

Introducción a la Seguridad Informática

Conceptos Básicos La Seguridad Informática en números



Conceptos básicos:

¿Qué es la seguridad de la información?

“La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida.

La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades”. (ISO-IEC 17799 – Año 2000)



Conceptos básicos:

La información puede existir en muchas formas.

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida por correo o utilizando medios electrónicos
- Presentada en imágenes
- Expuesta en una conversación

“Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.” (ISO-IEC 17799)



Conceptos básicos:

La seguridad de la información se define aquí como la preservación de las siguientes funcionalidades:

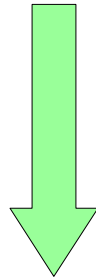
- Integridad
- Confidencialidad
- Disponibilidad

de los recursos y de la información



Conceptos básicos:

La evolución de la Seguridad Informática:



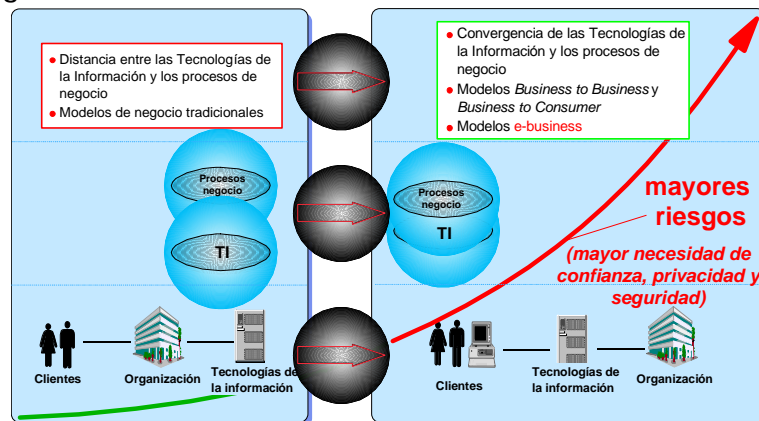
- 1965 - Departamento de Defensa de Estados Unidos.
- 1983 - Encriptación de información.
- 1985 - Virus.
- 1990 - Seguridad en redes.
- 1995 - Firewalls.
- 2000 - Seguridad en sistemas operativos. IDS's
- 2003 - Seguridad Informática Global.



Conceptos básicos:

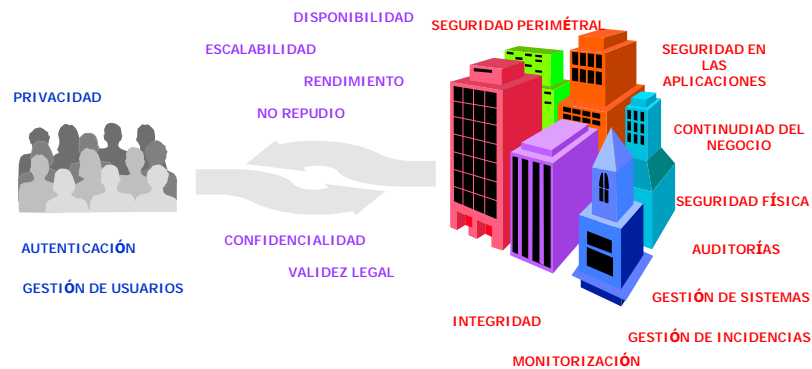
Crecimiento:

A medida que la distancia entre procesos de administración, negocio y tecnologías disminuye, el impacto de riesgos de seguridad aumenta.



Conceptos básicos:

Áreas asociadas a la Seguridad:



La seguridad informática en números:

- 85% (grandes compañías y agencias del gobierno) detectaron problemas de seguridad en los últimos 12 meses.
- 35% (186 respuestas) pudieron cuantificar sus pérdidas financieras. Estos 186 reportaron \$377.828.700 en pérdidas financieras.

