MODULO I
Arquitectura de Seguridad Informática

PROGRAMA

- Introducción a la Seguridad Informática.
- Amenazas y contramedidas.
- Desarrollo de la arquitectura de SI.
- Análisis de riesgos.
- Políticas, estándares, guías y su clasificación.
- Aspectos de implementación de políticas de seguridad.
- Planificación BCP/DRP.
- Auditoria de Seguridad Informática
- Adiestramiento

¿Qué es Seguridad Informática?

La seguridad informática comprende los siguientes aspectos:

- **Confidencialidad, los datos se mantienen ocultos a terceros.**
- **Integridad, los datos, aplicaciones, configuraciones, etc., no son alterados por terceros.**
- **Disponibilidad, los datos, aplicaciones, etc., pueden utilizarse en cualquier momento en que se requiera.**

Confidencialidad

- Protección de la información del acceso no autorizado.
- La autenticación y la autorización son los dos mecanismos utilizados para asegurar la confidencialidad.
- Debe desarrollarse un marco de referencia para clasificar la información de acuerdo a su nivel de confidencialidad.

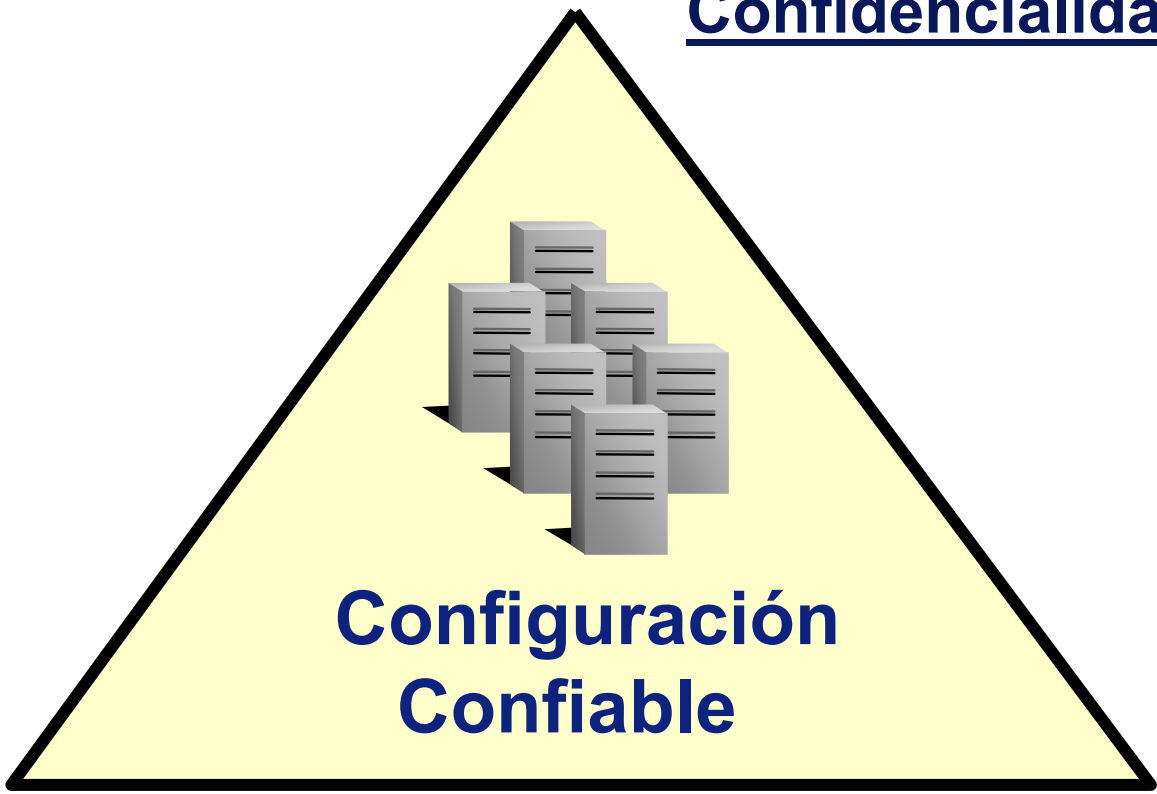
Integridad

- Protección de la información, las aplicaciones, los sistemas y las redes de cambios accidentales o intencionales no autorizados.
- Requiere de la validación y prueba de cualquier cambio en los sistemas. La autenticación es también importante.
- Debe desarrollarse un marco de referencia para clasificar la información de acuerdo a su nivel de integridad requerido.

Disponibilidad

- Asegurar que la información y los recursos estén disponibles para los usuarios autorizados cada vez que se necesite.
- Este aspecto es abordado en el Plan de Contingencia (*Business Continuity Planning/Disaster Recovery Planning*)
- Debe desarrollarse un marco de referencia para clasificar la información de acuerdo a su nivel requerido de disponibilidad.

Objetivos de Seguridad Informática



Amenazas y contramedidas

- Revisaremos las amenazas y vulnerabilidades más comunes relacionadas a la seguridad de la información.
- Las amenazas pueden ser causadas por uno o más eventos accidentales, deliberados o ambientales.
- Cada amenaza puede o no ser relevante para la organización.
- Se debe determinar las amenazas relevantes mediante un análisis de riesgos.

Algunas definiciones . . .

- *Amenaza:* Una causa potencial de un evento no deseado que puede resultar en perjuicio de la organización.
- *Vulnerabilidad:* Una característica de un activo informático que puede ser utilizado por una amenaza.
- *Responsabilidad:* Propiedad que asegura que para las acciones se puede determinar sin ambiguedades la entidad de origen.
- *Autenticidad:* Propiedad que asegura que la identidad de un sujeto o recurso es la que se afirma.
- *Confiabilidad:* La habilidad de un activo informático de tolerar fallas que pueden hacerlo inutilizable o incorrecto.

Amenazas ambientales

- Las amenazas ambientales incluyen a los desastres naturales y a otras condiciones ambientales.
- *Resultan en la pérdida de **disponibilidad** de la información que puede dar origen a:*
  - *Incapacidad de realizar tareas críticas.*
  - *Incapacidad de tomar decisiones.*
  - *Pérdida de imágen y confianza pública.*
  - *Pérdida económica*
  - *Afectar la salud y seguridad del personal.*
- *Si éstas amenazas se conjuntan con seguridad física inadecuada pueden originar pérdidad de **confidencialidad** de la información.*

Amenazas ambientales

- *Desastres naturales*
  - *Terremoto*
  - *Incendio*
  - *Inundación*
  - *Tormenta*
  - *Marea alta/Oleaje*

Amenazas ambientales

- *Condiciones ambientales*
  - *Contaminación*
  - *Interferencia electrónica*
  - *Temperatura y humedad extremas*
  - *Falla de alimentación eléctrica*
  - *Fluctuaciones eléctricas*
  - *Roedores*

Amenazas ambientales

- *Ejemplos de vulnerabilidades*
  - *Localización en zona sísmica.*
  - *Localización en área susceptible a incendios forestales.*
  - *Carencia de mantenimiento de equipos e instalaciones.*
  - *Monitoreo inadecuado de condiciones ambientales.*
  - *No se cuenta con UPS.*
  - *No se tienen planes de contingencia o procedimientos para recuperación de información y activos.*
  - *Archivos y sistemas de respaldo no disponibles.*

Amenazas accidentales

- Las amenazas accidentales están relacionadas a errores u omisiones. Los errores y omisiones de empleados y usuarios son la causa principal de problemas de seguridad informática.
- *Resultan en la pérdida de **disponibilidad, confidencialidad, integridad, responsabilidad, autenticidad y confiabilidad,** que puede dar origen a:*
  - *Interrupción de las funciones normales de la empresa.*
  - *Errores al tomar decisiones.*
  - *Pérdida de imágen y confianza pública.*
  - *Pérdida económica.*

Amenazas accidentales

- *Falla de los servicios de comunicación*
- *Falla de operaciones externas (outsourced)*
- *Pérdida o ausencia de personal clave*
- *Envío/re-envío equívoco de mensajes*
- *Errores de usuarios o staff operativo*
- *Errores de programación/software*
- *Fallas técnicas*
- *Errores de transmisión*

Amenazas accidentales

- *Ejemplos de vulnerabilidades*
  - *Carencia de redundancia y respaldos*
  - *Manejo inadecuado de incidentes*
  - *Procedimientos no documentados*
  - *Documentación faltante o inadecuada*
  - *Capacitación inadecuada del personal*
  - *Staff inexperto*
  - *Carencia de personal de respaldo*
  - *Falta de conciencia del usuario*

Amenazas deliberadas

- Las amenazas deliberadas (*ataques*) involucran la destrucción o manipulación deliberada de datos, software o hardware.
- *Resultan en la pérdida de **disponibilidad, confidencialidad, integridad, responsabilidad, autenticidad y confiabilidad,** que puede dar origen a:*
  - *Incapacidad de realizar tareas críticas.*
  - *Incapacidad de tomar decisiones.*
  - *Pérdida de imágen y confianza pública.*
  - *Pérdida económica.*

Amenazas deliberadas

- *Intrusión*
- *Denegación de servicio (DoS)*
- *Intervención (Eavesdropping, sniffing)*
- *Código malicioso*
- *Sabotaje*
- *Impostura*
- *Repudio*
- *Huelgas y paros*
- *Ingeniería social*
- *Robo y fraude*

Amenazas deliberadas

- *Ejemplos de vulnerabilidades*
  - *Carencia de firewall.*
  - *Utilizar sistemas operativos no actualizados.*
  - *Comunicaciones sin cifrar.*
  - *No utilizar software antivirus.*
  - *No tener control sobre el software que se baja de Internet.*
  - *Ex empleados que conservan el acceso a los recursos.*
  - *Carencia de controles de acceso a los datos.*

Tendencias en Ataques

- *De acuerdo al CERT/CC Overview Incident and Vulnerability Trends 2003 las tendencias en ataques son:*
  - *Troyanos/Código malicioso*
  - *Internet sniffers*
  - *Scanning/ataques en gran escala*
  - *Herramientas de ataque distribuido (recolección de salidas de sniffers)*
  - *Herramientas de ataques DoS distribuido*
- *Ver: http://www.cert.org/present/cert-overview-trends/*

Tendencias en Ataques

- *De acuerdo al CSI/FBI Computer Crime and Security Survey 2003:*
  - *530 empresas, agencias gubernamentales, instituciones financieras, universidades, etc.*
  - *56% reportó uso no autorizado (60% en 2002)*
  - *Total de pérdidas reportadas: $201,797,340 (en 2002 fueron $445 millones).*
  - *Mayor pérdida financiera ocasionada por robo de información propietaria ($70,195,900).*
  - *Denegación de servicio, segundo ataque más costoso ($65,643,300)*
  - *Formas más comúnes de ataque: virus (82%) y abuso interno de acceso a la red (%80).*

Amenazas y riesgos

- *Una amenaza es una causa potencial de un daño.*
- *Un riesgo es la probabilidad de que una amenaza se vuelva real.*
- *Una vez que se ha reconocido un riesgo, hay tres alternativas:*
  - *Aceptar el riesgo.*
  - *Reducir el riesgo: Hacer algo para reducir el riesgo a un nivel aceptable.*
  - *Transferir el riesgo: Comprar un seguro.*

