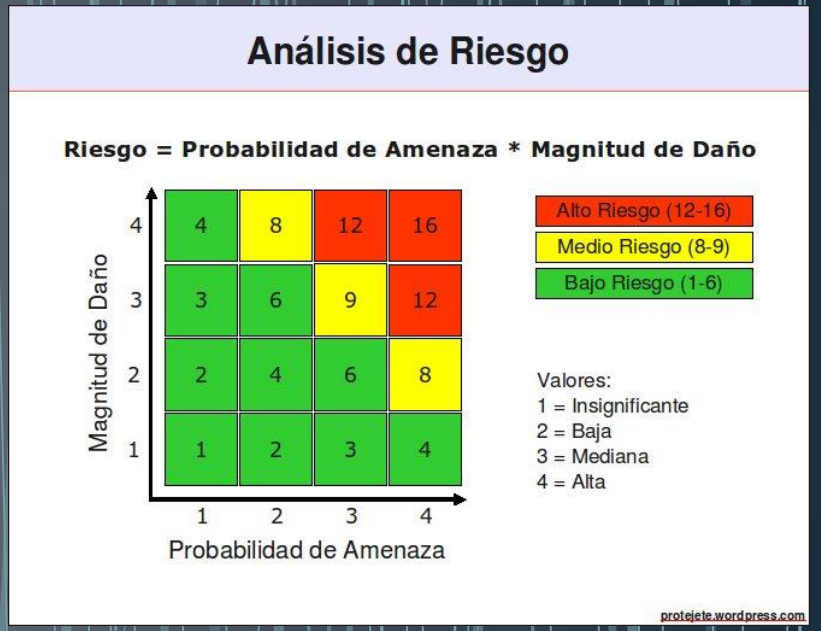
T3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN



Apartados del BOE (1/3)

- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos relacionales
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente

Apartados del BOE (2/3)

- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- Determinación de la probabilidad e impacto de materialización de los escenarios

Apartados del BOE (3/3)

- Establecimiento del nivel de riesgo para los distintos pares de activo-amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- Relación de las distintas alternativas de gestión de riesgos
- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit V2

Análisis del Riesgo: Definiciones

ACTIVO: Recursos del sistema de información o relacionados con éste, necesarios para que la organización funciones correctamente y alcance los objetivos propuestos por la dirección

TIPOS

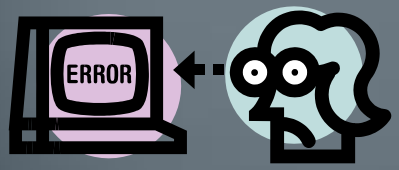
- **Información.** Información que tiene valor para los Procesos de Negocio.
- **Sistemas de Información**. Comunicaciones, Hardware y Software.
- **Entorno**. Equipamientos y suministros, Instalaciones (Edificaciones, CPD, ...) y Personal (de desarrollo, operación, ...).
- **Funcionalidad de la Organización**. Categorías relativas a clientes, estrategia, objetivos de negocio, así como productos
- **Valores de la Organización**. Aspectos legales y regulatorios, imagen, independencia, etc.

Análisis del Riesgo: Definiciones

AMENAZA: Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos

TIPOS:

Accidentes. Físico industrial, avería, físico natural, interrupción de servicios o suministros, Accidentes mecánicos o electromagnéticos .



Errores. de utilización, de diseño, de ruta, de secuencia o entrega, inadecuada monitorización, trazabilidad o registro del tráfico de Información.

Faltas en Aspectos Legales y Buenas Prácticas. Incumplimiento de las regulaciones legales aplicables o disposiciones legales que pueden ocasionar multas o sanciones por incumplimiento, ausencia de manuales, normas y procedimientos.

