

WALC 2004 Track 6

Seguridad Informática



Políticas de Seguridad

Juan Luis Chaves Sanabria

Centro Nacional de Cálculo Científico – CeCaCULA

Universidad de Los Andes

Mérida - Venezuela



Introducción

- **Organizaciones y la sociedad del conocimiento**
 - Los sistemas basados en tecnologías de la información cumplen un rol clave en la consecución de la misión de una organización.

- **¿ Qué es un sistema basado en tecnologías de la información ?**
 - Es todo sistema de soporte general (computador, infraestructura de red, *Internet*) o aplicación que se ejecute sobre un sistema de soporte general, empleando datos e información, para generar conocimiento que satisface un conjunto de requerimientos específicos

(Definición propuesta por el NIST en el documento *Risk Management Guide for Information Technology Systems*)



Introducción (2):

- ¿ Cómo garantizar que el conocimiento producido es seguro, confiable y oportuno ?
Depende de la "calidad" de:
 - los datos e información,
 - sistemas de soporte general y
 - Aplicacionesutilizados en su generación.

- La "calidad" de estos componentes de un sistema basado en tecnologías de información (*IT System*) se mide en base a tres objetivos de seguridad:
 - Confidencialidad
 - Integridad
 - Disponibilidad



Objetivos de Seguridad:

- **Confidencialidad:** Los datos sólo deben ser conocidos y accedidos por quienes estén debidamente autorizados
 - Debe protegerse la data de lecturas no autorizadas durante su almacenamiento, procesamiento o transmisión
- **Integridad:** Los datos sólo pueden ser modificados y/o eliminados por quienes estén autorizados para ello y los sistemas y aplicaciones sólo deben ser operados por personal autorizado
 - Debe protegerse la data, los sistemas y las aplicaciones contra intentos, accidentales o intencionales, de su manipulación no autorizada. Esto incluye: *Autenticidad, No repudiación y Contabilidad*
- **Disponibilidad:** Los sistemas que albergan datos e información deben garantizar que sólo podrán accederse, cuando así se requiera, por quienes tienen derecho a ello
 - Debe protegerse la data, los sistemas y las aplicaciones contra cualquier forma no autorizada de impedir o retardar su acceso u operación



Cómo alcanzar los objetivos de seguridad:

- **Basándose en las directrices propuestas en el estándar internacional ISO/IEC 17799:2000 *"Code of practice for information security management"*.**
 - Presenta un conjunto de asuntos, tópicos y prácticas que deben considerarse al momento de introducir, implementar o mantener la gestión de la seguridad de la información en una organización.
 - Desarrollado por *the British Standards Institution* como BS 7799-1
- ***ISO (International Organization for Standardization)*
*IEC (International Electrotechnical Commission)***
 - Conforman el sistema especializado para el desarrollo de estándares que tienen validez internacional
 - Desarrollan estándares adoptados y aceptados a nivel mundial



¿Qué tópicos cubre ISO/IEC 17799:2000?

- Recomienda prácticas dentro de una organización para tener y gestionar la:
 - Política de Seguridad de la Información
 - Estructuración del Proceso de Seguridad
 - Clasificación y Control de Activos de la Organización
 - Seguridad Personal
 - Seguridad Física y Ambiental
 - Gestión de las Comunicaciones y de las Operaciones
 - Control de Acceso
 - Desarrollo y Mantenimiento de sistemas
 - Gestión de la Continuidad del Negocio
 - Cumplimiento con el Marco Jurídico



1 Política de seguridad de la información

- **Objetivo:** Proporcionar directrices que soporten y orienten el proceso de seguridad de la información en la organización.
- Documento con las políticas de seguridad de la información.
 - Expresa el enfoque de la organización para manejar y controlar la seguridad de la información que posee.
 - Este documento *debe* ser aprobado por la gerencia de la organización y *debe* asegurarse su comunicación a todos los empleados de la organización
- Revisión y evaluación periódica de las políticas.
 - Asegurar su adecuación a las expectativas de seguridad de la información de la organización



1 Política de seguridad de la información

- ¿Qué debe incluir el documento?
 - Una definición de seguridad de la información, su alcance y objetivos y su importancia para garantizar el cumplimiento de la misión de la organización.
 - Factores que intervienen:
 - Servicios ofrecidos (y sus riesgos) vs. Seguridad proporcionada (nivel de seguridad)
 - Facilidad de uso vs. Seguridad
 - Costos de la seguridad (monetario, rendimiento) vs. Riesgos (perdida de confidencialidad, integridad y disponibilidad).
 - Determinarán que tan seguros o protegidos están los activos de información de una organización.
 - El éxito de un política de seguridad depende de sus objetivos, no de las herramientas utilizadas para implantar la política.
 - Imprescindible para poder seleccionar las herramientas de seguridad a utilizar.



1 Política de seguridad de la información

- ¿Qué debe incluir el documento? (2)
 - Las reglas , normas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre:
 - Los sistemas de soporte general y los elementos físicos asociados con éstos (computadores, dispositivos de interconexión edificación, impresoras, discos, cables, etc.),
 - el software y la información almacenada en tales sistemas.
 - los usuarios del sistema



1 Política de seguridad de la información

□ ¿Qué debe incluir el documento? (3)

Basados en los principios propuestos en el *RFC 1244 "Site Security Handbook"*.

- Una política de confidencialidad
- Una política de autenticación
- Una política de acceso
- Una política de contabilidad
- Planes para satisfacer las expectativas de disponibilidad de los recursos del sistema
- Una política de mantenimiento para la red y los sistemas de la organización
- Directrices para identificar y adquirir tecnología con rasgos de seguridad requeridos y/o deseables.
- Sanciones para quien infrinjan la política de seguridad
- Una política de reporte de incidentes y de divulgación de información



1 Política de seguridad de la información

- Revisión y evaluación de las políticas de seguridad de la información
 - La política de seguridad debe tener un responsable quien se encarga de su mantenimiento y revisión de acuerdo a un proceso predefinido que debe:
 - Ejecutarse periódicamente para evaluar la efectividad de las políticas en cuanto a: a) la naturaleza, cantidad e impacto de los incidentes reportados y b) el costo e impacto de los controles sobre la efectividad del negocio.
 - Ejecutarse cada vez que ocurra un evento que afecte el la seguridad de la información: nuevas vulnerabilidades, cambios en la infraestructura técnica u organizacional, ocurrencia de un incidente de seguridad significativo



1 Política de seguridad de la información

- ¿ Qué es un riesgo para un activo en tecnologías de la información ?
 - Es la probabilidad de que se explote, intencional o accidentalmente, una debilidad del activo con un efecto o impacto negativo sobre la misión de la organización en la cual se localiza.