Controles de seguridad

- *La reducción de riesgo se logra mediante la implementación de controles efectivos.*
- *Los controles se clasifican en tres categorias:*
  - *Controles administrativos*
  - *Controles físicos*
  - *Controles técnicos*

Controles administrativos

- *Los controles administrativos incluyen:*
  - *Políticas y procedimientos de seguridad.*
  - *Separación de deberes.*
  - *Inducción y adiestramiento en seguridad.*
  - *Planes de contingencia y recuperación.*
  - *Reportes de auditorias de seguridad.*
  - *Responsabilidades sobre datos/recursos.*

Controles físicos

- *Relacionadas a la protección de amenazas ambientales, así como a la protección de acceso físico a sistemas, equipo, etc., por parte de intrusos.*
- *Control de acceso físico:*
  - *Acceso a instalaciones solo a personal autorizado.*
  - *Servidores críticos en lugares cerrados bajo llave.*
  - *Dispositivos de red en racks cerrados.*
  - *Hardware en gabinetes cerrados.*
  - *Fijar equipo a muebles no movibles.*
  - *Respaldos y medios en sitio seguro, bajo llave.*

Controles físicos

- *Alimentación eléctrica*
  - *Acondicionamiento de potencia (supresión de picos)*
  - *Fuentes ininterrumpibles (UPS)*
  - *Usar alfombras anti-estáticas*
  - *Utilizar pulseras anti-éstáticas*
- *Clima y ambiente*
  - *Asegurar flujo de aire en equipo de cómputo*
  - *Temperatura controlada entre 10-26°C*
  - *Instalar aire acondicionado con filtraje de aire para evitar polvo.*

Controles físicos

- *Humo y fuego*
  - *Prohibir fumar en sitios de servidores.*
  - *Extinguidores de incendios.*
  - *Extinguidores automatizados en sitios importantes.*
  - *Detectores de humo.*
- *Agua*
  - *Humedad controlada entre 20% y 80%.*
  - *Sensores de agua en pisos.*
  - *No encender equipo humedo.*
- *Respaldos*
  - *Respaldos off-site*

Controles técnicos

- *Los controles técnicos (o lógicos) son implementados a través de hardware o de software y, una vez implementados, pueden trabajar sin intervención humana.*
- *Incluyen:*
  - *Aplicaciones criptográficas.*
  - *Endurecimiento (hardening) de servidores*
  - *Software antivirus.*
  - *Herramientas de administración de red.*
  - *Firewalls.*
  - *Sistemas detectores de intrusos (IDS).*

Controles técnicos

- *Aplicaciones criptográficas:*
  - *Utilizan algoritmos de cifrado simétrico, de clave pública, de hash, etc.*
  - *Proporcionan:*
    - *Confidencialidad – La información se cifra para que solo sea legible a quienes posean la clave correspondiente.*
    - *Autenticación – Existen diversos protocolos criptográficos para la autenticación de entidades a comunicarse.*
    - *No repudio – Mediante el uso de firmas y certificados digitales.*

Controles técnicos

- *Endurecimiento de servidores:*
  - *Los sistemas operativos con instalaciones por default son muy vulnerables:*
    - *Bugs en el SO.*
    - *Configuración incorrecta*
    - *Servicios innecesarios abiertos*
    - *Aberturas por servicios de administración y monitoreo remotos.*
    - *Mayoria de compromisos en servidores debido a vulnerabilidades previamente conocidas y documentadas !!*

Controles técnicos

- *Endurecimiento de servidores:*
  - *Instalar SO con opciones de configuración seguras.*
  - *Bajar e instalar parches para vulnerabilidades conocidas.*
  - *Cerrar servicios y aplicaciones innecesarios.*
  - *Endurecer servicios y aplicaciones restantes.*
  - *Configurar adecuadamente usuarios y grupos.*
  - *Configurar permisos de accesos*
  - *Emplear protecciones avanzadas (verificadores de integridad, analizadores de bitácoras, etc.)*

Controles técnicos

- *Seguridad perimetral:*
  - *La principal fuente de ataques es el punto de conexión de la redes a Internet.*
  - *Es necesario proteger el perímetro de la red local, aislándola del acceso no autorizado desde el exterior.*
  - *Se logra mediante la utilización de cortafuegos y de IDS (sistemas detectores de intrusos).*
  - *Transmisión segura de datos: VPNs.*
  - *NOTA: La seguridad perimetral es solamente uno de todos los controles técnicos necesarios.*

¿Porqué una Arquitectura de SI?

- *La implementación efectiva de controles de seguridad necesita de un plan integral.*
- *El plan estratégico de seguridad debe estar alineado con el plan estrátegico de tecnología informática de la empresa y, a través de éste, con el plan estratégico de negocios.*
- *La arquitectura de seguridad informática proporciona una visión sistémica de la infraestructura y administración de la seguridad informática dentro de la empresa.*

Arquitectura de SI

- *Los componentes de una ASI son:*
  - *Organización e infraestructura de seguridad.*
  - *Políticas, estándares y procedimientos de seguridad.*
  - *Evaluaciones de riesgos y de seguridad.*
  - *Programas de inducción y adiestramiento en seguridad.*
  - *Cumplimiento.*

Organización/Infraestructura

- *Debe desarrollarse para apoyar la continuidad del desarrollo e implementación de la arquitectura de seguridad.*
- *Debe incluir:*
  - *Definición de la autoridad de aprobación de todas las políticas y resolución de aspectos de seguridad.*
  - *Definición del Equipo de Seguridad para desarrollo de la ASI y el desarrollo, implementación y difusión de las políticas, estándares y procedimientos de seguridad.*
  - *Establecimiento de reuniones periodicas.*
  - *Identificación y documentación de las responsabilidades de seguridad de los miembros del equipo.*

Políticas, Estándares y Procedimientos

- *Política – Su propósito es informar a todos los usuarios sobre las expectativas de administración concernientes al uso apropiado de la información, los sistemas, y los recursos.*
- *Estándares – Diseñados para una operación consistente y más eficiente. Aseguran que los individuos operan consistentemente para minimizar riesgos y para hacer la adminsitración de sistemas y redes más eficiente.*
- *Procedimientos – Procesos y operaciones que proporcionan los detalles específicos de como realizar acciones particulares (mantenimiento, respaldos, manejo de bitácoras, etc.)*

Políticas, estándares y procedimientos

Evaluaciones de riesgos

- *Inicialmente, evaluación de riesgos de alto nivel:*
  - *Entorno de operación*
  - *Organización de la seguridad*
  - *Planeación y administración de seguridad*
  - *Políticas, planes y procedimientos de seguridad informática*
  - *Clasificación y control de información*
- *Evaluaciones detalladas: Aplicaciones, bases de datos, redes, sistemas operativos y telecomunicaciones.*
- *Cada uno de los sistemas de la empresa debera ser evaluado.*
- *Debe haber revaluaciones periodicas.*

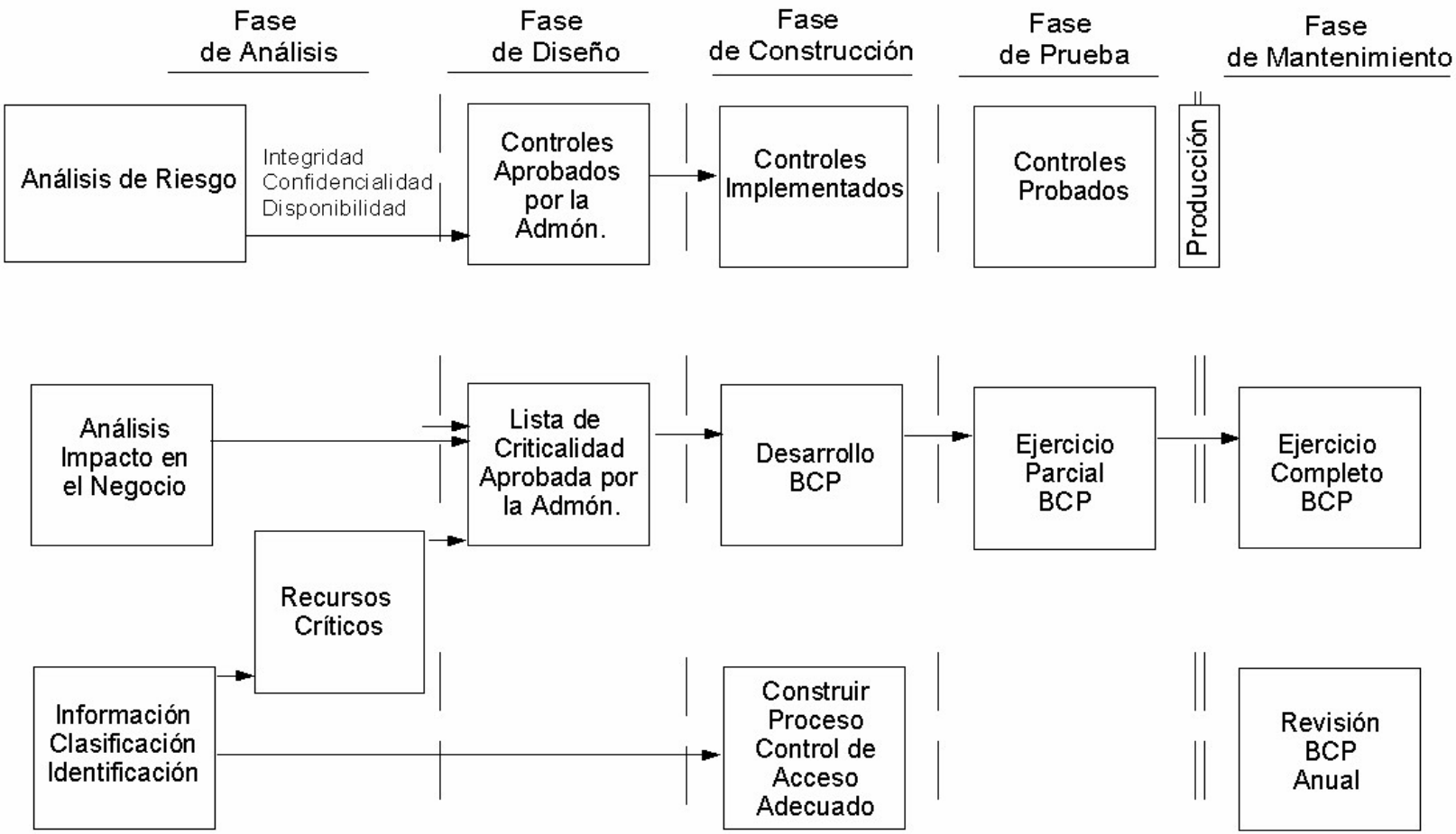
Programa de Inducción y Adiestramiento

- *Auxilia a reducir el riesgo de perdida de activos informáticos entrenando a los empleados para entender el valor de la seguridad informática, reconocer sus responsabilidades en la protección de activos y reconocer así como reportar violaciones potenciales.*
- *Consiste tanto de clases de adiestramiento como de recordatorios frecuentes.*
- *Requiere planeación, presupuesto, creatividad y apoyo de la administración.*
- *Para ser efectivo debe cubrir a toda la organización.*
- *Los beneficios son difíciles de ver y cuantificar en el corto plazo, pero los resultados finales pueden tener un impacto financiero significativo en la organización evitando incidentes innecesarios por negligencia, ignorancia o conducta negativa.*