Análisis del Riesgo: Amenazas

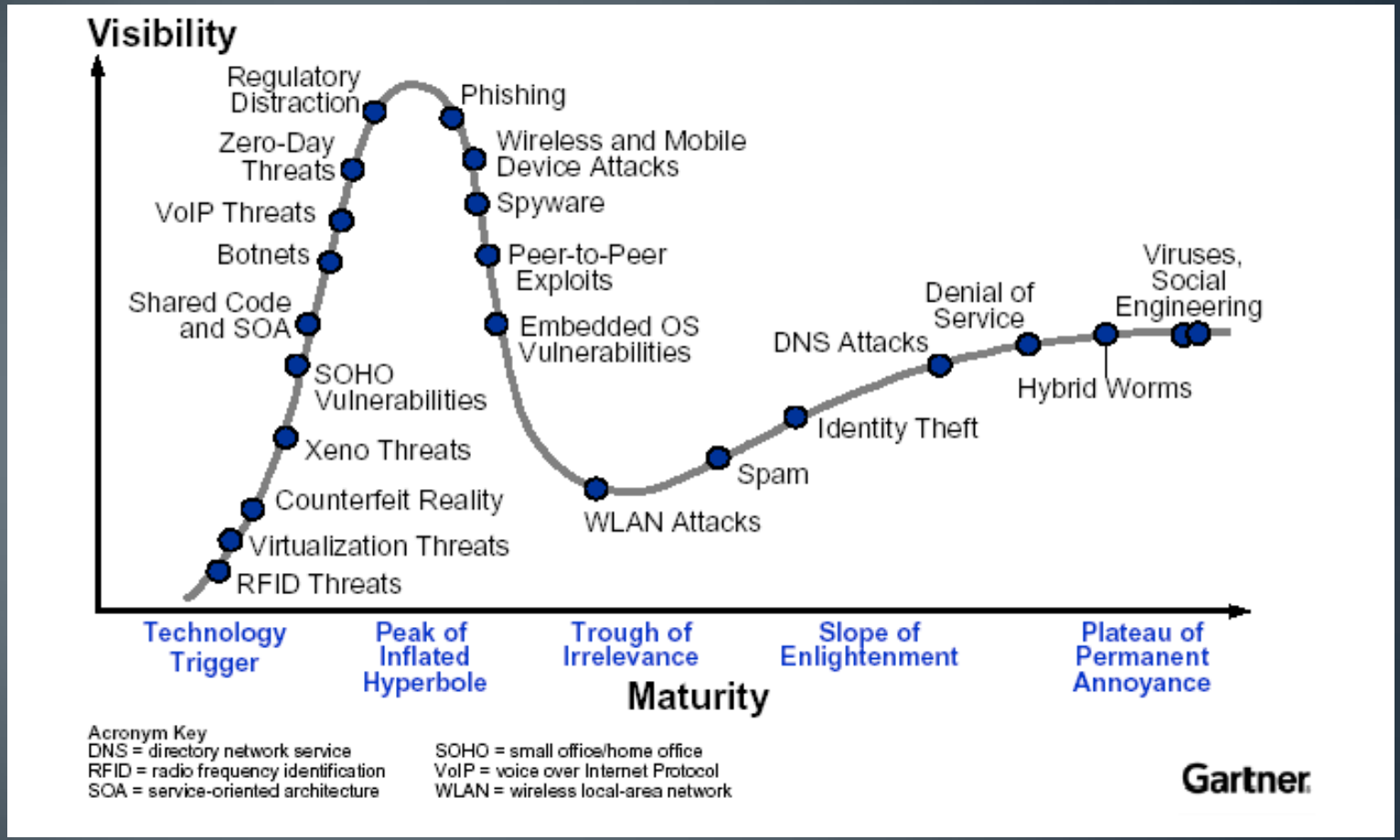
SANS Institute resources

The 7 Top Management Errors that Lead to Computer Security Vulnerabilities

Number Seven:	Pretend the problem will go away if they ignore it.
Number Six:	Authorize reactive, short-term fixes so problems re-emerge rapidly
Number Five:	Fail to realize how much money their information and organizational reputations are worth.
Number Four:	Rely primarily on a firewall.
Number Three:	Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed
Number Two:	Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
Number One:	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

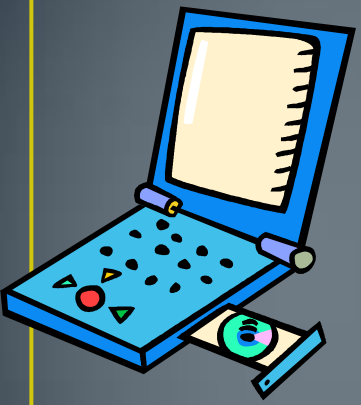
As determined by the 1,850 computer security experts and managers meeting at the SANS99 and Federal Computer Security Conferences held in Baltimore May 7-14, 1999

Análisis del Riesgo: Amenazas



Análisis del Riesgo: Definiciones

- **VULNERABILIDAD:** Probabilidad de ocurrencia de la materialización de la AMENAZA sobre un ACTIVO.