- ¿ Cómo se identifican y valoran los riesgos de daño sobre los activos de información de una organización ?
 - A través de un proceso de valuación del riesgo



1 Política de seguridad de la información

□ ¿Cómo abordar el proceso de valuación del riesgo?

(De acuerdo al documento *Risk Management Guide for Information Technology Systems* del NIST)

1. Caracterización del sistema y su entorno
2. Identificar las amenazas: de qué o de quién deben protegerse (*Threats*)
3. Explorar las formas en las cuales pueden hacerse efectivas las amenazas. (Vulnerabilidades)
4. Analizar las medidas de protección existentes y planificadas
5. Determinar la probabilidad de ocurrencia de cada *Threat*
6. Analizar el impacto de las *Threats*
7. Determinación del riesgo
8. Recomendaciones de controles de seguridad
9. Documentación de los resultados



1 Política de seguridad de la información

1. Caracterización del sistema y su entorno:

Identificar todas las cosas que pueden ser afectadas por un problema de seguridad (activos de información):

- **Gente:** usuarios, administradores, técnicos.
- **Datos e Información:** en ejecución, en línea, almacenada, respaldos, bases de datos, procesos en ejecución.
- **Software:** programas fuente, paquetes, bibliotecas, sistemas operativos, aplicaciones, servicios.
- **Hardware:** CPUs, dispositivos de interconexión, discos, líneas de comunicación, estaciones de trabajo, discos.
- **Documentación:** configuración de servicios, procedimientos administrativos, equipos, programas.
- **Accesorios:** papel, cartuchos de impresión, cartuchos de respaldo.



1 Política de seguridad de la información

2. Identificar las amenazas: de qué o de quién deben protegerse (*Threats*)

- Las amenazas se identifican y estudian de acuerdo al impacto que pueden causar sobre los bienes a proteger
 - Usuarios afectados
 - Importancia de la información que puede verse comprometida
- El impacto es variable y depende de la naturaleza del organismo que esté realizando el proceso de análisis de riesgo (militar, académico, científico)



1 Política de seguridad de la información

2. Identificar las amenazas: de qué o de quién deben protegerse (*Threats*) (2)

Clase de Threat	Activo de Información Afectado	Acción o ejecución de la Threat
Ambiente de operación	Toda la información digital	Suspensión servicio eléctrico
Humana Accidental	Registro de Proveedores	Ingeniería Social
Hardware	Los que interactuaban o estaban almacenados en el sistema	Falla del sistema
Hacker, Cracker	Sistema en desarrollo	Acceso no autorizado



1 Política de seguridad de la información

3. Explorar las formas en las cuales pueden hacerse efectivas las amenazas. (Vulnerabilidades)

Vulnerabilidad	Activo de Información Afectado	Acción o ejecución de la Threat
No disponer de UPS	Toda la información digital	Suspensión servicio eléctrico
Ausencia / Falta de entrenamiento	Registro de Proveedores	Ingeniería Social
Ausencia / Falta de mantenimiento	Los que interactuaban o estaban almacenados en el sistema	Falla del sistema
Debilidades en el diseño de seguridad del sistema	Sistema en desarrollo	Acceso no autorizado



1 Política de seguridad de la información

4. Analizar las medidas de protección existentes y planificadas

- Listado de todos los controles:

- Técnicos,
- Operacionales y
- de Gestión

Aplicados o planificados para aplicar dentro de la organización

- La consideración de estos controles en el proceso de avalúo del riesgo disminuirá la probabilidad de ocurrencia de una amenaza



1 Política de seguridad de la información

5. Determinar la probabilidad de ocurrencia de cada *Threat*:

- Está influenciada por:
 - La naturaleza de la vulnerabilidad que puede explotarse
 - La motivación o capacidad del atacante
 - Efectividad y existencia de controles para neutralizar la vulnerabilidad



1 Política de seguridad de la información

5. Determinar la probabilidad de ocurrencia de cada *Threat* (2):

- Los estadios o valores de probabilidad pueden adecuarse a los criterios definidos en cada organización.
- En el documento del NIST se proponen 3 niveles:

Alto	Atacante altamente motivado y capaz
Medio	Atacante motivado y capaz, pero presencia de controles que pueden impedir el éxito del ataque
Bajo	Atacante carece de motivación o capacidad, o existen controles para prevenir el éxito del ataque



1 Política de seguridad de la información

6. Analizar el impacto de las *Threats*

- Para proponer una escala que exprese el grado de incidencia negativa que cada una de ellas puede tener sobre la misión de la organización o los objetivos de seguridad.

Alto	(1) Pérdida de activos o recursos altamente costosos (2) Significativamente violar, estropear o impedir la misión de una organización (3) Generar muertes humanas o heridos graves
Medio	(1) Pérdida de activos o recursos costosos (2) Pudiera violar, estropear o impedir la misión de una organización (3) Puede generar heridos humanos leves
Bajo	(1) Pudiera resultar en la pérdida de algún activo o recurso (2) Pudiera afectar notablemente la misión, reputación o interés de una organización



1 Política de seguridad de la información

7. Determinación del riesgo

- En este paso se obtiene la valoración del nivel del riesgo para el sistema evaluado. Para cada par *Threat/Vulnerabilidad* identificado se le puede calcular el riesgo en función de:
 - Probabilidad de ocurrencia del par *Threat/Vulnerabilidad*
 - Magnitud del impacto de la ocurrencia del par *Threat/Vulnerabilidad*
 - La pertinencia de los controles de seguridad existentes o planificados para disminuir o neutralizar el riesgo de la ocurrencia del par *Threat/Vulnerabilidad*