Desarrollo de la ASI

- *El desarrollo de la ASI se realiza en las siguientes fases:*
  1. *Fase de análisis.*
  2. *Fase de diseño.*
  3. *Fase de implementación.*
  4. *Fase de pruebas.*
  5. *Fase de mantenimiento.*

Fases de desarrollo



Análisis de riesgos

- *Independientemente del proceso utilizado, el método siempre es el siguiente:*
  - *a) Identificar los activos.*
  - *b) Identificar los riesgos.*
  - *c) Determinar las vulnerabilidades.*
  - *d) Definir los controles.*

Análisis de Impácto en el Negocio (BIA)

- *Identifica los costos asociados a los riesgos por:*
  - *Pérdidas de flujo de efectivo*
  - *Reemplazo de equipo*
  - *Salarios derogados por repetición de trabajo*
  - *Pérdida de ganacias*
  - *Otros*
- *El impacto debe expresarse monetariamente ($$$) !!!*

Clasificación de Datos y Recursos

- Para proporcionar mecanismos de protección donde más se necesitan y colocar controles menos costosos en áreas menos críticas.
- Para cada objetivo de seguridad: *confidencialidad*, *integridad* y *disponibilidad* se clasifican los datos/recursos como de:
  - Alto impacto
  - Mediano impacto
  - Bajo impacto

Clasificación de Confidencialidad

- Alto impacto (Confidencial)
  - Datos altamente delicados que pueden comprometer a la empresa, a los clientes o empleados si se divulgan.
  - Su revelación viola la privacidad de un individuo.
  - Su revelación reduce la ventaja competitiva de una empresa.
  - Estrategias de negocios, direcciones en I&D, o avances en tecnología, relacionados al éxito financiero de un producto.
- Mediano impacto (Uso interno)
  - Para uso exclusivo de los empleados o grupos de empleados dentro de una división particular o departamento.
- Bajo impacto (Público)
  - Disponible para el público.

Clasificación de Integridad

- Alto impacto
  - No existe respaldo para la información/aplicación. No existe documentación.
  - Decisiones críticas de la empresa se hacen utilizando la información/salida de esta aplicación.
  - Un error en los datos se puede propagar a otros sistemas.
  - La corrupción de datos puede tener un impacto serio en las ganancias, el servicio al cliente, o las operaciones.
  - La aplicación o el sistema cambia frecuentemente y la información relacionada crece significativamente.
  - La aplicación o el sistema está integrado con muchas otras aplicaciones o procesos en diferentes plataformas.

Clasificación de Integridad

- Mediano impacto
  - Los datos pueden ser verificados o comparados con documentos fuente, reportes, etc.
  - Los errores en los datos tienen una probabilidad moderada de corromper otros sistemas.
  - La aplicación, el sistema o los procesos están limitados a ciertas áreas o departamentos de la empresa.
  - La aplicación o el sistema tiene cambios poco frecuentes y la información relacionada a él crece en proporción moderada respecto a su uso.
  - La aplicación o el sistema está integrado con pocas aplicaciones y tiene relativamente pocas interfaces.

Clasificación de Integridad

- Bajo impacto
  - Los datos son utilizados como una fuente secundaria de información.
  - Las decisiones y operaciones de la empresa no se basan significativamente en la información proporcionada por la aplicación.
  - Es un sistema *stand-alone* y es utilizado por una sola área o departamento.
  - Es un proceso relativamente estable o un sistema que no requiere de modificaciones.

Clasificación de Disponibilidad

- Alto impacto
  - Los datos se requieren diariamente para realizar funciones importantes en la empresa.
  - La indisponibilidad de los datos resulta en fuertes pérdidas económicas.
  - Existen compromisos legales para el acceso continuo al sistema.
  - Se tiene una reducción seria en la productividad de los empleados si los datos no están disponibles.

Clasificación de Disponibilidad

- Mediano impacto
  - Se tiene cierta reducción en la productividad de los empleados o cierta pérdida económica si los datos no están disponibles.
  - Los empleados pueden continuar trabajando manualmente por cierto periodo con cierta reducción de la eficiencia.
- Bajo impacto
  - No se requiere acceso inmediato a los datos para realizar funciones esenciales.
  - Pueden utilizarse procedimientos manuales por un periodo extenso de tiempo para continuar las operaciones de la empresa.

Definiciones. . .

- *Control/Salvaguarda – una contramedida que actua para prevenir, detectar o minimizar la consecuencias de ocurrencia de una amenaza.*
- *Factor de exposición – cuanto impácto o pérdida de activos se ha tenido*
  - *0% a 100%*
- *Pérdida Singular (PS) – cuando una amenaza ocurre, cantidad de pérdida de valor del activo esperada, en términos monetarios.*
- *Tasa de Ocurrencia Anualizada (TOA) – frecuencia de ocurrencia esperada de una amenaza durante un año.*

Tasas de ocurrencia de riesgos

- *Pérdida Esperada Anualizada (PEA) – un valor definido en el análisis de riesgos clásico que indica la pérdida esperada para una amenaza dada.*
- *Considerando el valor del activo (V) y la probabilidad del factor de exposición (L), la PEA será igual a:*
  - *V x L = PEA*

Tabla de multiplicadores

Nunca	*0*	*0.0*
Una en 300 años	*1/300*	*0.00333*
Una en 200 años	*1/200*	*0.055*
Una en 100 años	*1/100*	*0.01*
Una en 50 años	*1/50*	*0.02*
Una en 25 años	*1/25*	*0.04*
Una en 5 años	*1/5*	*0.20*
Una en 2 años	*½*	*0.5*
Anual	*1*	*1*
Mensual	*12*	*12*
Semanal	*52*	*52*
Diaria	*365*	*365*

Ejercicio…

- *Se tiene un centro de datos de $3 millones de dólares en una área susceptible a inundaciones. Cada 100 años, se produce una gran inundación que podría destruir el centro de datos.*
- *Calcular el PEA.*
- *Usando el PEA calculado, ¿cuál es la probabilidad de que la administración esté dispuesta a gastar $35,000.00 dólares anuales para controlar esta amenaza?*
- *¿Es efectivo en costo?*

Métodos cuantitativos de AR

- *PROS*
  - *Los resultados se basan substancialmente en procesos y métricas objetivas.*
  - *Se trabaja en la definición de valores de los activos y en la mitigación de riesgos.*
  - *Es esencial el trabajo en la evaluación costo/beneficio.*
  - *Los resultados se expresan en el mismo lenguaje de la administración:*
    - *Valor monetario, porcentajes, probabilidad.*

Métodos cuantitativos de AR

- *CONTRAS*
  - *Cálculos complejos*
  - *Requiere la estimación económica de valores de activos*
  - *Requiere del conocimiento de frecuencias de amenazas (estadísticas previas)*
  - *Mucho trabajo preliminar*
  - *Requiere una asesoria adecuada*
  - *Difícil cambiar de dirección*

Métodos cualitativos de AR

- *PROS*
  - *Cálculos simples*
  - *No es necesario determinar valores económicos de activos*
  - *No es necesario cuantificar frecuencia de amenazas*
  - *Es fácil involucrar personal que no es del área técnica ni de seguridad*
  - *Proporciona flexibilidad en el proceso*
  - *No requiere asesoria*

Métodos cualitativos de AR

- *CONTRAS*
  - *De naturaleza muy subjetiva*
  - *Esfuerzo limitado en la determinación del valor de los activos*
  - *No aporta información para el análisis costo/beneficio*
  - *No fácilmente aceptable para la administración*

QRA

- *Qualitative Risk Analysis*
  1) *Establecer el alcance*
  2) *Integrar un equipo competente*
  3) *Identificar las amenazas.*
     - *Llenar el campo en la hoja de determinación de factores de riesgo.*
  4) *Priorizar las amenazas*
     - *Tasa de ocurrencia de la amenaza (TOA)*
  5) *Priorizar el impácto*
     - *Estimar la pérdida si la amenaza ocurre*
  6) *Calcular impácto total*
     - *TOA+L=Factor de Riesgo*

QRA

- *Qualitative Risk Analysis*

7) *Identificar controles*

   - *Identifica controles físicos, administrativos y técnicos que ofrezcan un nivel de protección aceptable y de costo efectivo para el activo bajo revisión.*
   - *Cuatro capas:*
     - *Prevención*
     - *Aseguramiento*
     - *Detección*
     - *Recuperación*

8) *Análisis costo/beneficio*

9) *Ordenar controles por su prioridad*

10) *Reporte del análisis de riesgo*

FRAP

- *FACILITATED RISK ANALYSIS PROCESS*
  - *FRAP analiza un sistema, una aplicación o un segmento del negocio a la vez.*
  - *Se convoca a un equipo de personas que incluya administradores y de soporte.*
  - *El equipo realiza una lluvia de ideas sobre las amenazas potenciales, las vulnerabilidades y los impactos negativos resultantes sobre la integridad, confidencialidad y disponibilidad de los datos/recursos.*
  - *Se analiza el impacto sobre las operaciones de la empresa.*
  - *Se priorizan las amenazas y riesgos.*

FRAP

- *FACILITATED RISK ANALYSIS PROCESS*
  - *Después de identificar y categorizar los riesgos, el grupo identifica los controles que puedan mitigar los riesgos*
    - *Un grupo común de 26 controles es utilizado como inicio*
  - *La decisión de que controles se necesitan descansa en la administración de la empresa.*
  - *El equipo concluye documentando que riesgos existen y que controles se necesitan así como el plan de acción a seguir para la implementación de los controles.*

FRAP

- *FACILITATED RISK ANALYSIS PROCESS*
  - *Cada sesión de análisis de riesgo toma aproximadamente 4 horas.*
  - *Incluye de 7 a 15 personas.*
  - *Se requiere tiempo adicional para desarrollar el plan de acción.*
  - *No se intentan obtener números específicos para la probabilidad de las amenazas o estimar pérdidas anualizadas.*
  - *El reporte de riesgos y controles es confidencial y depositado en la administración de la empresa.*

Metodologia FRAP

1. *Reunión pre-FRAP (aprox. 1 hora)*
   - *Establecer álcance*
   - *Diagrama visual (proceso a analizar)*
   - *Miembros del equipo*
   - *Mecánica de las reuniones*
2. *Sesión FRAP (aprox. 3 horas)*
   - *Riesgos identificados*
   - *Riesgos priorizados*
   - *Controles sugeridos*
3. *Proceso post-FRAP (hasta 10 días)*
   - *Llenar hoja de referencias cruzadas*
   - *Identificación de controles existentes*
   - *Selección de controles para riesgos abiertos o aceptar riesgos*

Estándares Internacionales

- *Organizaciones*
  - *ISO/IEC*
  - *IETF*
  - *IEEE*
  - *NIST*
  - *ITU-T*
  - *W3C*
  - *NCSA*
  - *...*