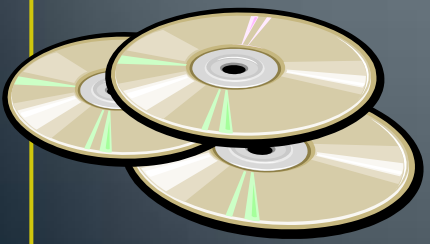
Un portátil es más vulnerable a la amenaza de robo que un sobremesa por desatención en sitios públicos o falta de medidas de seguridad (candados).

ROBO

Mantenimiento inadecuado

Los soportes no se almacenan en un entorno que cumpla con las especificaciones del fabricante

AVERÍA



La información de los soportes no se eliminan de forma segura

USO MALICIOSO

Gestión del Riesgo: Vulnerabilidades

Top 10 OWASP

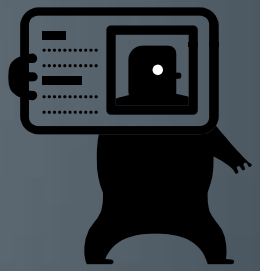
- Entrada de datos sin validar
- Violación de control de accesos
- Violación de administración de sesión y autenticación
- Vulnerabilidades de XSS (Cross Site Scripting)
- Desbordamiento de Bufer
- Vulnerabilidades de inyección: comandos sql,.
- Gestión deficiente de excepciones
- Almacenamiento inseguro
- Denegación de servicio
- Configuración insegura

Análisis del Riesgo: Definición

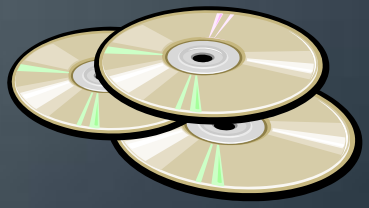
- **SALVAGUARDA**: Acción o procedimiento que potencialmente produce una acción reductora del Riesgo asociado al activo, al aplicarse sobre el mismo.

Preventivas: reducen la potencialidad de materialización de una Amenaza sobre un Activo.

CIFRADO



Curativas: que actúan sobre el Impacto que produce la Amenaza, reduciendo el mismo.



COPIAS DE SEGURIDAD

Análisis del Riesgo: Definición

RIESGO DE SEGURIDAD: Un Riesgo de Seguridad es la probabilidad de que una Amenaza dada aproveche una Vulnerabilidad para dañar un Activo o un grupo de Activos, produciendo un Impacto determinado.

TIPOS

- **Efectivo**: el que se da tras la aplicación de SALVAGUARDAS.
- **Intrínseco**: antes de aplicar SALVAGUARDAS.
- **Residual**: aplicando todas las posibles SALVAGUARDAS.

EJEMPLO

Activo: Edificio de oficinas, Amenaza: Fuego, Vulnerabilidad: Dispositivo antiincendios