1 Política de seguridad de la información

7. Determinación del riesgo (2):

Matrix nivel-riesgo

		Impacto	
Probabilidad de ocurrencia del par <i>Threat/Vulnerabilidad</i>	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	Bajo $10 \times 1.0 = 10$	Medio $50 \times 1.0 = 50$	Alto $100 \times 1.0 = 100$
Medio (0.5)	Bajo $10 \times 0.5 = 5$	Medio $50 \times 0.5 = 25$	Medio $100 \times 0.5 = 50$
Bajo (0.1)	Bajo $10 \times 0.1 = 1$	Bajo $50 \times 0.1 = 5$	Bajo $100 \times 0.1 = 10$



1 Política de seguridad de la información

7. Determinación del riesgo (3):

A partir de la matrix nivel-riesgo se obtiene la escala del riesgo y los niveles de riesgo

Nivel de Riesgo	Acciones a ejecutar
Alto ($>50 \leq 100$)	Imperiosa necesidad de ejecutar acciones correctivas. Debe ponerse en ejecución un plan de acción correctivo lo mas pronto posible
Medio ($>10 \leq 50$)	Acciones correctivas son necesarias y debe desarrollarse un plan para ejecutar esas acciones dentro de un periodo de tiempo percedero
Bajo ($\geq 1 \leq 10$)	La autoridad designada de aprobación (DAA) del sistema evaluado (activo) debe decidir si se requieren acciones correctivas o se asume el riesgo



1 Política de seguridad de la información

8. Recomendaciones de controles de seguridad

- Para reducir el nivel de riesgo identificado y determinado
- Los controles deben ser recomendados tomando en cuenta los siguientes factores:
 - Efectividad (compatibilidad)
 - Legislación y normas regulatorias
 - Políticas de seguridad organizacional
 - Impacto operacional (rendimiento)
 - Confiabilidad y ausencia de vulnerabilidades



1 Política de seguridad de la información

9. Documentación de los resultados:

- A través de un reporte de apoyo a la gerencia para entender los riesgos presentes en el sistema y soportar las decisiones de apartar recursos para reducir o corregir potenciales perdidas.
- El reporte de valuación de los riesgos debe contener y describir:
 - las amenazas (*threats*) y vulnerabilidades identificadas,
 - las medidas de riesgo y
 - las recomendaciones de los controles que contribuirían a mitigar los niveles de riesgo detectados.



2 Estructuración del Proceso de Seguridad:

□ **Objetivos:**

- Gestionar la seguridad de la información dentro de la organización
- Mantener la seguridad de las facilidades de procesamiento de la información organizacional y de los activos de información que son accedidos por terceros
- Preservar la seguridad de la información cuando la responsabilidad para el procesamiento de la información ha sido contratado a otra organización (*tercerización u outsourcing*).



2 Estructuración del Proceso de Seguridad:

- Gestionar la seguridad de la información dentro de la organización
 - Debe establecerse un marco de trabajo de gestión para iniciar y controlar el proceso de seguridad de la información dentro de la organización.
 - Establecer un foro de gestión de seguridad de la información
 - Establecer un ente coordinador de todos los aspectos relativos a la implementación de controles para la seguridad de la información.
 - Definir y delimitar roles y responsabilidades en cuanto a la seguridad de la información
 - Establecer procedimientos de autorización para la adopción de facilidades de procesamiento de información



2 Estructuración del Proceso de Seguridad:

- Gestionar la seguridad de la información dentro de la organización (2)
 - Debe establecerse un marco de trabajo de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. (2)
 - Designar o identificar un consejero especialista en seguridad de la información
 - Promover la cooperación entre organizaciones
 - Asegurar la revisión independiente o externa de la implementación de las políticas de seguridad de la información



2 Estructuración del Proceso de Seguridad:

- Mantener la seguridad de las facilidades de procesamiento de la información organizacional y de los activos de información que son accedidos por terceros
 - Cuando el acceso de terceros a los activos de información es una necesidad del negocio, una evaluación y análisis de riesgos debe realizarse para determinar las implicaciones de seguridad y los controles que son requeridos
 - Los requerimientos y controles de seguridad deben ser acordados y definidos en los contratos formales con los terceros



2 Estructuración del Proceso de Seguridad:

- Preservar la seguridad de la información cuando la responsabilidad para el procesamiento de la información ha sido contratado a otra organización (tercerización u *outsourcing*).

Acuerdos de *outsourcing* deben contener los riesgos, controles y procedimientos de seguridad para los sistemas de información, redes y ambientes de escritorio u oficina de la organización cuyo control y gestión es cedido.

- Requerimientos de seguridad en contratos de *outsourcing*
 - **Debe contener qué y cómo serán garantizados los requerimientos de seguridad.**



3 Clasificación y control de activos de la organización:

□ Objetivos:

- Mantener una protección adecuada de los activos de la organización
- Asegurar que los activos de información reciben un nivel apropiado de protección.



3 Clasificación y control de activos de la organización:

- Mantener una protección adecuada de los activos de la organización.
 - Inventario de activos: Claramente identificados, con su respectivo responsable y su valor e importancia
 - **Activos de información:** bases de datos, archivos, documentación de los sistemas, manuales de usuario, procedimientos de soporte y operacionales, etc.
 - **Activos de software:** aplicaciones, sistemas operativos, herramientas de desarrollo y utilidades.
 - **Activos físicos:** equipos de computación y comunicación, medios magnéticos, estantes, ups.
 - **Servicios:** electricidad, iluminación, telefonía.



3 Clasificación y control de activos de la organización:

- ❑ Asegurar que los activos de información reciben un nivel apropiado de protección.
 - Los activos de información deben clasificarse para indentificar sus necesidades, prioridades y grados de protección.
- ❑ Directivas para la clasificación:
 - Qué tan crítica es la información en términos de disponibilidad, integridad y confidencialidad (puede variar en el tiempo)
 - La clasificación de un item y su revisión periódica dentro de la escala siempre debe realizarla el responsable del mismo



3 Clasificación y control de activos de la organización:

- Asegurar que los activos de información reciben un nivel apropiado de protección. (2)
 - Manejo y etiquetado de la información:
 - Deben definirse un conjunto de procedimientos en concordancia con el esquema de clasificación adoptado por la organización
 - Los procedimientos deben cubrir los siguientes tipos de actividades de procesamiento:
 - Copiado
 - Almacenado
 - Transmisión por vía física o electrónica
 - Transmisión por conversación (incluyendo telefonía móvil, buzón de voz, máquinas contestadoras)
 - Destrucción