Estándares Internacionales

- *ISO/IEC 17799 y BS 7799-2.*
- *Common Criteria*
- *CDSA – Common Data Security Architecture*
- *GMITS – Guideline for the Management of IT Security (ISO)*
- *OSI Security (ISO)*
- *GASSP – Generally Accepted System Security Principles (I^2SF) – Promovida por la OCDE.*

ISO 17799 y BS 7799-2

- *ISO 17799:2000, código de práctica para la administración de la seguridad informática (ISM).*
- *BS 7799-2:2002, estándar de sistemas de administración de la seguridad informática (ISMS).*

ISO 17799

- *¿Qué es?*
  - *"Un conjunto de controles que abarcan las mejores prácticas en seguridad de la información."*
  - ***Básicamente...un estándar genérico de seguridad informática internacionalmente reconocido.***

ISO 17799

- *¿Porqué?*
  - *"Su intención es servir como un punto de referencia único para identificar un rango de controles requeridos para la mayoria de las situaciones en las cuales son utilizados los sistemas de información en la industria y el comercio."*

Historia de ISO 17799

- *Publicado por primera vez como Código de Práctica DTI en el Reino Unido.*
- ***Revaluado y públicado como versión 1 del BS 7799 en febrero de 1995.***
- ***NO fue adoptado ampliamente, por varias razones, como:***
  - ***No era suficientemente flexible***
  - ***Enfoque de "controles clave" simplista***
  - ***Otro problemas eran prioridad (Y2K)***

Historia de ISO 17799

- *Revisión del BS7799. Versión 2 es publicada en mayo de 1999.*
- *En el mismo año se lanzan los esquemas de acreditación y certificación formal.*
- *Comienzan a aparecer herramientas de apoyo.*
- *Se acelera la iniciativa ISO.*
- *Publicada como estándar ISO en diciembre del 2000.*

Contenido del ISO 17799

- *El contenido abarca diez tópicos principales:*
  - *Establecimiento de la política de seguridad de la organización.*
  - *Infraestructura de seguridad organizacional.*
  - *Clasificación y control de activos.*
  - *Seguridad en personal.*
  - *Seguridad ambiental y física.*
  - *Administración de operaciones y comunicaciones.*
  - *Control de acceso.*
  - *Mantenimiento y desarrollo de sistemas.*
  - *Administración de continuidad del negocio (BCM)*
  - *Cumplimiento (compliance).*

Ejemplo del ISO 17799

- *Control: 8.6.2 Eliminación de medios*
- *Los medios deberian eliminarse de manera segura una vez que ya no se requieran. Pueden darse fugas de información a personas externas mediante la eliminación descuidada de medios. Podrían establecerse procedimientos formales para la eliminación segura de medios para minimizar este riesgo. Podrían considerarse los siguientes controles...*
  - *a) Los medios que contengan información sensible deben ser almacenados y eliminados de manera segura...*
  - *b) La siguiente lista identifica items que pueden requerir eliminación segura...*
  - *...*
  - *e) La eliminación de items sensibles debería registrarse en bitácoras cuando sea posible con el propósito de mantener un rastro de auditoria.*

BS 7799-2

- *BS 7799-2:2002 Information Security Management Systems – Specification with Guidance of Use*
  - *Estándar británico, no ISO.*
- *Especifica requerimientos para definir, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS documentado.*
  - *Proporciona un enfoque sistemático a la administración de la seguridad informática.*
  - *Requerimientos de administración en concordancia con ISO 9001 e ISO 17799.*
- *ISO ha iniciado un estudio sobre BS 7799 que presumiblemente dará origen a un estándar ISO.*

Ambito del BS 7799-2

- *Requerimientos extensivos sobre el sistema de administración*
  - *Evaluación y administración de riesgos.*
  - *Compromiso de la administración y recursos.*
  - *Entrenamiento y concientización.*
  - *Revisión y mejora del sistema.*
- *Ciclo de vida: Plan/Do/Check/Act*
- *Annex A incluye 127 controles directamente derivados de la ISO 17799*
  - *"una organización debe considerar que [...] controles adicionales pueden ser necesarios"*
  - *"No todos los controles descritos pueden ser relevantes para todas las situaciones..."*

Ejemplo del BS 7799-2

- *Annex A.8: Los medios deben eliminarse de manera segura cuando ya no se requieran.*
- *4.2.1 Establecimiento del ISMS: La organización debe hacer lo siguiente. [...]*

  c) Definir un enfoque sistemático a la evaluación de riesgos. Identificar un método de evaluación de riesgos que se adapte al ISMS y los requerimientos de seguridad informática de la empresa, legales y regulatorios identificados. Establecer políticas y objetivos para el ISMS con el fin de reducir los riesgos a un nivel aceptable. Determinar los criterios para aceptar los riesgos e identificar los niveles aceptables de riesgo.

  d) Identificar los riesgos

  1) Identificar los activos dentro del ámbito del ISMS y los propietarios de los activos

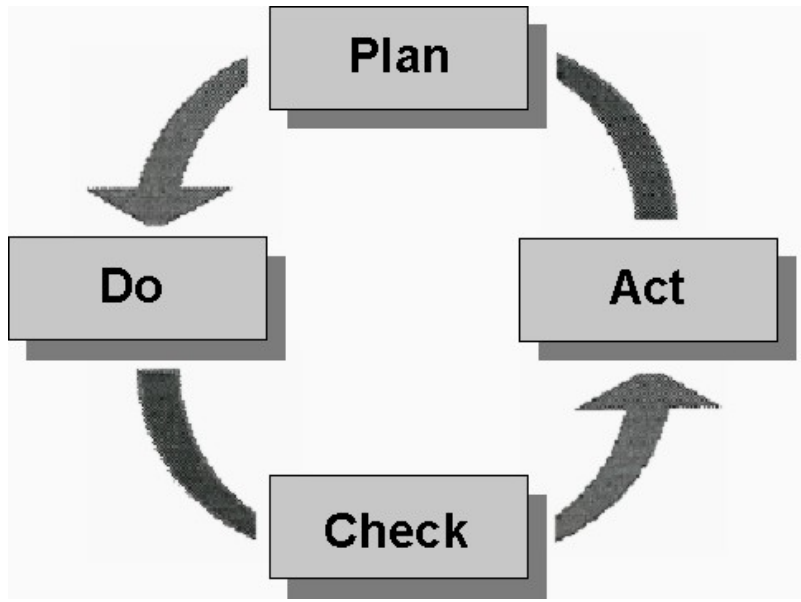
  2) Identificar las amenazas a esos activos

  3) Identificar las vulnerabilidades que pueden explotar las amenazas.

  4) Identificar el impacto que las pérdidas de confidencialidad, integridad y disponibilidad pueden tener en los activos.

Ciclo de vida ISMS

- *Plan: La organización debe...*
  - *Definir ámbito ISMS*
  - *Identificar y evaluar los riesgos*
  - *Administrar los riesgos*
- *Do: La organización debe...*
  - *Implementar un plan de mitigación de riesgos*
  - *Implementar controles seleccionados*
- *Check: La organización debe...*
  - *Realizar monitoreos*
  - *Conducir revisiones periodicas*
- *Act: La organización debe...*
  - *Implementar mejoras*
  - *Tomar acciones correctivas*



Common Criteria

- *Estándar desarrollado por:*
  - *Communications Security Establishment (CAN)*
  - *Communications-Electronic Security Group (UK)*
  - *Bundesamt fur Sicherbeit in der Informationstechnik (GER)*
  - *NSA, NIST (USA)*
  - *Service Central de la Securite des Systemes d'Information (FR)*
  - *National Security Agency (HOL)*
- *Basado principalmente en ITSEC de Europa.*
- *Adoptado como ISO 15408 en 1999.*

Common Criteria

- CC presenta requerimientos de seguridad para un producto o sistema bajo distintas categorias de *requerimientos funcionales* (CC parte 2) y *requerimientos de aseguramiento* (CC parte 3).
- *Requerimientos funcionales* CC – Definen características de seguridad deseadas.
- *Requerimientos de aseguramiento* CC – Bases para tener confianza en que las medidas de seguridad declaradas son efectivas y correctamente implementadas.

Enfoque de los CC

- La confianza en la seguridad informática puede obtenerse a través de acciones que puedan tomarse durante el proceso de *desarrollo*, *evaluación* y *operación*.
  - *Desarrollo* – CC define un conjunto de requerimientos de seguridad para productos y sistemas candidatos.
  - *Evaluación* – Asegurar que los objetivos de seguridad son satisfechos.
  - *Operación* – Revaluación ante nuevas vulnerabilidades o revisión de supocisiones ambientales.

Conceptos clave

- Protection Profile (PP) – Define un conjunto de requerimientos y objetivos de seguridad para una categoria de productos o sistemas que satisfacen necesidades similares. Se han desarrollado PP para firewalls, bases de datos, etc.
- Target of Evaluation (TOE) – Producto o sistema a evaluar.
- Security Target (ST) – Contiene los requerimientos y objetivos de seguridad para un TOE específico y define las medidas funcionales y de aseguramiento de que el TOE satisface los requerimientos.

Catálogo de Componentes

- La parte 2 de los CC contiene el catálogo de componentes funcionales:
  - Audit (FAU)
  - Cryptographic Support (FCS)
  - Communication (FCO)
  - User Data Protection (FDP)
  - Identification and Authenticacion (FIA)
  - Security Management (FMT)
  - Privacy (FPR)
  - Protection of the TOE Security Functions (FPT)
  - Resource Utilisation (FRU)
  - TOE Access (FTA)
  - Trusted Path/Channels (FTP)

Niveles de Evaluación

- Los CC contienen un conjunto de niveles de evaluación (*Evaluation Assurance Levels – EAL*) construidos usando componentes de las familias de aseguramiento.
- Hay siete niveles EAL jerárquicos:
  - EAL1 – probado funcionalmente
  - EAL2 – estructuralmente probado
  - EAL3 – metódicamente probado y verificado
  - EAL4 – metódicamente diseñado, probado y revisado
  - EAL5 – diseñado semiformalmente y probado
  - EAL6 – diseño verificado semiformalmente y probado
  - EAL7 – diseño verificado formalmente y probado

ISO 17799 vs. CC

- *ISO 17799 es un estándar de administración y concierne a aspectos no técnicos relacionados a sistemas de TI instalados.*
- *ISO 17799 toca aspectos tales como personal, procedimientos, seguridad física y administración de seguridad en general.*
- *CC es un estándar técnico para apoyar la especificación y evaluación técnica de características de seguridad en productos de TI.*
- *CC proporciona una estructura y una sintáxis que puede utilizarse para especificar requerimientos técnicos de seguridad en productos.*

GASSP

- *Principios:*
  - *Principio de responsabilidad*
  - *Principio de atención*
  - *Principio de ética*
  - *Principio de multidisciplinareidad*
  - *Principio de proporcionalidad*
  - *Principio de integración*
  - *Principio de diligencia*
  - *Principio de revaluación*
  - *Principio de equidad*

Prácticas de seguridad CERT

- *Prácticas:*
  - *Endurecimiento de sistemas mediante el establecimiento de configuraciones seguras.*
  - *Prepararse para intrusiones mediante la detección y la respuesta.*
  - *Detectar intrusiones rápidamente.*
  - *Responder a intrusiones rápidamente.*
  - *Mejorar la seguridad para proteger contra futuros ataques.*

