análisis y gestión de riesgos de los sistemas de información). Es

preciso definir qué hay que proteger y por qué. Ello nos conducirá a la adopción de nuestra política de seguridad.

2. Política de seguridad

Es el conjunto de normas, reglas y prácticas que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de una organización. Afecta a los subestados de autenticidad, confidencialidad, integridad y disponibilidad: mediante la restricción de utilización, la prevención de alteraciones y la protección de procesos informáticos.

Su plasmación puede efectuarse a través de la elaboración de un *Documento de seguridad* que contemple la tipificación de los recursos protegidos (activos), los mecanismos de control de accesos, la gestión de soportes y copias, las obligaciones del personal… en definitiva las medidas que se implanten.

3. Organización y planificación de la seguridad

La función de seguridad de sistemas de información incluye unos contenidos con carácter general:

-aplicación de la política de seguridad

-desarrollo de normas, sistemas y procedimientos de detección de amenazas

-administración de la seguridad y de las salvaguardas tanto preventivas como correctivas

además de una serie de contenidos más específicos que los *Criterios de Seguridad* detallan.

Como criterios generales, es preciso identificar el papel de los diversos “actores“ relacionados con los activos, como usuarios, depositarios y propietarios del mismo. Pero además habrá que delimitar las responsabilidades de cada uno de ellos. En función del tamaño de la organización, además del responsable de la aplicación y del responsable o administrador de seguridad, se puede instituir un comité de seguridad. Cada uno de ellos tiene su cometido en la cadena de la garantía de la seguridad.

4. Análisis y gestión de riesgos

Es la primera y más importante tarea en toda actuación organizada en materia de seguridad, dado que permite conocer el estado de seguridad y determinar la valoración del riesgo. El análisis permite identificar las amenazas que acechan a los activos y determina su vulnerabilidad; la gestión selecciona e implanta las medidas de seguridad o salvaguardas adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos y así minimizar sus posibles perjuicios. Ambas tareas deben ser revisadas periódicamente. MAGERIT, a través de técnicas matriciales, es una buena herramienta para el análisis cuantitativo de los riesgos.

5. Identificación y clasificación de activos a proteger

Es preciso realizar y mantener un inventario de los activos a proteger, identificando a sus propietarios y documentando en el caso de activos de información los usuarios a los que se autoriza el acceso, especialmente en el caso de ficheros con datos de carácter personal.

6. Salvaguardas ligadas al personal

Los *Criterios de Seguridad* proponen las siguientes salvaguardas ligadas al personal: definir y documentar sus funciones, formar y concienciar sobre las mismas, control periódico de sus obligaciones y firmar acuerdos de confidencialidad en el caso de manejo de datos de carácter personal por personal temporal.

7. Seguridad física

Establece los criterios que permiten asegurar la protección de ciertas áreas, el control de los perímetros, de las entradas físicas, de la implantación de equipamientos de seguridad. Así, repasa cuestiones como la protección frente a instalaciones eléctricas, incendios, clima, agua, agentes químicos…Asimismo recomienda la ubicación de equipos y terminales que manejen información sensible en lugares alejados del tránsito de personal o usuarios. Aconseja ubicar las copias de seguridad en sitios diferentes. Estos son sólo unos ejemplos de entre las cuestiones que en este campo plantean los *Criterios de Seguridad*.

8. Autenticación

Se refiere a la capacidad de verificar que un usuario, convenientemente identificado, que accede a un sistema o aplicación es quien dice ser; o que un usuario que ha generado un documento o información es quien dice ser (mediante la firma electrónica). Estamos ante la verificación del usuario.

Existen diferentes niveles de autenticación en función de los niveles de seguridad establecidos (baja, normal, alta, crítica). Se establecen una amplia gama de recomendaciones para tener en cuenta en la asignación y gestión de contraseñas.

9. Confidencialidad

Es la condición que asegura que los datos o la información no estén disponibles, ni se revelen, a personas, entidades o procesos no autorizados.