3 Clasificación y control de activos de la organización:

- Asegurar que los activos de información reciben un nivel apropiado de protección. (3)
 - Manejo y etiquetado de la información:
 - **Salidas o respuestas de sistemas conteniendo información clasificada como crítica deben marcarse con una etiqueta adecuada dentro de su contenido**



4 Seguridad Personal:

□ Objetivos:

- Reducir los riesgos de error humano, hurto, fraude o mal uso de las facilidades que procesan información
- Asegurar que los usuarios son concientes de las amenazas a la seguridad de la información, que deben involucrarse en su protección y que son preparados y equipados para cumplir con la política de seguridad corporativa dentro de sus actividades diarias en el trabajo
- Minimizar el daño provocado por incidentes de seguridad o por mal funcionamiento de los sistemas y aprender de tales incidentes



4 Seguridad Personal:

- Reducir los riesgos de error humano, hurto, fraude o mal uso de las facilidades que procesan información
 - Incluir en los contratos de personal la seguridad de la información en las responsabilidades generales y específicas del trabajo
 - Adoptar políticas de selección, supervisión y promoción de personal. Especialmente para aquellos que manejarán información sensible.
 - Establecer todos los términos y condiciones de los empleos relacionados con la seguridad de la información. Incluyendo responsabilidades después de cesar la relación laboral y las acciones a tomar en caso de ser desanteadidos.
 - Establecer acuerdos de confidencialidad como parte de las condiciones de empleo



4 Seguridad Personal:

- Asegurar que los usuarios son concientes de las amenazas a la seguridad de la información, que deben involucrarse en su protección y que son preparados y equipados para cumplir con la política de seguridad corporativa dentro de sus actividades diarias en el trabajo
 - Educar y entrenar en seguridad de la información: políticas, procedimientos, responsabilidades legales, controles
 - Educar y entrenar en el uso adecuado y correcto de las facilidades de procesamiento de la información para evitar posibles riesgos de seguridad



4 Seguridad Personal:

- Minimizar el daño provocado por incidentes de seguridad o por mal funcionamiento de los sistemas y aprender de tales incidentes
 - Asegurar que todos los empleados y terceros conozcan el uso de los procedimientos establecidos para reportar y responder a incidentes de seguridad (huecos, amenazas, debilidades o mal funcionamiento) rápidamente.
 - Los procedimientos deben incluir a quien contactar y las medidas a ser tomadas por quien detectó el incidente y por quien recibió el reporte
 - Aprendizaje de los incidentes. Sirven para justificar controles adicionales y en el proceso de revisión de las políticas de seguridad
 - Procesos disciplinarios para quienes infrinjan políticas y procedimientos de seguridad



5 Seguridad Física y Ambiental:

□ Objetivos:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización
- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio.
- Prevenir el compromiso o robo de información y de las facilidades de procesamiento de información



5 Seguridad Física y Ambiental:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización
 - Segurización física del perímetro alrededor de las posesiones y facilidades de procesamiento de la información con el objeto de controlar el acceso y prevenir eventos naturales como inundaciones e incendios
 - Adopción de controles de entrada a áreas físicas sensibles:
 - Accesos deben seguir un procedimiento: justificación de ingreso para propósitos permitidos, registro de ingreso y salida, dar a conocer las instrucciones sobre las normas de seguridad en el área y sobre los procedimientos de emergencia



5 Seguridad Física y Ambiental:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización (2)
 - Adopción de controles de entrada a áreas físicas sensibles: (2)
 - Accesos a información sensitiva y a las facilidades de procesamiento de información debe ser controlada y restringida a personal autorizado por medio de mecanismos de autenticación adecuados y herramientas de auditoría de accesos.
 - Uso obligatorio de alguna forma de identificación visible y conminar a quien no la lleve puesta a que la presente y coloque
 - Derechos de acceso a áreas seguras deben ser revisados regularmente y actualizados.



5 Seguridad Física y Ambiental:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización (3)
- Aseguramiento de oficinas, cuartos y facilidades:
 - Deben ser dispuestas facilidades de acceso para evitar ingreso del público
 - Los edificios deben dar la mínima indicación de las facilidades de procesamiento de información en ellos alojadas
 - Equipo de soporte (faxes, fotocopiadoras, etc) deben ubicarse apropiadamente para evitar el ingreso a áreas seguras
 - Puertas y ventanas desatendidas deben ser selladas y protecciones externas deben ser consideradas para las ventanas



5 Seguridad Física y Ambiental:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización (4)
 - Aseguramiento de oficinas, cuartos y facilidades: (2)
 - Sistemas de detección de intrusos deben ser dispuestos para cubrir todas las puertas y ventanas externas accesibles, áreas no ocupadas y en las salas de máquinas y comunicaciones
 - Facilidades de procesamiento de información manejadas por la organización deben estar físicamente separadas de aquellas manejadas por terceros
 - Los directorios internos donde se localizan activos críticos no deben ser accesibles por el público
 - Equipos de respaldo y restauración deben localizarse en lugares distintos a donde se encuentran las facilidades que soportan



5 Seguridad Física y Ambiental:

- ❑ Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización (5)
 - Trabajando en áreas seguras:
 - ❑ Personal debe enterarse de las actividades dentro de un área segura a medida que sea necesario conocerlo
 - ❑ Evitar trabajo no supervisado en áreas seguras
 - ❑ Areas seguras sin ocupar deben ser físicamente bloqueadas y revisadas periódicamente
 - ❑ Acceso de personal de terceros debe ser autorizado sólo cuando está justificado o es requerido. Este tipo de acceso debe ser autorizado y vigilado
 - ❑ Cualquier equipo de grabación (camara, video, audio, etc) no debe ser permitido, a menos que sea autorizado



5 Seguridad Física y Ambiental:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización (6)
- Aislamiento de las áreas de carga y despacho:
 - Áreas de carga y despacho deben ser vigiladas y, preferiblemente, aisladas de los activos de información para evitar accesos no autorizados
 - Material que se recibe debe ser inspeccionado y registrado para identificar riesgos potenciales