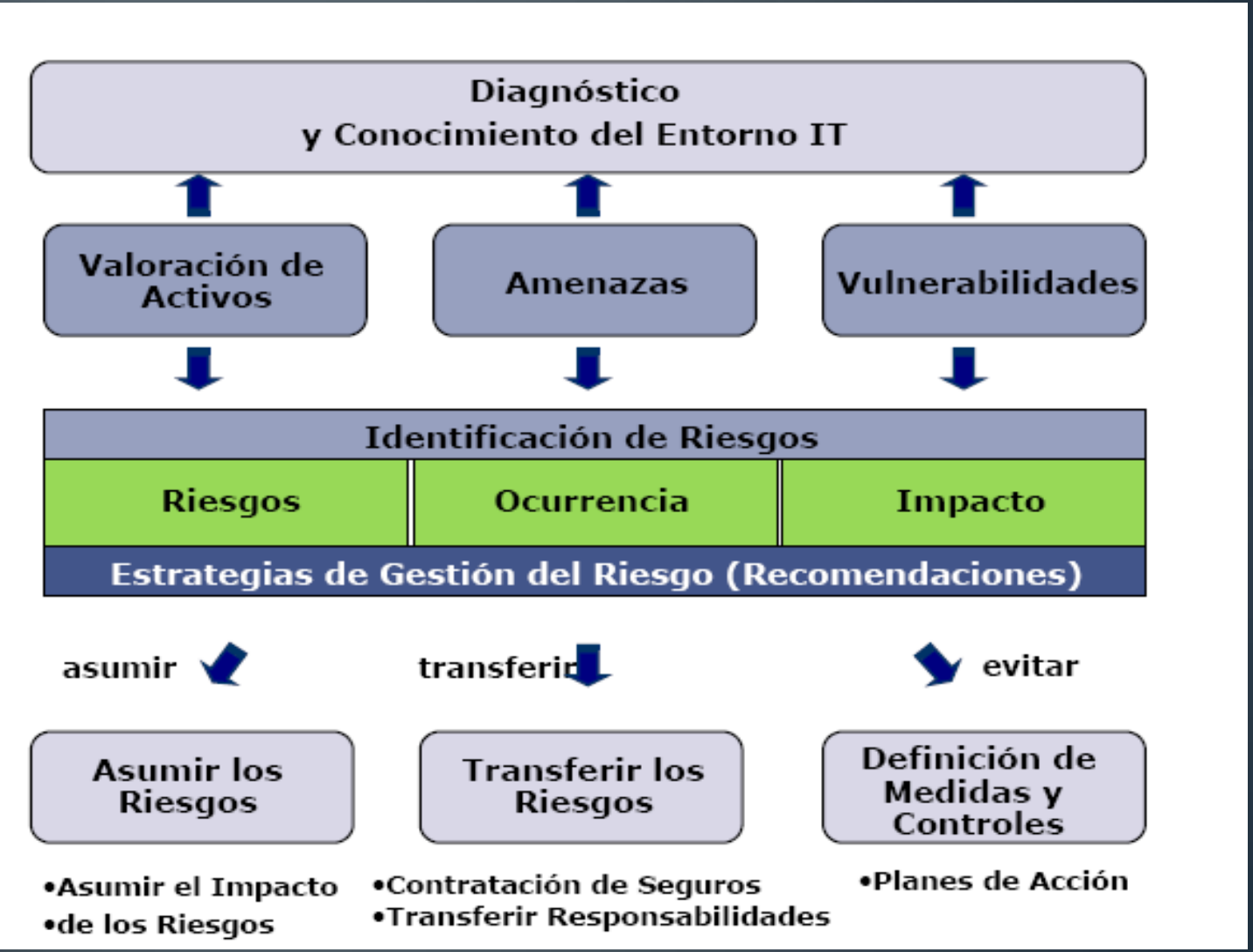
Análisis del Riesgo

Análisis del Riesgo: Dependencia de Controles 27001

Análisis del Riesgo: Valoración activos ACIDA

	VALORACIÓN DE LA INFORMACIÓN									
	AUTENTICIDAD *Garantía de la identidad de los datos.*		**CONFIDENCIALIDAD** *Grado de restricción en cuanto al acceso y la divulgación.*		**INTEGRIDAD** *Grado de veracidad, consistencia y fiabilidad de la información.*		**DISPONIBILIDAD** *Necesidad de tener la información siempre lista para su uso*		**AUDITABILIDAD** *Registro de las acciones u operaciones que hace el usuario*	
NIVEL	**Descripción**	**Impacto**	**Descripción**	**Impacto**	**Descripción**	**Impacto**	**Descripción**	**Impacto**	**Descripción**	**Impacto**
1	**ANÓNIMA**: Información que no requiere conocer el origen / autor, ni el responsable de la misma. Ej: propaganda, folletos informativos.	**Ningún efecto.**	**PÚBLICA** Información sin restricciones en su difusión. Ej: folletos de marketing, contenidos de web públicas.	**No existe impacto.**	**BAJA**: Información cuya modificación no implica ningún riesgo y puede realizarla cualquier persona. Ej: Tablón de anuncios.	**No causa impacto alguno.**	**REGENERABLE**: Se puede volver a disponer de la información en un periodo inferior a medio mes. Ej: Documentación de bienvenida para nuevos empleados.	**Afecta minimamente las actividades de personas concretas.**	**LIBRE**: No hay necesidad de registrar ninguna acción o evento. Ej: Documentos propios administrativos.	**Efecto nulo.**
2	**REMITIDA**: Información que requiera conocer los datos del emisor y el origen de la misma. Ej: Circulares firmadas, uso de usuario y contraseña.	**Pérdidas mínimas de imagen como consecuencia de confiar en un emisor equivocado.**	**USO INTERNO**: Información que puede ser conocida por cualquier persona de la organización. Ej: Normativas internas, Intranet.	**Posible publicidad negativa.**	**FIABLE**: Información restringida en su actualización a cualquier persona de la organización con acceso permitido. Ej: Modelos de plantillas de documentación definidos.	**Pérdida de imagen.**	**RECUPERABLE**: La información debe recuperarse en un tiempo inferior a una semana. Ej: Documentos de procedimientos de instalación de nuevos equipos.	**Afecta a las actividades / objetivos de un grupo de personas.**	**GENÉRICA**: Solo se registran datos de forma genérica. Ej: Accesos a la Intranet.	**Desconocimiento de cuando se realizan modificaciones sobre la información.**
