TEMA 1.- SEGURIDAD DE LA INFORMACIÓN: UNA VISIÓN INTEGRAL

MAGERIT V2 define la Seguridad de la Información como:

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

- **Disponibilidad**: sin duda, la característica más importante. La información debe estar disponible cuando sea necesario y por quien esté autorizado a ello.
- **Integridad**: es la característica de la información relativa a su fiabilidad. Se trata de evitar que la información sea alterada o modificada sin autorización
- **Confidencialidad**: la información sólo debe ser accesible por las personas, programas o sistemas autorizados a ello, evitando accesos no autorizados, bien sea de forma casual o intencionada

Otras dimensiones : Autenticación, No Repudio (en Origen y Destino).

DEFINICIONES

Datos: Son los símbolos que representan hechos, situaciones, condiciones o valores. Suponen la materia prima para la producción de información.

Información: Es el resultado de procesar, transformar o interpretar datos. **Supone un elemento de valor para el individuo y para la organización**

Daño: Perjuicio que se produce a consecuencia de un fallo en el sistema, bien sea fortuito o provocado.

Ataque: Acción de provocar un daño a un sistema de forma intencionada

Riesgo: Relación entre la magnitud del daño y la probabilidad de que dicho daño ocurra.

Amenaza: situación de daño cuyo riesgo de producirse es significativo

Vulnerabilidad: deficiencia de un sistema susceptible de producir, fortuita o intencionadamente, un fallo en el mismo.

Activo: Un elemento que posee valor para la organización.

Tradicionalmente, el ámbito de la **Seguridad Informática** (o Seguridad en TIs) ha puesto su énfasis en la respuesta ante amenazas debidas a los ataques por explotación de vulnerabilidades. Posteriormente, se incorporó como disciplina el **análisis de riesgos**, con tres ejes principales: los **activos** (bienes de la organización o individuo), las **vulnerabilidades** y las **amenazas**.

La Seguridad de la información conlleva una visión más amplia en el proceso de análisis de riesgos. Se integran aquí, además de los ejes tradicionales (activos, vulnerabilidades y amenazas), los riesgos propios de la organización (organizacionales, operacionales, físicos y de TIs). **Integra** el **Factor Humano**.

Así, **La Seguridad de la Información** se centra en garantizar la **Disponibilidad, Integridad, Confidencialidad, No repudio y Autenticación de la información, con** independencia del medio físico en que se almacene o transporte: digital, impreso, etc.

Desde la perspectiva del negocio: la **Seguridad de la Información** es la **protección de la información** de un rango amplio de **amenazas** para **garantizar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de la inversión.**

TRES PRINCIPIOS BÁSICOS DE LA SEGURIDAD

1.- La Seguridad no es un producto. Es un PROCESO. Ciclo de Vida:

- Diseño
- Transición (puesta en marcha)
- Operación (día a día)
- Actualización y optimización (procesos de mejora del servicio)

2.- La Seguridad plena es una utopía

Esto afecta a todas las etapas:

- En el **diseño**, minimizando la "superficie de ataque": "*Todo lo que no está explícitamente permitido, está prohibido*".
- En el **desarrollo** y **puesta en explotación**: considerando posibles **vulnerabilidades** y **amenazas**, así como garantizando los principios o **dimensiones**
- En los **procedimientos** y normas de uso: concretando qué se puede hacer y qué no.
- En el uso diario: mediante **políticas**, **revisiones**, etc.

3.- La seguridad es una cadena y, como tal, romperá por el eslabón más débil

El factor humano (fallos debidos a negligencias o desconocimiento) resulta ser, con demasiada frecuencia, el elemento más débil del conjunto.

Preguntas clave: qué proteger, contra quien, cómo y hasta donde

¿Qué queremos proteger?

Inventario de activos, donde un "activo" será todo elemento físico, lógico o humano que conforma el sistema que queremos proteger:

- Hardware, Software, Equipos de Comunicaciones, Bases de Datos, Personal
- Otros: contratos de mantenimiento, protocolos de actuación, etc.

¿Contra quién nos queremos proteger?

- Análisis de los perfiles de los posibles atacantes
- ¿Debemos protegernos de nosotros mismos?

¿Cómo lo vamos a proteger?