5 Seguridad Física y Ambiental:

- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio.
- Ubicación y protección del equipamiento:
 - Debe ubicarse en áreas que minimicen el acceso innecesario
 - Controles deben ser adoptados para minimizar el riesgo de amenazas potenciales como: robo, fuego, explosiones, humo, inundaciones, polvo, vibraciones, interferencias electromagnéticas.
 - Establecer políticas sobre comer, beber y fumar cerca de los activos de información
 - Acondicionamiento y vigilancia de las condiciones ambientales en donde están ubicados los equipos



5 Seguridad Física y Ambiental:

- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio (2)
- **Provisión de energía eléctrica:**
 - Equipamiento debe ser protegido contra fallas de servicio y otras anomalías eléctricas
 - Cualquiera de las opciones que se adopten para garantizar la continuidad del servicio eléctrico, deben ser regularmente revisadas y probadas para garantizar el adecuado funcionamiento de tales equipos
- **Seguridad del cableado eléctrico y de telecomunicaciones:**
 - Deben ser protegidos contra interferencia y daños
 - Adoptar medios de transmisión alternativos y redundantes



5 Seguridad Física y Ambiental:

- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio (3)
 - Mantenimiento del equipamiento:
 - Equipamiento debe ser puesto en mantenimiento de acuerdo a las especificaciones e intervalos de servicio recomendados por el proveedor
 - Únicamente personal autorizado puede llevar a cabo las reparaciones y el servicio de mantenimiento
 - Deben llevarse registros de todas las fallas ocurridas, así como de las sospechas. Igualmente con todo el mantenimiento preventivo y correctivo realizado
 - Controles y medidas de respaldo deben ser tomadas cuando algún equipo debe ser trasladado para mantenimiento



5 Seguridad Física y Ambiental:

- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio (4)
 - Seguridad en traslado de equipos fuera de la organización:
 - Deben estar bajo constante vigilancia en lugares públicos
 - Deben seguirse las recomendaciones de los fabricantes para el traslado de equipos
 - Normas y controles para el traslado de equipos hacia el hogar de los empleados deben ser definidas
 - Deben adquirirse pólizas con cobertura adecuada para cubrir equipos fuera de la organización
 - Disposición o re-uso seguro del equipamiento:
 - Debe asegurarse que toda información o software sensible sea removido de manera irrecuperable.



5 Seguridad Física y Ambiental:

- Prevenir el compromiso o robo de la información y de las facilidades de procesamiento de la información
 - Política de escritorios y pantallas vacías para reducir el riesgo de acceso no autorizado, pérdida o daño de la información
 - Dispositivos de comunicación desatendidos como fax, telex y teléfonos deben ser protegidos.
 - Fotocopiadoras deben ser bloqueadas para evitar su uso fuera del horario establecido o por personas no autorizadas
 - Establecer mecanismos de verificación de equipos que entran y salen de la organización para detectar apropiaciones indebidas o no autorizadas de la propiedad



6 Gestión de las operaciones y comunicaciones

□ Objetivos:

- Asegurar la operación correcta y segura de las facilidades de procesamiento de información
- Minimizar el riesgo de fallas del sistema
- Proteger la integridad del software y de la información
- Mantener la integridad y disponibilidad de los servicios de procesamiento de la información y comunicación
- Asegurar la protección de la información dentro de ambientes de redes y de su infraestructura de soporte
- Prevenir daño a los activos de información y la interrupción de las actividades del negocio
- Prevenir pérdida, modificación o manejo inadecuado de la información intercambiada entre organizaciones



6 Gestión de las operaciones y comunicaciones

- Asegurar la operación correcta y segura de las facilidades de procesamiento de información
 - Documentar los procedimientos de operación. Deben incluir instrucciones precisas para la ejecución de cada trabajo
 - Implementar controles para gestionar el cambio operacional de equipos, software o procedimientos
 - Establecer procedimientos y responsabilidades para el manejo eficiente y ordenado de incidentes de seguridad.
 - Deben cubrirse todos los tipos de incidentes de seguridad potenciales: fallas de los sistemas de información y pérdidas de servicio, negaciones de servicio, errores debido a datos del negocio incompletos o incorrectos, violación de la confidencialidad



6 Gestión de las operaciones y comunicaciones

- Asegurar la operación correcta y segura de las facilidades de procesamiento de información (2)
- Establecer procedimientos y responsabilidades para el manejo eficiente y ordenado de incidentes de seguridad. (2)
 - Deben incluirse procedimientos para identificar el incidente, planear la adopción de correctivos para prevenir su recurrencia, colección y preservación de evidencias, comunicación con los afectados o con los involucrados con la recuperación del incidente y para reportar el evento a la autoridad apropiada
 - Diseñar planes de contingencia para recuperar los servicios y sistemas lo mas rápido posible. Estos planes deben incorporar controles que permitan recrear todos los pasos que se siguieron en la recuperación del incidente



6 Gestión de las operaciones y comunicaciones

- Asegurar la operación correcta y segura de las facilidades de procesamiento de información (3)
 - Separación de trabajos o servicios para reducir las oportunidades de incurrir en errores por mal empleo de información o de facilidades de procesamiento.
 - Separación de las facilidades en desarrollo de las que están en producción (operación).
 - Reglas y normas para la transferencia de software en desarrollo a software operacional deben establecerse
 - Gestión del manejo de facilidades de procesamiento de información por externos
 - Controles deben acordarse con el contratado para reducir los riesgos de su actividad



6 Gestión de las operaciones y comunicaciones

- Minimizar el riesgo de fallas del sistema
 - Demandas de capacidad deben proyectarse para asegurar la disponibilidad de capacidad y de recursos adecuados cuando se requieran
 - Definición de criterios para la aceptación de los sistemas
- Proteger la integridad del *software* y de la información
 - Adoptar controles de detección y prevención contra software malicioso y no autorizado
- Mantener la integridad y disponibilidad de los servicios de procesamiento de la información y comunicación
 - Deben establecerse procedimientos de rutina para llevar a cabo la estrategia de respaldo acordada y para verificar que funciona correctamente



6 Gestión de las operaciones y comunicaciones

- Mantener la integridad y disponibilidad de los servicios de procesamiento de la información y comunicación (2)
 - Deben llevarse registros (*logs*) de las actividades del equipo de operaciones. Estos *logs* deben incluir:
 - Horas de entrada y salida del sistema
 - Errores del sistema y acciones correctivas tomadas
 - Confirmación del correcto manejo de los archivos de datos y salidas del sistema
 - El nombre del operador que hace el registro