Fuente: The Computer Security Institute with the participation of the Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 12 March 2001,



La seguridad informática en números:

- La mayor pérdida financiera es debido al robo de información (34 respuestas reportaron \$ 151.230.100) y fraude financiero (21 respuestas reportaron \$ 92.935.500).
- 36% reportaron las intrusiones.
- 40% detectaron una intrusión proveniente del exterior
- 38% Detectaron ataques de Negacion del servicio
- 91% Detectaron abusos de los empleados de los privilegios de acceso sobre Internet
- 95% Detectaron virus informáticos, solo el 85% en el 2000



Introducción a la Norma ISO 17.799

Tecnología de la información

Código de práctica para la
administración de la
seguridad de la información



La Seguridad Informática actual

- Riesgos e impacto en los negocios
- Normas aplicables
- Enfoque ISO 17799



Algunas premisas:

- No existe la “verdad absoluta” en Seguridad Informática.
- No es posible eliminar todos los riesgos.
- No se puede ser especialista en todos los temas.
- La Dirección está convencida de que la Seguridad Informática no hace al negocio de la compañía.
- Cada vez los riesgos y el impacto en los negocios son mayores.
- No se puede dejar de hacer algo en este tema.



Algunos datos:

Según una encuesta del Departamento de Defensa de USA:

Sobre aprox. 9.000 computadores atacados,
7.900 fueron dañados.

400 detectaron el ataque.

Sólo 19 informaron el ataque.



Algunas realidades:

En mi compañía ya tenemos seguridad porque ...

... implementamos un firewall.

... contratamos una persona para el área.

... en la última auditoría de sistemas no me sacaron observaciones importantes.

... ya escribí las políticas.

... hice un penetration testing y ya arreglamos todo.



Qué Información proteger?

- en formato electrónico / magnético / óptico
- en formato impreso
- en el conocimiento de las personas



Principales riesgos y su impacto en los negocios



Principales riesgos y el impacto en los negocios:

- Desde cualquier PC *fuera* de la Compañía se puede tomar control de cualquier PC *dentro* de la Compañía.
- Alguien puede mandar e-mails en nombre de otro.
- En minutos, cualquier usuario puede conocer las contraseñas.
- Los e-mails y documentos pueden ser “consultados y modificados” en cualquier punto de la red.
- Cualquier usuario puede infectar con virus la red de la Compañía.
- La mayor parte de los fraudes son a través del uso de los sistemas.
- Cualquier hacker puede dejar los sistemas sin servicios.
- Una compañía puede ser enjuiciada por incumplimiento de leyes y reglamentaciones (Habeas Data, Propiedad Intelectual).



Principales riesgos y el impacto en los negocios:

- Se pueden robar o extraviar computadoras portátiles con información crítica.
- Se puede acceder indebidamente a las redes a través de Internet o vía MODEM.
- Las comunicaciones satelitales pueden ser interceptadas.
- Los equipos informáticos pueden sufrir caídas o destrucciones.
- Ciertos programadores pueden desarrollar programas tipo “bomba”.
- Pueden existir programas tipo “troyanos” para capturar información sensible.
- Puede haber “escuchas” de comunicaciones telefónicas de voz y de datos.



Principales riesgos y el impacto en los negocios:

- Los comprobantes legalmente requeridos pueden no estar disponibles.
- La información impresa puede ser copiada.
- En los sistemas de la Compañía se mantiene información no apropiada.
- En los equipos puede haber software no licenciado.
- La propiedad de la información y desarrollo a favor de la Compañía puede no estar asegurada.
- El personal contratado puede no tener los mismos niveles de seguridad en sus equipos.
- Algunos empleados y terceros pueden no mantener contratos de confidencialidad.



Principales riesgos y el impacto en los negocios:

- Los soportes de la información pueden ser robados o destruidos.
- Se puede distribuir información alterada a socios, accionistas, auditores y entes de contralor.
- Se puede no disponer de la información en el momento adecuado.
- Puede haber envíos de mails “anónimos” con información crítica o con agresiones.
- Se pueden distribuir datos que atenten contra la privacidad de los empleados.
- Se puede obtener la documentación impresa de la basura.
- Alguien puede acceder a la información no recogida de las impresoras.



Principales riesgos y el impacto en los negocios:

En estos tipos de problemas es difícil:

- Darse cuenta que pasan, hasta que pasan.
- Poder cuantificarlos económicamente, por ejemplo ¿cuánto le cuesta a la compañía 4 horas sin sistemas?
- Poder vincular directamente sus efectos sobre los resultados de la compañía.