Método OCTAVE (CERT)

- *OCTAVE:*
  - *Operationally Critical Threat, Asset and Vulnerability Evaluation.*
  - *Fase 1:*
    - *Proceso 1: Identificar conocimiento de la administración.*
    - *Proceso 2: Identificar conocimiento del área operativa.*
    - *Proceso 3: Identificar conocimiento del staff.*
  - *Fase 2:*
    - *Proceso 5: Identificar componentes claves.*
    - *Proceso 6: Evaluar componentes seleccionados.*
  - *Fase 3:*
    - *Proceso 7: Conducir análisis de riesgos.*
    - *Proceso 8: Desarrollar estrategia de protección, seleccionar estrategias de protección.*

Desarrollo de Políticas de SI

- *Política de seguridad informática:*
  - *Conjunto de reglas cuyo cumplimiento garantiza la consecución y mantenimiento de los objetivos de seguridad informática.*
  - *Políticas:*
    - *Uso aceptable de recursos*
    - *Autenticación y seguridad en red*
    - *Seguridad en Internet (perimetral)*
    - *Seguridad en correo electrónico*
    - *Manejo de código malicioso*
    - *Cifrado (Protección de datos)*

Políticas de SI

- *Definen la conducta adecuada*
- *Proporcionan la base para determinar las herramientas y procedimientos adecuados*
- *Establecen un consenso*
- *Proporcionan un fundamento a las acción de RH en respuesta a una conducta inadecuada*
- *Pueden auxiliar en la persecución de delitos*

Confianza

- *La confianza es el primer principio en el cual basar el desarrollo de las políticas de seguridad.*
- *Paso inicial: Determinar quien tiene acceso.*
- *Decidir el nivel de confianza es un acto delicado:*
- *Demasiada confianza puede originar problemas de seguridad*
- *Poca confianza puede hacer difícil encontrar y conservar empleados.*
- *¿Qué tanto se confía en los recursos y en la gente?*

Proceso de Diseño de PSI

- *Elegir el equipo de desarrollo de políticas.*
- *Designar a una persona o entidad como el aval oficial de la política.*
- *Decidir sobre el ámbito y objetivos de la política*
  - *El ámbito debe ser una declaración escrita sobre que aspectos cubre la política.*
- *Decidir que tan específica debe ser la política*
  - *NO debe ser un plan detallado de implementación*
  - *NO debe incluir hechos que cambien frecuentemente*

Proceso de Diseño de PSI

- *Se debe dar una oportunidad a un grupo representativo de las personas afectadas por la política de revisarla y comentarla.*
- *Se debe dar oportunidad a gente de soporte de revisarla.*
- *Se debe incorporar una inducción a la política como parte de la orientación del empleado.*
- *Se debe dar una revisión y actualización a la política una o dos veces al año.*

Requerimientos Básicos

- *La política debe:*
  - *Ser implementable y poder hacerse cumplir*
  - *Ser concisa y fácil de entender*
  - *Equilibrar protección con productividad*
- *La política debería:*
  - *Establecer razones por las cuales es necesaria*
  - *Describir que es cubierto por la política*
  - *Definir contactos y responsabilidades*
  - *Discutir como serán manejadas las violaciones*

Estructura de la Política

- *Dependiente del tamaño y objetivos de la organización.*
- *¿Un solo documento o varios documentos más pequeños?*
  - *Documentos más pequeños, más fáciles de mantener/actualizar*
- *Alguna políticas son genéricas, otras son específicas para ciertos entornos*
- *Algunas políticas clave:*
  - *Uso aceptable*
  - *Acceso remoto*
  - *Protección de información*
  - *Seguridad perimetral*
  - *Seguridad básica para hosts/dispositivos*

Política de Uso Aceptable

- *Define el uso aceptable del equipo y de los servicios de cómputo, y las medidas apropiadas de los empleados para proteger los recursos e información propiedad de la organización.*
- *Se debe pedir a los usuarios leer y firmar la conformidad con la política de uso aceptable como parte del proceso de crear una cuenta.*
- *Es una política clave que todos los sitios debe tener.*
- *Ejemplo de contenido:*
  - *1.0 Introducción*
  - *2.0 Propósito*
  - *3.0 Ambito*
  - *4.0 Política*
    - *4.1 Uso general y propiedad*
    - *4.2 Información propietaria*
    - *4.3 Uso inaceptable*
  - *5.0 Sanciones*

Algunos elementos

- *Debe establecer las responsabilidades de los usuarios en relación a la protección de la información contenida en sus cuentas*
- *Debe establecer si los usuarios pueden leer y copiar archivos que no son de su propiedad, pero son accesibles a ellos.*
- *Debe establecer el nivel de uso aceptable del correo electrónico y acceso a Internet.*
- *Debe discutir uso aceptable de recursos de la empresa para fines ajenos a la misma.*
- *Ejemplo: http://www.sans.org/resources/policies/*

Política de Uso Aceptable

4.0 Política

4.1 Uso general y propiedad

1. *[...]*
3. *Se recomienda que cualquier información que los usuarios consideren confidencial sea cifrada. Para lineamientos de clasificación de información consultar (...). Para lineamientos sobre cifrado de datos y documentos consultar (...).*
4. *Para propósitos de mantenimiento de la red y la seguridad, el personal autorizado de <Compañia> puede monitorear equipos, sistemas y tráfico de red en cualquier momento.*
5. *<Compañia> se reserva el derecho de auditar redes y sistemas de forma periodica para asegurar el cumplimiento de esta política.*

Política de Uso Aceptable

4.2 Seguridad e Información Propietaria

1. *[...]*
2. *Mantener seguras la contraseñas y no compartir cuentas. Los usuarios autorizados son responsables de la seguridad de sus cuentas y contraseñas. Las contraseñas de sistema deberán ser cambiadas quincenalmente, las de usuarios deberán cambiarse semestralmente.*
3. *Todas las PC, laptops, estaciones de trabajo deberan asegurarse con un protector de pantalla protegido con contraseña configurado con activación automática en 10 minutos o menos, o con desconexión automática (logoff) cuando los equipos estén desatendidos.*
4. *[...]*

Política de Uso Aceptable

4.3 Uso Inaceptable

Las siguientes actividades están estrictamente prohibidas, sin excepción:

1. *Violaciones de derechos de autor sobre [...]*
2. *Copiado no autorizado de material con derechos de autor incluyendo, pero no limitado a [...]*
3. *Introducción de programas maliciosos en la red o en servidores.*
4. *Revelar la contraseña de usuario a otros o permitir el uso de la cuenta a terceros.*
5. *Utilizar equipo de computo de <Compañia> para realizar actividades ilegales o fraudulentas.*
6. *Realizar escrutinio de puertos o de seguridad sin autorización previa.*
7. *Efectuar cualquier forma de monitoreo de red que intercepte datos que no conciernen al empleado. [...]*

Política de Acceso Remoto

- *Define métodos aceptables para conectarse de manera remota a la red interna.*
- *Esencial en organizaciones grandes donde las redes están geográficamente dispersas y se extienden incluso a los hogares.*
- *Debe cubrir todos los métodos disponibles para acceder remotamente a recursos internos:*
  - *Dial-in (SLIP,PPP)*
  - *ISDN/Frame Relay*
  - *Acceso mediante Telnet/SSH*
  - *Cable modem/vpn/DSL*

Algunos elementos

- *Debe definir quienes tienen permitido el acceso remoto*
- *Debe definir que métodos son permitidos para el acceso remoto*
- *Debe discutir quienes tienen permitido el acceso remoto de banda ancha tal como ISDN, frame relay o cable modem*
  - *Requerimientos extra*
  - *Uso apropiado*
- *Debe discutir las restricciones sobre datos que puedan ser accesados remotamente.*

Política de Protección de Información

- *Proporciona una guía a los usuarios sobre el procesamiento, almacenamiento y envío de información.*
- *El principal objetivo es asegurar que la información es protegida adecuadamente contra modificaciones o revelación.*
- *Puede ser apropiado hacer que los empleados nuevos firmen conformidad con la política.*
- *Debe definir niveles de confidencialidad de la información.*

Algunos elementos

- *Debe definir quienes tienen acceso a información confidencial.*
  - *Mínimo privilegio (need-to-know)*
  - *Circunstancias especiales*
  - *Acuerdos de confidencialidad*
- *Debe definir como será almacenada y transmitida la información confidencial (cifrado, manejo de medios, etc.)*
- *Debe definir en que sistemas se almacenará información confidencial.*

Algunos elementos

- *Debe discutir que niveles de información confidencial puede imprimirse en impresoras físicamente inseguras.*
- *Debe definir como debe removerse información confidencial de los sistemas y de medios de almacenamiento:*
  - *Demagnetización de medios de almacenamiento*
  - *“Limpiado” de discos duros*
  - *Triturado de copias duras*
- *Debe discutir permisos por defecto para directorios y archivos compartidos.*

Política de Seguridad Perimetral

- *Describe, en general, el mantenimiento de la seguridad perimetral.*
- *Describe quien es el responsable del mantenimiento de la seguridad perimetral.*
- *Describe como se administran los cambios de hardware y software en los dispositivos de seguridad perimetral.*

Algunos elementos

- *Debe discutir quien tiene acceso privilegiado a sistemas de seguridad perimetral.*
- *Debe discutir el proceso para solicitar un cambio de configuración en un dispositivo de seguridad perimetral y como es aprobada la solicitud.*
- *Debe discutir a quien se permite obtener información concerniente a la configuración perimetral y listas de acceso.*
- *Debe discutir el proceso de revisión periodica de configuración de sistemas de seguridad perimetral.*

Política de Código Malicioso

- *Proporciona requerimientos básicos para la utilización de software antivirus.*
- *Proporciona guias para reportar y manejar infecciones de virus.*
- *Debe discutir la política para la descarga e instalación de software de dominio público.*
- *Debe discutir la frecuencia en las actualizaciones de los archivos de datos sobre virus.*
- *Debe discutir el procedimiento de verificación para la instalación de software nuevo.*

Política de Plan de Contingencias

- *Establece objetivos en caso de contingencias.*
- *Elementos claves de la política son:*
  - *Roles y responsabilidades*
  - *Ambito de los planes de contingencia*
  - *Requerimientos de recursos y adiestramiento*
  - *Programación de pruebas y ejercicios*
  - *Programación de mantenimiento*
  - *Frecuencia de realización de respaldos de medios, localización de almacenamiento, convención de etiquetado, frecuencia de rotación de medios y método de transporte offsite.*

Aspectos de implementación de políticas

- *El personal tiende a ver las políticas como:*
  - *Impedimento a la productividad*
  - *Medidas de control*
- *El personal puede tener diferentes opiniones sobre la necesidad de los controles de seguridad.*
- *Las políticas deben afectar a todos en la organización.*
- *Deben tener un fundamento legal y estar apoyadas por el departamento de RH.*
- *En México, cuidar aspectos relacionados con la Ley de Transparencia y Acceso a la Información.*