Los logs se utilizarán para verificar el empleo correcto de los procedimientos de operación



6 Gestión de las operaciones y comunicaciones

- Mantener la integridad y disponibilidad de los servicios de procesamiento de la información y comunicación (3)
 - Deben llevarse registros (*logs*) de las fallas en el sistema.
 - Deben existir reglas claras para manejar fallas reportadas. Estas deben incluir:
 - Revisión de los *logs* de fallas para asegurar que han sido resueltas satisfactoriamente
 - Revisión de las medidas correctivas para asegurar que los controles no han sido comprometidos y que la acción tomada está completamente permitida



6 Gestión de las operaciones y comunicaciones

- Asegurar la protección de la información dentro de ambientes de redes y de su infraestructura de soporte
 - Procurar separar las operaciones de responsabilidad operacional de las redes de las operaciones sobre computadores (servicios)
 - Establecer responsabilidades y procedimientos para el manejo de equipos remotos en todas las áreas de la organización
 - Si son justificados por el análisis de riesgos, deben establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que atraviesan redes públicas.
 - Si la disponibilidad de los servicios de red y la conexión de los equipos es crítica, deben adoptarse medidas y controles para así garantizarlos



6 Gestión de las operaciones y comunicaciones

- Prevenir daño a los activos de información y la interrupción de las actividades del negocio
 - Manejo de medios de almacenamiento removibles (documentos, discos, cintas, *cassettes*, reportes)
 - Cada tipo de medio debe ser almacenado en un ambiente seguro en concordancia con los requerimientos del fabricante y de las normas de seguridad
 - Desecho de los medios de almacenamiento removibles
 - Para el caso de los medios de almacenamiento electrónicos, su contenido debe ser removido con métodos que impidan su recuperación
 - Picar, desmenuzar e incinerar son medios de disposición seguros
 - Deben llevarse registros de todos los desechos realizados, esto es para fines de auditoría (quien lo autorizó, etc)



6 Gestión de las operaciones y comunicaciones

- Prevenir daño a los activos de información y la interrupción de las actividades del negocio (2)
 - Establecer controles y procedimientos para el manejo y almacenamiento de la información con el objeto de evitar su exposición, compromiso o mal empleo.
 - Adoptar controles para proteger la documentación del sistema de accesos no autorizados
- Prevenir pérdida, modificación o manejo inadecuado de la información intercambiada entre organizaciones
 - Establecer controles y normas para proteger información en tránsito entre organizaciones
 - Los intercambios deben regirse en base a acuerdos que incluyan responsabilidades y el apego a cualquier legislación relevante (comercio electrónico, etc)



6 Gestión de las operaciones y comunicaciones

- Prevenir pérdida, modificación o manejo inadecuado de la información intercambiada entre organizaciones (2)
 - Asegurar la información publicada electrónicamente
 - Debe establecerse una política para el uso del correo electrónico y colocar controles para reducir los riesgos de seguridad generados por este servicio
 - Deben establecerse políticas, procedimientos y controles para proteger el intercambio de información a través del uso de cualquier facilidad de comunicación (voz, fax, video, chat, etc).



7 Control de Acceso:

□ Objetivos:

- Controlar el acceso a la información
- Asegurar que los derechos de acceso a los sistemas de información son autorizados, apartados y mantenidos adecuadamente.
- Prevenir accesos de usuarios no autorizados
- Asegurar la protección de servicios de red
- Prevenir accesos no autorizados a los equipos de computo
- Prevenir accesos no autorizados a la información almacenada en los sistemas de la organización
- Detectar actividades no autorizadas
- Asegurar la seguridad de la información cuando se empleen facilidades de computación móvil y tele-trabajo



7 Control de Acceso:

- Controlar el acceso a la información
 - Establecer una política de control de acceso de acuerdo a los requerimientos del negocio
 - Qué usuarios tienen acceso a que recursos y con qué privilegios (igual con empleados y personal de mantenimiento)
 - Usos permitidos y no permitidos de los recursos
 - Condiciones para aceptar conexiones al sistema
 - Comunicación cifrada o en claro de los datos
 - Especificación de mensajes de notificación y advertencia



7 Control de Acceso:

- Asegurar que los derechos de acceso a los sistemas de información son autorizados, apartados y mantenidos adecuadamente.
- Definir procesos y procedimientos de gestión de acceso de usuarios a los sistemas de información y los servicios
 - Procedimientos de autorización, identificación, derechos y niveles de acceso, condiciones, privilegios, registro y vigilancia de los accesos.



7 Control de Acceso:

- Prevenir accesos de usuarios no autorizados
 - Establecer las responsabilidades y obligaciones de los usuarios autorizados para contribuir con la efectividad de las políticas de control de acceso
 - Normas de uso del *password*
 - Normas de seguridad en los equipos de los usuarios



7 Control de Acceso:

- Asegurar la protección de servicios de red
 - Formular una política sobre el uso de la red y sus servicios
 - Redes y servicios de redes cuyo acceso está permitido
 - Procedimientos de autorización para acceder a diferentes clases de redes y de servicios de redes
 - Procedimientos y controles para proteger el acceso a las redes y los servicios de redes autorizados
 - Establecer puntos de acceso predefinidos que faciliten la implementación de los controles de acceso a la red



7 Control de Acceso:

- Asegurar la protección de servicios de red (2)
 - Establecer mecanismos para la autenticación de usuarios (conexiones) externos
 - Establecer mecanismos para autenticación de nodos de red
 - Introducir controles para segregar los servicios de una red en grupos que pueden estar aislados o protegidos unos de otros
 - Agregar a los servicios de red ofrecidos los niveles o atributos de seguridad requeridos



7 Control de Acceso:

- Prevenir accesos no autorizados a los equipos de computo
 - Activar las facilidades de seguridad que ofrecen los sistemas operativos para restringir el acceso a los recursos de computación (autenticación, duración de sesiones, identificación de terminales, *timeouts*, registro de accesos exitosos y fallidos, etc)