3	**CONFIRMADA**: Información que precise confirmar el origen y el destino, así como la necesidad de verificar la recepción. Ej: Notificación con acuse de recibo.	**Posibles pérdidas monetarias como consecuencia de enviar información a terceros no contrastados.**	**RESTRINGIDA**: Información cuyo conocimiento y difusión se debe limitar a un determinado grupo organizativo. Ej: documentación departamental, estructura de directorios por departamento.	**Publicidad negativa y posible pérdida de clientes.**	**GARANTIZADA**: Información que exige disponer de medidas que garanticen su veracidad. Ej: Inventarios de clientes, Documentos técnicos.	**Pérdidas económicas por y posible pérdida de clientes.**	**NECESARIA**: Recuperación de la información en un plazo inferior a tres días. Ej: Información de accesos al edificio.	**Disminución de actividades en algún área.**	**PARTICULAR**: Se debe registrar a nivel de usuarios las acciones críticas de Alta, Baja y Modificación. Ej: Configuración de servidores.	**Incapacidad de persecución de delitos.**
4	**CERTIFICADA**: Información que requiera certificación por una tercera parte del origen y del destino.. Ej: E-mail con firma digital, notario.	**Pérdidas económicas e implicaciones legales por desconfianza de autor.**	**CONFIDENCIAL**: Información que debe tener accesos restringidos a un grupo muy reducido y controlado de personas. Ej: Nóminas, BBDD empleados.	**Pérdida económica alta e importantes daños en la imagen y posibles repercusiones legales.**	**SENSIBLE**: Información que debe tener alto nivel de exactitud. Ej: Ofertas entregadas a clientes.	**Fuertes pérdidas financieras y pérdida de clientes.**	**CRÍTICA**: Recuperación de la información en un plazo inferior a un día. Ej: Sistema de correo.	**Alteración de actividades internas.**	**RESTRINGIDA**: Se debe registrar a nivel de usuarios las acciones críticas de Alta, Baja, Modificación y Lecturas. Ej: Contabilidad.	**Fraude.**
5	**CRÍTICA**: Información que requiera certificación por una tercera parte, del origen, del destino, así como del contenido de la información enviada. Ej: Documentos firmados digitalmente por centros autorizados con validez legal, Notificación por conducto notarial.	**Graves implicaciones legales y pérdidas económicas.**	**SECRETA**: información de suma importancia y de carácter crítico para la organización, a la que tendrán acceso personas muy concretas. Ej: Business Plan, Ficheros estratégicos de la compañía.	**Graves problemas estratégicos y patrimoniales.**	**CRUCIAL**: Información de suma importancia desde el punto de vista de la veracidad, coherencia y exactitud para la Organización. Ej: Información económica y financiera de la organización.	**Graves problemas estratégicos y patrimoniales.**	**VITAL**: La información debe recuperarse inmediatamente. Ej: Sistemas de control de suministro.	**Interrupción elevada de actividades del negocio.**	**TRAZA TOTAL**: Se debe registrar a nivel de usuarios TODAS las acciones de Alta, Baja, Modificación, lecturas, e intentos de lectura. Ej: Datos de salud.	**Incumplimiento de obligaciones legales.**

Análisis del Riesgo: Gestión del Riesgo



Análisis del Riesgo