Procedimientos de Seguridad

- *Las políticas solo definen que será protegido. Los procedimientos definen como se protegerán los recursos y los mecanismos para hacer cumplir las políticas.*
- *Los procedimientos definen en detalle las acciones a tomar en caso de incidentes específicos.*
- *Los procedimientos proporcionan una referencia rápida en el momento de un incidente.*
- *Los procedimientos eliminan el problema de que un empleado clave esté ausente cuando ocurra un incidente de seguridad !!*

Planes de Contingencia

- *La organización debe utilizar un conjunto de planes para preparar adecuadamente la respuesta, recuperación y continuidad de actividades ante una interrupción que afecte los sistemas informáticos, los procesos y las instalaciones.*
- *Términos similares:*
  - *Business Continuity Planning (BCP)*
  - *Disaster Recovery Planning (DRP)*
  - *Business Resumption Planning (BRP)*
  - *Contingency Planning (CP)*
  - *Etc., etc.*

Proceso de Planeación de Contingencia

- *Realizar análisis de impácto en el negocio*
- *Desarrollar la política de planes de contingencia.*
- *Identificar e implementar controles preventivos*
- *Desarrollar estrategias de recuperación*
- *Desarrollar plan de contingencia*
- *Prueba, adiestramiento y ejercicios del plan.*
- *Mantenimiento del plan.*

Proceso de Planeación de Contingencia

- *Realizar análisis de impacto en el negocio*
  - *Identificar recursos críticos*
  - *Identificar impacto de intermisión y tiempos permisibles de suspensión*
  - *Desarrollar prioridades de recuperación*
- *Desarrollar la política de planes de contingencia.*
  - *Identificar requerimientos regulatorios*
  - *Establecer políticas de planeación de contingencias*
  - *Obtener aprobación de la política*
  - *Publicar la política*
- *Identificar controles preventivos*
  - *Implementar controles*
  - *Mantenimiento de controles*

Proceso de Planeación de Contingencia

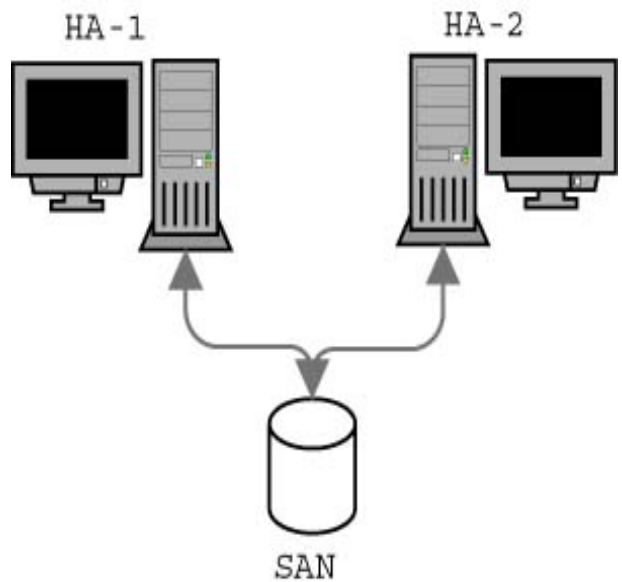
- *Desarrollar estrategias de recuperación*
  - *Identificar métodos*
  - *Integrar a la arquitectura*
- *Desarrollar plan de contingencia*
  - *Documentar estrategias de recuperación*
- *Prueba, adiestramiento y ejercicios del plan.*
  - *Establecer objetivos de la prueba*
  - *Establecer criterios de éxito*
  - *Documentar lecciones aprendidas*
  - *Incorporarlas al plan*
  - *Entrenar al personal*
- *Mantenimiento del plan.*

Controles Preventivos

- *Fuentes de poder ininterrumpibles (UPS)*
- *Generadores basados en gasolina o diesel.*
- *Sistemas de aire acondicionado*
- *Sistemas de supresión de incendios*
- *Detectores de fuego y humo*
- *Sensores de agua*
- *Cubiertas plásticas para equipo de cómputo*
- *Almacenamiento offsite de respaldo de medios, registros no electrónicos y documentación*
- *Respaldos periodicos, frecuentes*

Estrategias de Recuperación

- *Métodos de respaldo*
  - *respaldo de medios*
  - *caja fuerte electrónica*
  - *mirroring de discos/hosts*
- *Sitios alternos*
  - *Cold sites*
  - *Warm sites*
  - *Hot sites*
  - *Mobile sites*
  - *Mirrored sites*



Estrategias de Recuperación

- *Reemplazo de equipo*
  - *Acuerdos con provedores*
  - *Equipo almacenado*
  - *Equipo compatible existente*
- *Roles y responsabilidades*

Pruebas, entrenamiento y ejercicios

- *Prueba del plan – Hace posible identificar y resolver deficiencias del plan.*
  - *Establecer objetivos y criterios de éxito.*
  - *Escenario: Puede ser el del peor caso o el del caso más probable.*
  - *Debe imitar la realidad tan cercanamente como sea posible.*
- *Entrenamiento – El personal que apoya el plan debe recibir adiestramiento para que sean capaces de ejecutar sus respectivos procedimientos de recuperación.*

Pruebas, entrenamiento y ejercicios

- *Ejercicios – Se realizan con el objetivo de adiestrar y preparar a los miembros del equipo.*
  - *Table Top – Los participantes revisan y discuten las acciones que tomarán, sin realizar ninguna de estas acciones.*
  - *Simulación – Los participantes realizan algunas o todas las acciones que se tomarán al hacerse la activación del plan.*
  - *Operativo – Los participantes realizan algunas o todas las acciones, bajo condiciones operativas reales.*
  - *Desastre mofa – Los participantes son retados a determinar las acciones que realizarian en caso de un escenario específico de desastre. Pueden realizar o simular las acciones.*

Componentes del Plan

- *Información de Apoyo*
  - *Introducción*
  - *Concepto de Operaciones*
- *Fase de Notificación/Activación*
  - *Procedimientos de notificación*
  - *Evaluación de daño*
  - *Activación del plan*
- *Fase de recuperación*
  - *Secuencia de actividades de recuperación*
  - *Procedimientos*
- *Fase de reconstitución*
  - *Restaurar sitio original*
  - *Probar sistemas*
  - *Terminación de operaciones*

Información de Apoyo

- *Introducción*
  - *Propósito – Objetivos del plan.*
  - *Aplicabilidad – Areas impactadas por el plan.*
  - *Ambito – Problemas, aspectos y situaciones consideradas. Sistema(s) y sitios cubiertos.*
  - *Registro de cambios – Modificaciones realizadas al plan.*
- *Concepto de Operaciones*
  - *Descripción del sistema – Descripción general del sistema cubierto por el plan.*
  - *Línea de sucesión – Personal responsable de asumir la autoridad para ejecutar el plan en caso dela persona designada no esté disponible.*
  - *Responsabilidades – Equipo, jerarquia, roles y responsabilidades.*

Fase de Notificación/Activación

- *Procedimientos de Notificación – Deben describir los métodos utilizados para notificar al personal de recuperación durante horario normal y fuera de horario.*
  - *Call tree*
- *Evaluación de daños – Describir procedimientos de evaluación de daños.*
  - *Causas de la emergencia o interrupción*
  - *Potencial de interrupciones o daño adicional*
  - *Area(s) afectada(s) por la emergencia*
  - *Status de infraestructura física*
- *Activación del plan – Debe activarse si y solo si se satisfacen uno o más de los criterios de activación del plan. Los criterios de activación son únicos para cada organización.*

Fase de Recuperación

- *Inicia una vez que:*
  - *El plan ha sido activado*
  - *Se ha evaluado el daño (si es posible)*
  - *El personal ha sido notificado*
  - *Se han movilizado los equipos adecuados*
- *Secuencia de actividades de recuperación –*
  - *Los procedimientos de recuperación deben reflejarlas prioridades establecidas por el BIA.*
  - *Deben escribirse por pasos, en forma secuencial de manera que los componentes del sistema sean restaurados de forma lógica.*
  - *Deben incluir instrucciones para coordinar equipos.*

Fase de Reconstitución

- *Inicia una vez que han terminado las actividades de recuperación y las operaciones normales se han transferido de vuelta a las instalaciones de la organización.*
- *Si la instalación original es irrecuperable, actividades de preparación de nuevas instalaciones.*
- *Principales actividades:*
  - *Asegurar infraestructura adecuada*
  - *Instalar hardware, software y firmware*
  - *Establecer conectividad con red y sistemas externos*
  - *Probar operaciones de los sistemas*
  - *Respaldar datos operacionales del sistema de contingencia y subirlos al sistema restaurado.*
  - *Dar de baja el sistema de contingencia*
  - *Terminar operaciones de contingencia*
  - *Asegurar, remover y/o relocalizar todos los materiales sensibles del sitio de contingencia.*

Consideraciones Técnicas

1. Computadoras de escritorio y portatiles:

- *Documentar configuraciones de sistema y de aplicaciones*
- *Estandarizar hardware, software y periféricos*
- *Proporcionar asesoría sobre respaldo de datos*
- *Asegurar la interoperabilidad de componentes*
- *Coordinar con políticas de seguridad y controles*
- *Respaldar datos y almacenar fuera de sitio*
- *Usar discos duros alternos*
- *Discos imágen*
- *Implementar redundancia en componentes críticos*
- *Utilizar fuentes de poder ininterrumpibles*

Consideraciones Técnicas

2. Servidores:

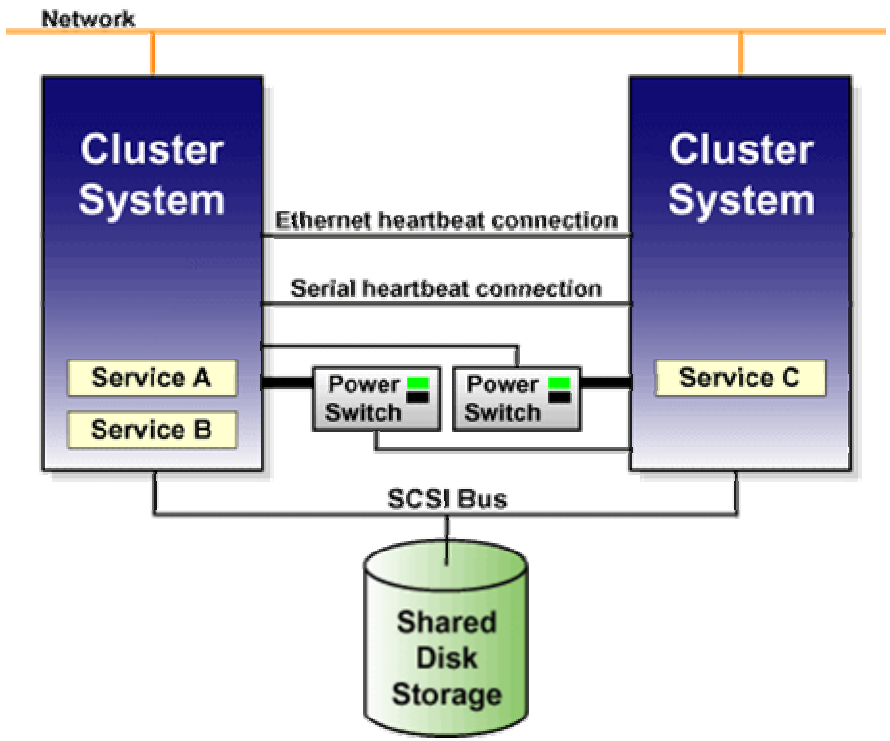
- *Documentar configuraciones de sistema y aplicaciones*
- *Estandarizar hardware, software, y periféricos*
- *Coordinar con políticas y controles de seguridad*
- *Asegurar interoperabilidad entre componentes*
- *Respaldar datos y almacenar fuera de sitio*
- *Respaldar aplicaciones y almacenar fuera de sitio*
- *Usar fuentes ininterrumpibles de poder*
- *Implementar redundancia en componentes de sistema críticos*
- *Implementar tolerancia a fallas en componentes de sistema críticos*
- *Replicar datos*
- *Implementar soluciones de almacenamiento*