7 Control de Acceso:

- Prevenir accesos no autorizados a la información almacenada en los sistemas de la organización
 - Debe restringirse de acuerdo a lo establecido en la política de control de acceso.
 - Sistemas críticos deben tener un ambiente de computación dedicado (aislado)
- Detectar actividades no autorizadas
 - Habilitar sistemas de monitoreo que permitan:
 - Detectar incumplimientos de las políticas de control de acceso
 - Registrar eventos que proporcionen evidencia en caso de ocurrir incidentes de seguridad
 - Verificar el uso adecuado de las facilidades de procesamiento de información

Es importante que los relojes de todos los sistemas estén sincronizados para asegurar la fidelidad de las auditorías a los registros



7 Control de Acceso:

- Asegurar la seguridad de la información cuando se empleen facilidades de computación móvil y tele-trabajo
 - Establecer una política con procedimientos y estándares a cumplir para asegurar estas actividades (criptografía, virus, robo, etc)



8 Desarrollo y mantenimiento de sistemas

□ Objetivos:

- Asegurar que la seguridad esté incluida como requerimiento dentro los sistemas en operación
- Prevenir la pérdida, modificación o mal uso de los datos de los usuarios dentro de las aplicaciones
- Garantizar la confidencialidad, autenticidad e integridad de la información
- Asegurar que los proyectos de tecnologías de la información y actividades de soporte son conducidas en una manera segura
- Mantener la seguridad del *software* de las aplicaciones y sus datos



8 Desarrollo y mantenimiento de sistemas

- Asegurar que la seguridad esté incluida como requerimiento dentro los sistemas en operación
- Análisis y especificación de requerimientos de seguridad
 - Incorporar mecanismos de control, monitoreo, recuperación y respaldo
 - Incorporar los resultados derivados del análisis de riesgos de los activos de información del negocio involucrados en el sistema



8 Desarrollo y mantenimiento de sistemas

- ❑ Prevenir la pérdida, modificación o mal uso de los datos de los usuarios dentro de las aplicaciones
 - Validación de datos de entrada
 - Implantar controles sobre el procesamiento de los datos para prevenir o minimizar el riesgo de fallas y la pérdida de integridad de los datos
 - Usar programas para recuperar la consistencia luego de fallas
 - Incluir mensajes de autenticación, alerta y errores
 - Validación de los datos de salida



8 Desarrollo y mantenimiento de sistemas

- Garantizar la confidencialidad, autenticidad e integridad de la información
 - A través de sistemas y técnicas criptográficas
 - Justificado por un análisis de riesgo que así lo determine
 - Implica el desarrollo de una política de uso de los controles criptográficos: gestión de las llaves, tamaño adecuado de las llaves, roles y responsabilidades, etc



8 Desarrollo y mantenimiento de sistemas

- Asegurar que los proyectos de tecnologías de la información y actividades de soporte son conducidas en una manera segura
- Proveer controles y procedimientos para implantar *software* nuevo o revisado sobre los sistemas en operación
 - Estipular planes de prueba, validación y verificación del buen funcionamiento del *software*
 - Asegurar que se cumplan todos los criterios de aceptación definidos para el *software*
 - Llevar un registro de todas las actualizaciones realizadas a los sistemas en operación
 - Versiones previas deben ser mantenidas como medida de contingencia
- Establecer controles y procedimientos para proteger y manejar los datos empleados para probar los sistemas



8 Desarrollo y mantenimiento de sistemas

- Asegurar que los proyectos de tecnologías de la información y actividades de soporte son conducidas en una manera segura (2)
- Implementar un estricto control de acceso sobre los códigos fuentes de los programas
 - Utilizar prácticas de manejo de versiones
 - Listados de programas deben ser almacenados en ambientes seguros
 - Llevar un registro de todos los accesos realizadas a los códigos fuentes de los sistemas
 - Mantenimiento y copia de fuentes de las aplicaciones debe supeditarse a un plan de control o gestión de cambios



8 Desarrollo y mantenimiento de sistemas

- Mantener la seguridad del *software* de las aplicaciones y sus datos
 - Asegurar que todos los cambios propuestos al sistema sean revisados para verificar que no comprometen la seguridad del:
 - Sistema
 - Ambiente operativo
 - Datos
 - Realizar revisiones técnicas a las aplicaciones en operación cada vez que se actualizan o cambian los sistemas operativos de soporte, para verificar que no exista impacto adverso en cuanto a operación y seguridad
 - Utilizar *software* (utilitario o de operación) de fuentes confiables



8 Desarrollo y mantenimiento de sistemas

- Mantener la seguridad del *software* de las aplicaciones y sus datos (2)
 - Los contratos de desarrollo de software por terceros deben estipular:
 - Acuerdos sobre licencias, propiedad del código y derechos de propiedad intelectual
 - Cumplir con certificaciones de excelencia y calidad
 - Acuerdos de fiel cumplimiento y fianzas de garantía
 - Derechos para auditar la calidad y excelencia del trabajo realizado
 - Pruebas previas a la instalación para detectar código troyano



9 Gestión de la continuidad del negocio

- **Objetivo:** Contrarrestar las interrupciones a los procesos y actividades críticas del negocio por los efectos de fallas mayores o desastres
- Definir un proceso de gestión de la continuidad del negocio
 - Identificar y priorizar los procesos críticos del negocio de acuerdo a su impacto en la continuidad del negocio
 - Considerar la adquisición de un seguro contra siniestros adecuado
 - Formular y documentar una estrategia de continuidad del negocio basada en los objetivos y prioridades del negocio
 - Formular y documentar planes de continuidad del negocio en concordancia con la estrategia acordada
 - Realizar pruebas periódicas y ajustes de los planes y procesos formulados
 - Asegurar que la gestión de la continuidad del negocio forme parte de la estructura y procesos de la organización



9 Gestión de la continuidad del negocio

- Contrarrestar las interrupciones a los procesos y actividades críticas del negocio por los efectos de fallas mayores o desastres (2)
 - Desarrollar un plan estratégico, basado en el análisis de riesgo de la organización, para determinar las directrices a seguir para lograr la continuidad del negocio
 - Escribir e implementar los planes de continuidad
 - Identificar y acordar todas las responsabilidades y procedimientos de emergencia
 - Adoptar procedimientos de emergencia que permitan recuperar y restaurar el negocio (sus prioridades) en el tiempo estipulado
 - Documentación de procedimientos y procesos acordados
 - Entrenar los usuarios en los procedimientos y procesos acordados, incluyendo gestión de la crisis
 - Probar y perfeccionar los planes de continuidad