Principales riesgos y el impacto en los negocios:

Se puede estar preparado para que ocurran lo menos posible:

- sin grandes inversiones en software
- sin mucha estructura de personal

Tan solo:

- ordenando la Gestión de Seguridad
- parametrizando la seguridad propia de los sistemas
- utilizando herramientas licenciadas y libres en la web



Normas aplicables:

Entre los distintos organismos relacionados comercial y/o institucionalmente con los temas de Seguridad de la Información, podemos encontrar los siguientes:

- Information Systems and Audit Control Association - ISACA: COBIT
- British Standards Institute: BS
- International Standards Organization: Normas ISO
- Departamento de Defensa de USA: Orange Book
- ITSEC – Information Technology Security Evaluation Criteria: White Book
- Sans Institute



Normas aplicables:

Information Systems and Audit Control Association - ISACA

COBIT

Control Objectives for Information and Related Technology

Misión del COBIT

- Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.



Normas aplicables:

Este organismo emite las COBIT AUDIT GUIDELINES, que:

- Son estándares internacionalmente aceptados para la práctica de seguridad informática, definidos por la Information Systems and Audit Control Association – ISACA.
- Comprenden una serie de Objetivos de Control a cumplir en los distintos aspectos del “gobierno” de IT, dentro de los cuales se encuentran los temas específicos de Seguridad y Control:
 - ➔ Planeación y organización
 - ➔ Adquisición e implementación
 - ➔ Entrega de servicios y soporte
 - ➔ Monitoreo



Normas aplicables:

British Standards Institute

- Emitió el BS Code of Practice for Information Security Management (BS 7799), con un conjunto de estándares internacionalmente aceptados para la práctica de seguridad informática, sobre los que luego se basaron para la emisión de la Norma ISO 17.799.



Normas aplicables:

International Standards Organization: Normas ISO

- La principal norma de Evaluación e Implementación de medidas de Seguridad en Tecnologías de la Información es la NORMA ISO 17799.
- Está organizada en diez capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema.



Normas aplicables:

Departamento de Defensa de USA: Orange Book

- Proporciona una base para la evaluación de la eficacia de los controles y de la seguridad en los recursos informáticos de procesamiento de datos.
- Tiene distintas categorías de clasificación según los requerimientos que cumpla cada recurso informático.

Tiene distintas categorías de clasificación:

→ D	Minimal Security	Not provide security features
→ C1	Discretionary Protection	No accountability or types of access
→ C2	Controlled access protection	Accountability of individual users, ACL, Audit events
→ B1	Labeled Protection	Mandatory access controls, labeling requirements
→ B2	Mandatory Protection	Labels include devices
→ B3	Security Domains	Highly resistant to penetration
→ A	Verified Protection	Trusted distribution



Normas aplicables:

ITSEC – Information Technology Security Evaluation Criteria

- Estándar publicado en Alemania conocido como el White Book de Europa, que sirve de estándar de seguridad para Information Security en países europeos.



Normas aplicables:

SANS Institute

- Organización que nuclea a los Administradores de Seguridad y que emite documentación relacionada con riesgos de Seguridad y los mecanismos técnicos para combatirlos y para mitigarlos.



Normas aplicables:

CIRT (Computer Incident Response Team)

- Los CIRTs son organizaciones dedicadas al análisis de Incidentes. El objetivo de estas organizaciones es crear una comunidad de rápida respuesta ante incidentes de seguridad informática, brindando servicios de alerta temprana, llevando estadísticas de los ataques más frecuentes y brindando recomendaciones para hacer las redes más seguras. Estos centros se alimentan de los incidentes de seguridad de distintos usuarios en el mundo.



Gestión de Seguridad Norma ISO 17799



Normas de Gestión ISO

International Standards Organization:
Normas ISO

- ISO 9001 – Calidad
- ISO 14001 – Ambiental
- ISO 17799 – Seguridad de la Información
- La principal norma de Evaluación e Implementación de medidas de Seguridad en Tecnologías de la Información es la NORMA ISO 17799.
- Basada en el BRITISH STANDARD 7799.
- ISO (Europa) y NIST (USA).



Norma ISO 17799 Seguridad de la Información

Dos partes:

- 17799 – 1 . NORMALIZACION (Mejores Prácticas)

Homologada en Argentina IRAM/ISO/IEC 17799

- 17799 – 2 . CERTIFICACION

Aún no fue publicada por ISO.

Hoy en día las certificaciones son sobre el BS 7799.