Tecnología de contingencia en servidores

- *Respaldos:*
  - *Completo*
  - *Incremental*
  - *Diferencial*
- *RAID*
  - *Tecnicas de redundancia:*
    - *Mirroring*
    - *Paridad*
    - *Striping*
- *RAID-0 solo striping*
- *RAID-1 solo mirroring*
- *RAID-2 striping a nivel de bits*
- *RAID-3 striping a nivel bit con paridad dedicada*
- RAID-4 striping a nivel de bloque con paridad dedicada
- RAID-5 striping a nivel de bloque y paridad distribuida
- Discos *hot-swap*
- Fuentes de poder redundantes
- Caja fuerte electrónica
- Balanceo de carga en servidores
- Virtualización:
  - Network-attached storage (NAS)
  - Storage area network (SAN)
  - Internet SCSI (iSCSI)

Clustering

- ***Cluster:*** *Conjunto de servidores que se comportan como un solo servidor. Típicamente utilizado para lograr alta disponibilidad o alto desempeño.*
- *Cluster de alta disponibilidad:*



Tecnología de Clustering

- *Sun Cluster 3*
- *IBM High Availability Cluster Multiprocessing (HACM) para AIX*
- *Compaq TruCluster Server*
- *Kimberlite http://www.missioncriticallinux.com/products/cluster.php*
- *Linux HA http://www.linux-ha.org/*
- *Sistemas Legato http://www.veritas.com/*
- *PolyServe http://www.polyserve.com/*
- *Windows 2000 Advanced Server y Datacenter Server*

Componentes de un sistema HA

- Componentes de un sistema de alta disponibilidad:
  - Servicios de membresía
  - Servicios de comunicación
  - Administración de cluster
  - Monitoreo de recursos
  - Administración de recursos
  - Almacenamiento replicado/compartido:
    - Compartido: SCSI compartido, SAN, etc.
    - Replicado:
      - Protocolo de aplicación (DNS, NIS, etc.),
      - Rsync
      - Drbd, nbd, etc.

Estrategias de Tolerancia a Fallas

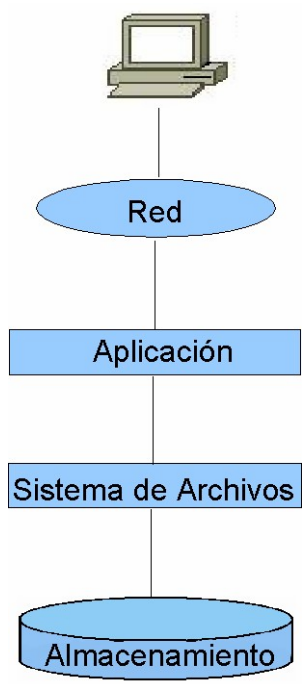
- *Espera inactiva – Nodo de respaldo permanece inactivo, monitoreando al nodo activo (heartbeat). Un nodo es prioritario.*
- *Espera rotatoria – Como en espera inactiva pero sin prioridades en nodo.*
- *Fallover simple – Nodo de respaldo corre aplicaciones no críticas.*
- *Takeover mutuo – Es básicamente una espera inactiva de dos vias.*
- *Acceso concurrente – Todos los nodos están activos y accesan el almacenamiento externo concurrentemente. (Oracle Parallel Server).*

Estrategias de Tolerancia a Fallas

- Redundancia en conexión de red
  - Takeover de dirección IP (IPAT)
  - Takeover de dirección MAC
  - Heartbeat
    - UDP
    - No IP:
      - Cable RS232 null modem corriendo TTY
- Opciones de almacenamiento
  - DAS – Direct Attached Storage
  - NAS – Network Attached Storage
  - SAN – Storage Area Network

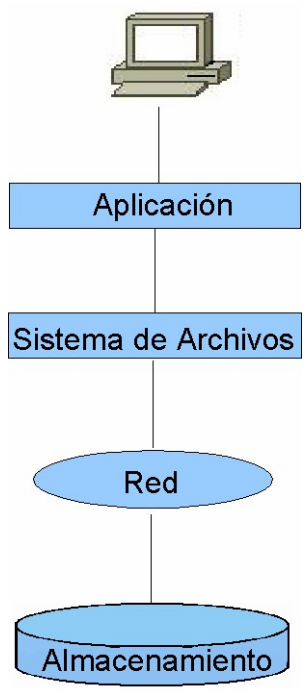
DAS Direct Attached Storage

- *Método tradicional de conectar el almacenamiento a un servidor mediante un canal de comunicación dedicado entre el servidor y el dispositivo de almacenamiento.*
  - *Ejemplo, SCSI*
  - *Discos, RAID u otro*
  - *Interfaz a nivel bloque*



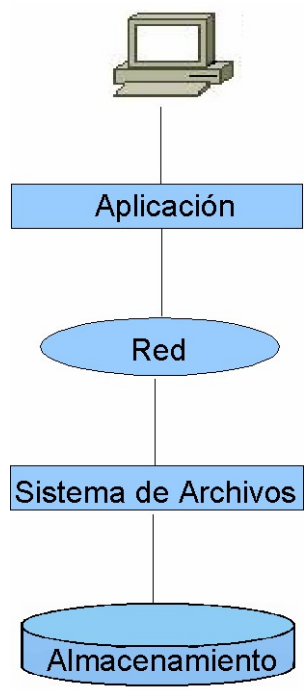
SAN Storage Area Network

- *Red dedicada de almacenamiento diseñada específicamente para conectar almacenamiento, dispositivos de respaldo y servidores.*
  - *Redes conmutadas Fibre Channel*
  - *Localizado o disperso*
  - *Interfaz a nivel bloque*
  - *Sistema de archivos en servidor*



NAS Network Attached Storage

- *Arreglo de almacenamiento con su propio sistema de archivos se conecta directamente a la red.*
  - *Interfaz de sistemas de archivos de red*
    - *NFS (UNIX)*
    - *SMB/CIFS (WinNT/Win2k)*
  - *Utiliza RPCs*



SAN versus NAS

- *SAN*
  - *Orientado a bloques*
  - *Basado en Fibre Channel*
  - *Almacenamiento protegido y aislado de acceso de clientes*
  - *Servidores de alto desempeño*
  - *Instalación compleja*
- NAS
  - Orientado a archivos
  - Basado en Ethernet
  - Provisto para acceso general de clientes
  - Soporta aplicaciones cliente NFS/CIFS de bajo desempeño
  - Puede instalarse rápida y fácilmente

Consideraciones Técnicas

3. Servidores Web:

- *Documentar el sitio web*
- *Coordinar con políticas y controles de seguridad*
- *Considerar contingencias de la infraestructura que lo soporta*
- *Implementar balanceo de cargas*
- *Elaborar procedimientos de respuesta a incidentes*

4. Redes de área local (LAN)

- *Documentar la red*
- *Coordinar con políticas y controles de seguridad*
- *Identificar puntos de falla únicos*
- *Implementar redundancia en componentes críticos*
- *Monitorear la LAN*
- *Integrar tecnología de WLAN y acceso remoto*

Consideraciones Técnicas

5. Redes de área amplian (WAN):

- *Documentar WAN*
- *Coordinar con provedores*
- *Coordinar con políticas y controles de seguridad*
- *Identificar puntos de falla únicos*
- *Instalar redundancia en componentes críticos*
  - *Redundancia en enlaces*
  - *Redundancia en provedores de servicios de redes*
  - *Redundancia en dispositivos de enlace*
  - *Redundancia en ISPs*
- *Instituir SLAs. (Service Level Agreement)*

Respuesta a Incidentes

- *Incidente de seguridad – Una violación real o potencial de una política de seguridad explícita o implícita.*
- *Categorías de incidentes:*
  - *Acceso incrementado*
  - *Revelación de información*
  - *Corrupción de información*
  - *Denegación de servicios*
  - *Robo de recursos*
- *Proceso de respuesta a incidentes (de acuerdo a FedCIRC)*
  - *Fase 1: Detección, evaluación y canalización (triage)*
  - *Fase 2: Contención, recolección de evidencia, análisis e investigación, y mitigación.*
  - *Fase 3: Corrección, recuperación, post-mortem.*

Respuesta a Incidentes

- *Fase 1: Detección, evaluación y canalización.*
  - *Paso 1-1: Documentar todo. Registrar todo lo que ocurre en detalle: nombres, fechas, y eventos. Puede ser notas manuscritas y no inicialmente ordenadas.*
  - *Paso 1-2: Contactar IRT primario. En ausencia de un IRT interno, debe contactarse a un IRT externo.*
  - *Paso 1-3: Preservar evidencia. Asegurar integridad y disponibilidad de la evidencia.*
  - *Paso 1-4: Verificar el incidente. Basándose en los datos disponibles, establecer si ha ocurrido o no un incidente.*
  - *Paso 1-5: Notificar al personal apropiado. Seguir plan de notificación de incidentes.*

Respuesta a Incidentes

- *Fase 1: Detección, evaluación y canalización.*
  - *Paso 1-6: Determinar estado del incidente. ¿Está áctivo el incidente?*
  - *Paso 1-7: Evaluar ámbito. Determinar cuales y cuantos sistemas fueron afectados.*
  - *Paso 1-8: Evaluar riesgo. Considerar que está en riesgo basándose en la actividad del incidente.*
  - *Paso 1-9: Establecer objetivos. Dependiendo de la actividad puede incluir preservar la reputación, proteger datos clasificados, asegurar disponibilidad, etc.*
  - *Paso 1-10: Evaluar opciones.*
  - *Paso 1-11: Implementar canalización.*
  - *Paso 1-12: Escalamiento y pase.*

Respuesta a Incidentes

- *Fase 2: Contención, recolección, análisis y mitigación.*
  - *Paso 2-1: Verificar contención. Validar que la contención y las actividades de canalización fueron efectivas.*
  - *Paso 2-2: Revisar ámbito, riesgos y objetivos.*
    - *¿Cómo? ¿Cuándo? ¿Quién?*
    - *¿Existió actividad después del incidente inicial?*
    - *¿Quién fue el origen del ataque?*
    - *¿Recomendaciones inmediatas y futuras?*
  - *Paso 2-3: Recolectar evidencias. Identificar y capturar datos relevantes a la investigación del incidente.*
    - *Bitácoras de cortafuegos, IDS, DHCP, correo, etc.*
    - *Evidencia externa: ISPs, web hosters, etc.*