9 Gestión de la continuidad del negocio

- Contrarrestar las interrupciones a los procesos y actividades críticas del negocio por los efectos de fallas mayores o desastres (3)
- Establecer un marco de trabajo común para todos los planes de continuidad
 - Condiciones de activación: procesos a seguir, responsables e involucrados en cada fase y sus suplentes
 - Procedimientos de emergencia ante el incidente que pone en riesgo la continuidad del negocio o la vida humana.
 - Procedimientos de restauración o activación de servicios en localidades alternativas temporales y en los tiempos acordados
 - Procedimientos para retornar a la operatividad normal
 - Un calendario de mantenimiento para probar y perfeccionar los planes de continuidad
 - Entrenamiento y enseñanza del plan para asegurar su efectividad



9 Gestión de la continuidad del negocio

- Contrarrestar las interrupciones a los procesos y actividades críticas del negocio por los efectos de fallas mayores o desastres (4)
- Probar, mantener y reevaluar los planes de continuidad del negocio



10 Cumplimiento con el marco jurídico

□ Objetivos:

- Evitar lagunas y brechas de cualquier ley civil y criminal, de obligaciones estatutarias, regulatorias o contractuales y de cualquier requerimiento de seguridad
- Asegurar que los sistemas cumplen con las políticas y estándares de seguridad de la organización
- Maximizar la efectividad y minimizar la interferencia en los procesos de auditoría de los sistemas



10 Cumplimiento con el marco jurídico

- Evitar lagunas y brechas de cualquier ley civil y criminal, de obligaciones estatutarias, regulatorias o contractuales y de cualquier requerimiento de seguridad
 - Para cada sistema de información definir y documentar todos los requerimientos legales relevantes y las normas para asegurar su cumplimiento
 - Derechos de propiedad intelectual: *copyrights*, licencias, etc.
 - Salvaguarda de registros organizacionales
 - Identificar y clasificar la información que debe ser protegida: contable, base de datos, transacciones, procedimientos
 - Establecer guías para la retención, almacenamiento, manejo y desecho de registros e información
 - Llevar un cronograma para controlar el tiempo de almacenaje de los registros y su refrescamiento por degradación
 - Adoptar medidas para proteger los registros de pérdida, falsificación y destrucción



10 Cumplimiento con el marco jurídico

- ❑ Evitar lagunas y brechas de cualquier ley civil y criminal, de obligaciones estatutarias, regulatorias o contractuales y de cualquier requerimiento de seguridad (2)
 - Establecer directrices a todo nivel (gerencia, usuarios y proveedores de servicio) sobre las responsabilidades y procedimientos a seguir para garantizar la protección e intimidad de la información de los clientes
 - Establecer medidas para la prevención del uso de las facilidades de procesamiento de información en propósitos diferentes a los del negocio
 - ❑ Deben incluir acciones disciplinarias
 - ❑ Si las medidas de prevención implican "monitorear" el uso del sistema, debe cumplirse con el marco jurídico de la nación para llevarlo a cabo.
 - ❑ Concientizar a los usuarios del ámbito de sus actividades y las consecuencias legales de irrespetarlas



10 Cumplimiento con el marco jurídico

- Evitar lagunas y brechas de cualquier ley civil y criminal, de obligaciones estatutarias, regulatorias o contractuales y de cualquier requerimiento de seguridad (3)
 - Adaptar los controles criptográficos a las normas que regulan su funcionamiento dentro de la nación
 - Adoptar normas y controles que garanticen la correcta recolección de evidencia para soportar una acción legal
 - Asegurar que los sistemas cumplen con cualquier estándar o código válido para la obtención de evidencia admisible
 - Asegurar la calidad y completitud de la evidencia siguiendo su rastro con prácticas que demuestren su veracidad (testigos, fiscales, grabaciones, registros de copias de evidencias)



10 Cumplimiento con el marco jurídico

- Asegurar que los sistemas cumplen con las políticas y estándares de seguridad de la organización
 - Cada gerente debe asegurar que todos los procedimientos de seguridad de su jurisdicción son llevados correctamente
 - Realizar revisiones programadas a todos los entes involucrados con el negocio para asegurar que cumplen con las políticas y estándares de seguridad de la organización
 - Auditar periódicamente la plataforma tecnológica para verificar el cumplimiento de los estándares de seguridad implementados



10 Cumplimiento con el marco jurídico

- Maximizar la efectividad y minimizar la interferencia en los procesos de auditoría de los sistemas
- Definir controles para salvaguardar la operatividad de los sistemas y las herramientas de auditoría durante la ejecución de los procesos de auditoría
 - Acordar y definir los requerimientos y alcances de cada auditoría
 - Los recursos a utilizar deben estar explícitamente identificados
 - Requerimientos para acciones especiales o delicadas deben ser identificadas y su proceder acordado
 - Todos los acceso durante la auditoría deben ser monitoreados y registrados para producir trazos de referencia
 - Todos los procedimientos, requerimientos y responsabilidades deben ser documentados



10 Cumplimiento con el marco jurídico

- Maximizar la efectividad y minimizar la interferencia en los procesos de auditoría de los sistemas (2)
- Proteger las herramientas de auditoría del sistema
 - Definir quienes son los autorizados para utilizar las herramientas de auditoría
 - Separar y aislar las herramientas de auditoría con medidas de protección que prevengan su posible mal uso o compromiso



Material relacionado con el tema

- Del instituto nacional de estándares y tecnología (*NIST*)
 - <http://csrc.nist.gov/publications/nistpubs/index.html>
 - SP 800-12 Computer Security Handbook
 - SP 800-14 Generally Accepted [Security] Principles & Practices
 - SP 800-18 Guide for Developing Security Plans
 - SP 800-26 Security Self-Assessment Guide for Information Technologies Systems
 - SP 800-30 Risk Management Guide for Information Technologies Systems
 - SP 800-34 Contingency Plan Guide for Information Technologies Systems
- RFC 1244 Site Security Handbook
- Guía de implantacion BS 7799-2:2002