Norma ISO 17799 Seguridad de la Información

Está organizada en diez capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema para llevar adelante una correcta:

GESTION DE SEGURIDAD DE LA INFORMACION

Alcance

- Recomendaciones para la gestión de la seguridad de la información
- Base común para el desarrollo de estándares de seguridad



Norma ISO 17799 Seguridad de la Información

Preservar la:

- **confidencialidad:**
accesible sólo a aquellas personas autorizadas a tener acceso.
- **integridad:**
exactitud y totalidad de la información y los métodos de procesamiento.
- **disponibilidad:**
acceso a la información y a los recursos relacionados con ella toda vez que se requiera.



Norma ISO 17799 Seguridad de la Información

Dominios:

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento



Qué es la Seguridad de la Información?

La información = activo comercial

Tiene valor para una organización y por consiguiente debe ser debidamente protegida.

“Garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades”

“La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados”



Formas o medios que se distribuye o almacena:

- Impresa,
- escrita en papel,
- almacenada electrónicamente,
- transmitida por correo o utilizando medios electrónicos,
- presentada en imágenes, o
- expuesta en una conversación.



Gestión de Seguridad de la Información

Implementando un conjunto adecuado de CONTROLES:

- Políticas
- Prácticas
- Procedimientos
- Estructuras Organizacionales
- Funciones del Software



Cómo establecer los requerimientos de Seguridad?

● Evaluar los riesgos:

- ➔ se identifican las amenazas a los activos,
- ➔ se evalúan vulnerabilidades y probabilidades de ocurrencia, y
- ➔ se estima el impacto potencial.

● Requisitos legales, normativos, reglamentarios y contractuales que deben cumplir:

- ➔ la organización,
- ➔ sus socios comerciales,
- ➔ los contratistas y los prestadores de servicios.

● Conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.



Selección de controles:

“Los controles pueden seleccionarse sobre la base de la Norma ISO 17799, de otros estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda”

Costo de implementación vs riesgos a reducir y las pérdidas monetarias y no monetarias

Revisiones periódicas de:

- Riesgos
- Controles implementados



Selección de controles:

- Controles “esenciales” desde el punto de vista legal:
 - protección de datos y confidencialidad de información personal
 - protección de registros y documentos de la organización
 - derechos de propiedad intelectual

- Controles considerados como “práctica recomendada” de uso frecuente en la implementación de la seguridad de la información:
 - documentación de la política
 - asignación de responsabilidades en materia de seguridad
 - instrucción y entrenamiento
 - comunicación de incidentes relativos a la seguridad
 - administración de la continuidad de la empresa



Factores críticos del éxito:

- política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;
- una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;
- apoyo y compromiso manifiestos por parte de la gerencia;
- un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;
- comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;



Factores críticos del éxito:

- distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas;
- instrucción y entrenamiento adecuados;
- un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.



Dominio 1

Política de Seguridad



Dominio 1: POLITICA DE SEGURIDAD

Nivel gerencial debe:

- aprobar y publicar la política de seguridad
- comunicarlo a todos los empleados



Dominio 1: POLITICA DE SEGURIDAD

Debe incluir:

- objetivos y alcance generales de seguridad
- apoyo expreso de la dirección
- breve explicación de los valores de seguridad de la organización
- definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información
- referencias a documentos que puedan respaldar la política



Dominio 1: POLITICA DE SEGURIDAD



Dominio 1: POLITICA DE SEGURIDAD

Es política de la compañía:

● **Eficacia:**

Garantizar que toda la información utilizada es necesaria y útil para el desarrollo de los negocios.

● **Eficiencia:**

Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

● **Confiabilidad:**

Garantizar que los sistemas informáticos brindan información correcta para ser utilizada en la operatoria de cada uno de los procesos.



Dominio 1: POLITICA DE SEGURIDAD

● Integridad:

Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de los negocios en cada uno de los sistemas informáticos y procesos transaccionales.

● Exactitud:

Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

● Disponibilidad:

Garantizar que la información y la capacidad de su procesamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los negocios.



Dominio 1: POLITICA DE SEGURIDAD

● Legalidad:

Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito.

● Confidencialidad:

Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.



Dominio 1: POLITICA DE SEGURIDAD

● Autorización:

Garantizar que todos los accesos a datos y/o transacciones que los utilicen cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

● Protección Física:

Garantizar que todos los medios de procesamiento y/o conservación de información cuentan con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

● Propiedad:

Asegurar que todos los derechos de propiedad sobre la información utilizada por todos sus empleados en el desarrollo de sus tareas, estén adecuadamente establecidos a favor de la compañía.