Por ello, en este apartado se indican las diferentes clases de cifrado de información y cuáles deben ser usadas preferentemente. Establecen una amplia gama de recomendaciones para la asignación y gestión de claves criptográficas.

10. Integridad

Es la seguridad de que la información, o los datos, están protegidos contra modificación o destrucción no autorizada, y certidumbre de que los datos no han cambiado desde la creación a la recepción. Por ello, por ejemplo, se propone que las copias de los documentos se efectúen en soportes no reescribibles, que se utilice el atributo de sólo lectura en los archivos de información, que se analicen los accesos y recursos utilizados documentando qué registros han sido accedidos por qué usuarios, que se empleen recursos como el fechado electrónico y la firma electrónica.

En el caso concreto de la firma electrónica, su aplicación a la integridad viene del hecho de que está vinculada al firmante de manera única, permite la identificación del firmante y está vinculada a los datos a los que se refiere, de modo que cualquier cambio ulterior es detectable.

11. Disponibilidad

Es el grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Ello tiene implicaciones en la gestión del software, en las instalaciones físicas (necesidad de disponer de suministro eléctrico duplicado, por ejemplo), en el control de soportes circulantes (disquetes, CD's…), control de virus, etc.

12. Control de acceso

Es el servicio de seguridad que previene el uso de un recurso salvo en los casos y en la manera autorizados.

Es una función de seguridad esencial para proteger los datos y los tratamientos de posibles manipulaciones no autorizadas. Intervienen diversos componentes: identificación y autenticación de usuarios, autorización de derechos de acceso a distintos recursos del sistema, acceso a redes, sistemas, aplicaciones y datos, y el control y auditoría del acceso.

Su importancia es clave en el control de la seguridad. Por ello, los *Criterios* le dedican una amplia atención. Partiendo del análisis de las necesidades reales que tiene la Organización y sus componentes, se decidirán, aplicarán y verificarán los niveles de acceso de cada usuario. Es pertinente mantener y revisar dichos niveles periódicamente, con el fin de evitar distorsiones en nuestro sistema, prestando especial atención a los accesos más privilegiados. El criterio de necesidad de uso es el que debe regir la asignación de dichos privilegios. Restricciones horarias, restricciones contra la copia, mantener un registro de eventos relativos al control de acceso, interrumpir la sesión automáticamente después de un período de tiempo sin que el usuario haya realizado ninguna acción… son otras posibles medidas encaminadas al control de accesos, que es una de las piedras angulares de la gestión de la seguridad.

Además, se adoptarán medidas excepcionales para los equipos portátiles y el acceso de terceras personas.

13. Acceso a través de redes

Se entiende por acceso a través de redes cualquier tipo de comunicación, con los sistemas informáticos o de comunicaciones de una organización, realizada mediante enlaces de telecomunicaciones.

Para ello es oportuno introducir mecanismos protectores como los cortafuegos, cifrar la información transmitida a través de redes, establecer procesos de gestión de redes que faciliten estas tareas (como la segregación de redes).

14. Firma electrónica

El empleo de sistemas basados en criptografía de clave pública ha demostrado ser una de las mejores alternativas para asegurar la autenticidad, integridad y confidencialidad de los sistemas. Su uso está cada vez más extendido y también la legislación en la materia.

CONCEPTOS

Las definiciones están recogidas de la Ley 59/2003, de 19 de diciembre, de firma electrónica:

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

***Firma electrónica avanzada**: es la firma electrónica que

- permite la identificación del firmante y detectar cualquier cambio ulterior de los datos firmados
- está vinculada al firmante de manera única y a los datos que se refiere
- ha sido creada por medios que el firmante puede mantener bajo su exclusivo control

***Firma electrónica reconocida:** es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tiene validez respecto de los datos consignados de forma electrónica.

***Documento electrónico:** es el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente. Puede ser soporte tanto de documentos públicos como privados.

***Prestador de servicios de certificación**: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica. Están obligados a formular una **Declaración de prácticas de certificación** en el marco de la ley.