- Identificar elementos, tecnologías, pautas, normas, procedimientos y buenas prácticas que han de ser aplicados para garantizar los principios de la Seguridad de la Información
- Identificar previamente las amenazas y las posibles defensas

¿Hasta dónde lo queremos proteger?

- Los métodos modernos de **evaluación cuantitativa de riesgos**, permitirán establecer el punto de compromiso adecuado entre el valor de lo que se desea proteger y el coste total de la inversión

Diferentes enfoques de la seguridad de la información

- Centrado en la **Normativa** que aplica en la empresa. En el caso de España, la normativa básica se centra en:
  - Ley orgánica de Protección de Datos de Carácter Personal (LOPD)
  - Ley de Servicios de la Sociedad de la Información y Comercio electrónico (LSSICE)
  - Ley de Firma Electrónica
  - Ley de Propiedad Intelectual (LPI)
  - Ley General de Telecomunicaciones
- Centrado en el **Negocio**: Obtención de un nivel adecuado de seguridad en la organización, aportando Gestión, Valor y posibilidad de Recuperación.
- Enfocado hacia las **amenazas Tecnológicas**: Hacking, Malware, fuga de información, Ingeniería social, etc.

En la práctica, para lograr una **concepción integral de la seguridad** será necesario considerar estas **tres** vertientes (**normativa, negocio y amenazas tecnológicas**), plasmando luego el resultado en la Política de Seguridad de la Organización.

Seguridad vs privacidad: en busca del equilibrio

1948 – ONU – Declaración Universal de los Derechos Humanos: Derecho a la PRIVACIDAD.

1975 – Constitución Española (Art. 18.4): La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

1992 – LORTAD

1998 – Ley General de las Telecomunicaciones

1999 – LOPD

La **privacidad** en sistemas digitales exige el empleo de **criptografía**.

Pero... la globalización del terrorismo y la Ley de Moore (duplicación capacidad TIs cada dos años) pueden motivar a los gobiernos a limitar el derecho a la privacidad

EEUU: 1991 – Chip Clipper – Phil Zimmermann – Desarrollo del PGP – Acusación de exportación de materal militar

Europa: 1993 – Iniciativa de Directiva Europea – Claves privadas bajo control gubernamental

1996 – La criptografía deja de ser material militar

Necesidad de garantizar la privacidad ... suponiendo que un gobierno democrático, deje de serlo.

Visión integral de la Seguridad

1.- El factor humano: Seguridad en el Personal

Eslabón más débil – 70% de los incidentes son internos – Escasa o nula cultura de seguridad

Medidas básicas: Formación, acuerdos de confidencialidad y seguimiento de personal que realiza tareas críticas

2.- Seguridad física y del entorno

La protección mediante barreras físicas y mecanismos de control, de los elementos tangibles de un sistema de Tecnologías de la Información. Se trata de considerar tanto las amenazas provocadas por personas, como por aquellas que tienen su origen en fenómenos naturales

Especial atención a la seguridad física de cualquier componente (repetidor Wifi, Switch, etc.) y a las técnicas de ingeniería social.

3.- Seguridad Lógica

Aplicación de barreras y procedimientos que **protejan** el acceso a los datos de forma que sólo sean accesibles por las personas autorizadas

Objetivos fundamentales: Delimitar acceso a aplicaciones y datos, disponibilidad ante fallos

Resulta imprescindible un **equilibrio** entre fortaleza y usabilidad, entre coste y complejidad

4.- Seguridad Organizativa. Políticas de Seguridad

De la necesidad de formalizar el marco de trabajo relativo a la Seguridad de la Información, aparece el concepto de Política de Seguridad de la Organización:

“Un conjunto de normas que deben cumplirse por todas las personas que tengan acceso a cualquier información y/o tecnología de una organización”

Ha de ser:

- **Abarcable**: debe poder implantarse de forma efectiva
- **Inteligible**: tanto a nivel de conceptos como de las implicaciones de no cumplir sus directrices
- **Obligado cumplimiento**: incluirá procesos de auditoría para detectar posibles desviaciones
- **Concreción de responsabilidades**: delimitará los roles necesarios y sus responsabilidades
- **Asequible**: no debe entorpecer el trabajo
- **Mejorable**: incorporará mecanismos de autoevaluación y actualización

Seguridad a través de la oscuridad vs Seguridad a través del conocimiento

Criptografía: escritura oculta. Aplicaciones militares: Alto secreto

Hasta la era digital, todos los sistemas de cifrado se basaban en el secreto del sistema de cifrado empleado

Primeros sistemas digitales: secretos y más secretos. Seguridad: basada en la oscuridad informativa.

La seguridad por oscuridad es la filosofía en base a la que se considera que una aplicación informática será segura en la medida en que su **código interno no sea difundido**

Primeros sistemas criptográficos: basados en el **secreto. Ineficaces:** "*todo lo que un sólo hombre sea capaz de esconder, otro lo desvelará*

Seguridad Basada en el Conocimiento: Principio de Kerckhoff: : "*un criptosistema debe ser seguro, incluso si todo lo relacionado con el funcionamiento del sistema, excepto la clave, es de conocimiento público*".

Nuevos algoritmos criptográficos: concurso público. Criptoanálisis constante.

Identidad Digital. Rastro Digital. Metadatos.

Desde la primera cuenta de acceso (usuario/contraseña) hasta la gestión de múltiples identidades digitales, dejamos un Rastro Digital (cuentas de correo, perfiles y fotos en redes sociales, web personal, opiniones vertidas en foros, conjunto de búsquedas en google, compras realizadas, etc.).

- LA RED NO OLVIDA (perdurabilidad de los datos)
    - ¿Cómo manejar los problemas de privacidad asociados?
- EL RASTRO DIGITAL NOS HACE VULNERABLES
    - La manipulación como herramienta de marketing

METADATOS: Pueden plantear serios problemas de seguridad.

¿Qué saben de nosotros?

- Echelon : Sistema de interceptación de comunicaciones de voz. Autoactivación por “palabras clave” (NSA)
- Carnivore: Sistema similar escaneo en Internet (FBI)
- Sitel: versión “made in Spain”. Rastreo integral de comunicaciones (voz e Internet) bajo “control judicial”

Hacia una identidad “legal”: DNIe y certificados digitales

España ha sido pionera en la implantación de un verdadero sistema nacional de identidad digital. DNIe (2006):

- Identidad digital
- Firma electrónica avanzada
- Mejora en el servicio al ciudadano: entrega inmediata

Aproximación desde el punto de vista legal:

La Ley 59/2003 de 19 de diciembre define la firma electrónica como “el conjunto de datos en forma electrónica, consignados a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante”. Dentro de la ley se distinguen dos tipos de firma electrónica:

- **Firma electrónica avanzada**: es aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados.
- **Firma electrónica reconocida**: se considera como tal a la firma electrónica **avanzada** basada en un certificado digital reconocido y generada mediante un dispositivo seguro de creación de firma.

Este tipo de firma avanzada (DNIe) tendrá respecto a los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

Un futuro cambiante. Nuevos desafíos de Seguridad

Web 1.0, Web 2.0, Web Semántica, Redes Sociales, ubicuidad de acceso, Internet de los dispositivos, Cloud Computing....

Esto define una nueva "extensión" de Internet. No sólo se trata de redes "domésticas". Los semáforos, los radares en las autopistas, las cámaras de vigilancia, los sensores meteorológicos….cualquier cosa que se gestione remotamente. El intercambio de información ya no es exclusivo entre personas.

Es necesario **redefinir** los conceptos de Seguridad de la Información, ampliar las dimensiones existentes y replantear B**uenas Prácticas, Políticas y Estándares**. Se habla de una "Seguridad global", sin límites geográficos. Pero, el mayor peligro: unos (gobiernos) y otros (corporaciones) tendrán (tienen) la terrible tentación de romper el **equilibrio entre Seguridad y Privacidad**.

Igualmente, algo que hasta ahora se había respetado: la **NEUTRALIDAD** de Internet, también está **EN PELIGRO**.

No obstante: las TIs ofrecen respuestas que alivian problemas derivados de su propia implantación.

La Red está creando una **INTELIGENCIA COLECTIVA**. Nunca la humanidad había dispuesto de algo semejante. **ESTO SE PONE REALMENTE INTERESANTE.**