***Certificado electrónico**: documento firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

***Certificado reconocido**: los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten. Incluirán obligatoriamente una serie de elementos: código identificativo, identificación del prestador de servicios, firma electrónica avanzada, identificación del firmante, período de validez del certificado…entre otros que indica la ley.

***Documento nacional de identidad electrónico**: es el DNI que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

***Datos de creación de firma**: son los datos únicos (códigos, claves criptográficas…) que el firmante utiliza para crear la firma electrónica.

***Dispositivo seguro de creación de firma**: programa o sistema informático que sirve para aplicar los datos de creación de firma y que ofrece una serie de garantías.

***Datos de verificación de firma**: son los datos únicos que se utilizan para verificar la firma electrónica.

***Dispositivo seguro de verificación de firma**: programa o sistema informático que sirve para aplicar los datos de verificación de firma con una serie de garantías.

La firma electrónica en las comunicaciones administrativas será al menos firma electrónica avanzada con certificado reconocido y con una serie de requisitos mínimos.

Existe abundante normativa técnica aplicable.

15. Protección de soportes de información y de copias de respaldo

La protección de los soportes de información (discos duros, disquetes, cd-rom, cintas, ordenadores portátiles, etc.) debe incluir un conjunto equilibrado de medidas proporcionado a la naturaleza de los datos y documentos que contengan.

Además de las medidas concretas contra el deterioro físico, es preciso establecer procedimientos de realización, recuperación y pruebas de las copias de respaldos que contemplen copias de los programas, aplicaciones, documentación, bases de datos, sistemas operativos, logos; debe definirse la periodicidad con que se realizan las copias (diaria, semanal, mensual), número de copias que se realizan, etc. Los procedimientos de realización de copias serán automáticos y periódicos, y se emplearán en su elaboración formatos no propietarios que garanticen su accesibilidad en el tiempo. Se establecerán mecanismos de comprobación de presencia física y contenido de las copias de respaldo. El borrado de datos preferente será cualquiera que esté basado en ciclos de reescritura de ficheros. .

Los soportes electrónicos transportables estarán etiquetados con el máximo nivel de seguridad de la información que contengan.

16. Desarrollo y explotación de sistemas

Se debe tener en cuenta los aspectos de seguridad de la aplicación en todas las fases de su ciclo de desarrollo. Desde la planificación hasta la implantación y el mantenimiento,

incorporando las funciones de salvaguarda antes de su puesta en explotación. El análisis y gestión de riesgos se hará previamente, con el fin de incorporar las salvaguardas antes de completar el desarrollo.

17. Gestión y registro de incidencias

Es otra función esencial para el análisis de los problemas informáticos y en especial de los incidentes de seguridad. Se trata de implantar un registro de incidencias que permita reflejar tipo de incidencia, momento, persona que realiza la notificación de la incidencia y efectos de la misma. Los usuarios deben conocer los mecanismos para comunicar las incidencias y estar formados para saber cómo reaccionar ante ellas.

El registro de incidencias permitirá a la organización investigar los incidentes o intrusiones para averiguar las causas, autores y daños que ha conllevado; también permitirá detectar problemas de software.

18. Plan de contingencias

Es la forma detallada en que la organización debe reaccionar para asegurar que las aplicaciones sigan activas ante determinados eventos, accidentales o deliberados.

Partiendo del análisis y gestión de riesgos, debemos desarrolla un plan de contingencias que permita restaurar el servicio en el menor tiempo posible tras una incidente. Dicho plan identificará acciones y personas concretas con el fin de limitar al máximo la toma de decisiones durante el período de recuperación tras el incidente. El plan[1] deberá ser mantenido y actualizado.

19. Auditoría y control de la seguridad

Como en todo proceso, también la seguridad debe ser auditada con un proceso sistemático, independiente y documentado que permita evaluar con objetividad.

[1] Los *Criterios de Seguridad* detallan los elementos que deben conformar el plan de contingencias.