Respuesta a Incidentes

- *Fase 2: Contención, recolección, análisis y mitigación.*
  - *Paso 2-4: Analizar evidencia. Altamente dependiente de la experiencia, herramientas y conocimiento del equipo investigador.*
  - *Paso 2-5: Plantear y verificar hipótesis. Formular respuestas hipotéticas a las preguntas planteadas en el paso 2-2. Deben estar soportadas en lo posible por la evidencia.*
  - *Paso 2-6: Mitigación intermedia. De acuerdo a lo crítico de la situación, y a las prioridades y disponibilidad de recursos, pueden aplicarse algunas recomendaciones de mitigación mientras la investigación prosigue.*

Respuesta a Incidentes

- *Fase 3: Finalizar análisis y reporte.*
  - *Paso 3-1: Archivar evidencia. Toda la evidencia debe ser almacenada en forma segura.*
  - *Paso 3-2: Implementar correcciones. Corregir vulnerabilidades identificadas durante la investigación. Pueden incluir acciones a mediano y a largo plazo.*
  - *Paso 3-3: Ejecutar recuperación. Si un incidente ha resultado en la destrucción o corrupción de datos, será necesaria la recuperación.*
  - *Paso 3-4: Post-mortem. Reporte final del incidente, incluyendo lecciones aprendidas.*

Prevención de Incidentes

- *Uno de los aspectos centrales en la Política de Seguridad.*
- *Aproximadamente un 80% de intrusiones se podrían evitar si se aplicáran parches conocidos.*
- *La evaluación periodica de vulnerabilidades debe formar parte de la política de seguridad.*
- *La aplicación sistemática de parches debe formar parte de los procedimientos de seguridad.*
- *Se debe realizar la suscripción a servicios de notificación de vulnerabilidades:*
  - *CERT advisories. http://www.cert.org/contact_cert/certmaillist.html*

Auditoria de SI

La auditoria de seguridad informática tiene como objetivos:

- Detectar las vulnerabilidades y los puntos de fallo que pueden representar una amenaza para la seguridad de un sistema de información.
- Determinar las medidas necesarias para mejorar la seguridad del sistema de información.

Etapas de la Auditoria

La auditoria se realiza en tres etapas:

- Recolección de datos.
- Análisis y pruebas adicionales.
- Elaboración de reporte.

Recolección de Datos

La etapa de recolección de datos incluye, entre otras, las siguientes actividades:

- Mapeo de la red
- Identificación de sistemas
- Escrutinio de puertos
- Muestreo de tráfico
- Detección de vulnerabilidades
- Recolección de políticas y procedimientos de seguridad

Mapeo de la red

Se determinan:

- Enlaces de datos
- Ruteadores y firewalls
- Dispositivos de red
- Rangos de direcciones
- Dominios y DNS
- ISPs

Identificación de Sistemas

Para cada equipo en la red se determina:

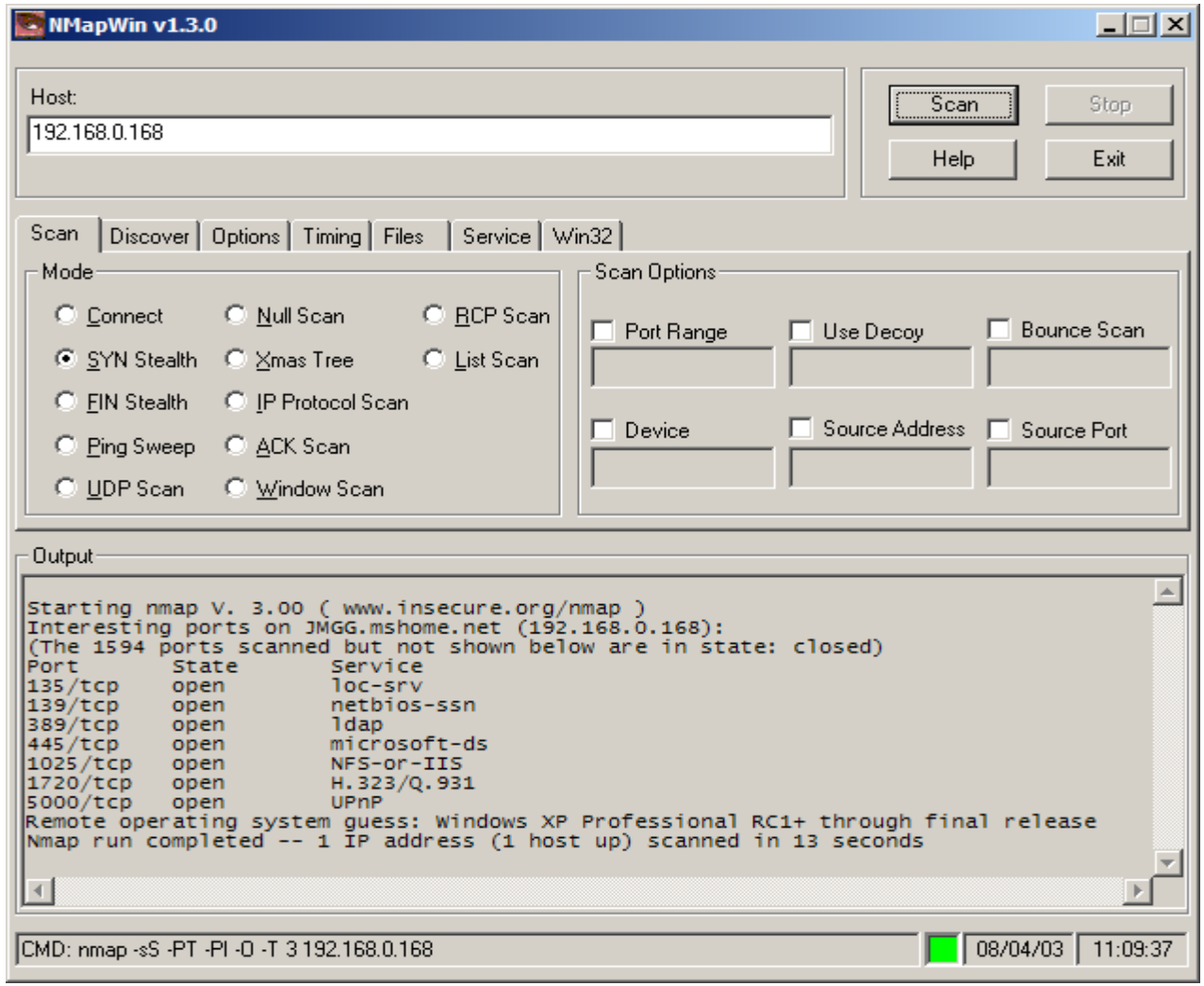
- Sistema operativo, versión y actualizaciones instaladas.
- Versiones de firmware y fabricante en caso de dispositivos de red.

Escrutinio de Puertos

En cada equipo se detecta:

- Puertos abiertos (TCP, UDP, ICMP)
- Servicios disponibles (ftp, http, dns, etc.)
- Protocolos utilizados (incluyendo versiones)
- Recursos compartidos (NetBIOS, NFS, etc.)
- Aplicaciones específicas

Escrutinio de Puertos



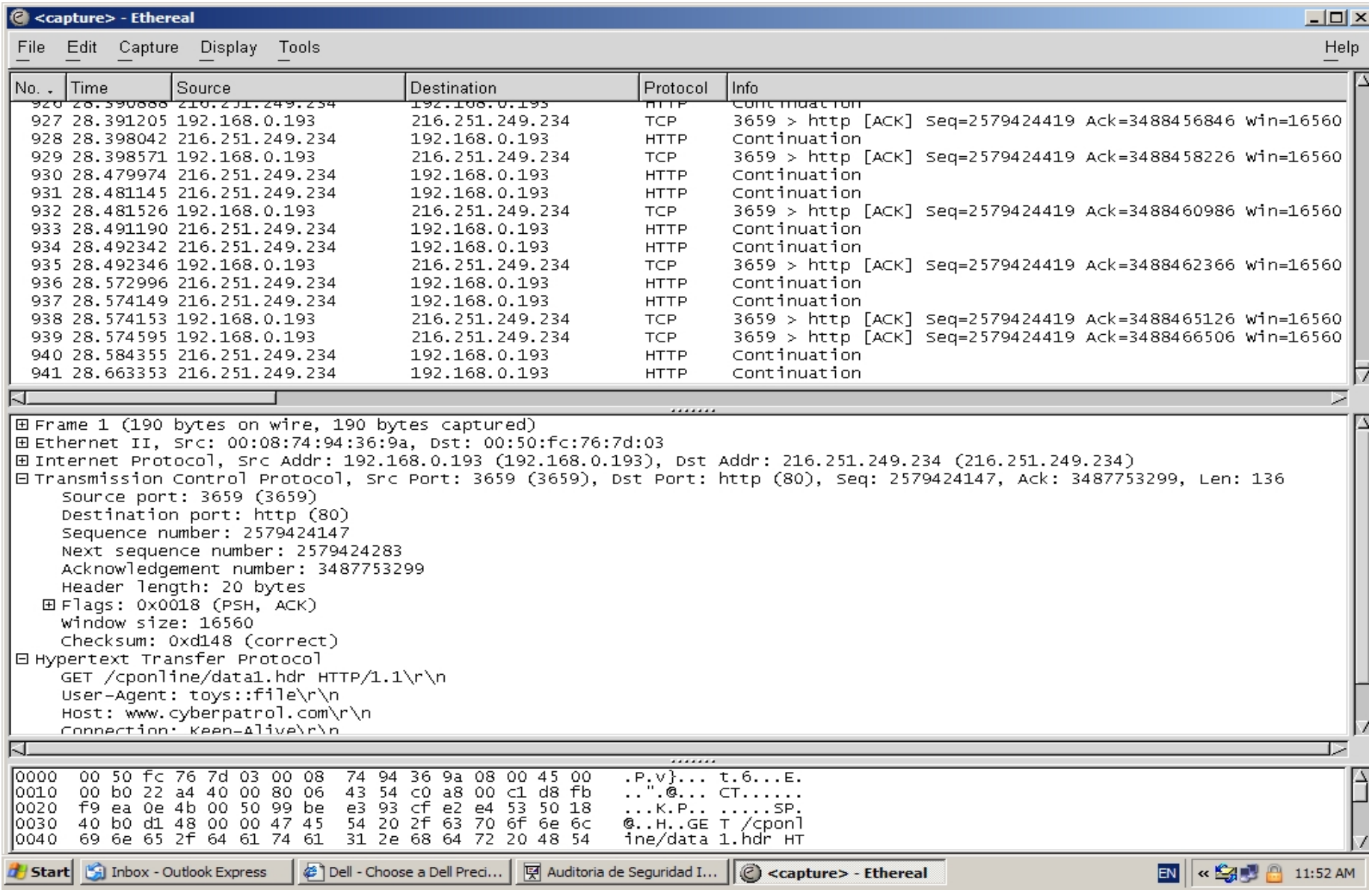
Muestreo de Tráfico

Para cada segmento de la red:

- Se captura una muestra del tráfico de red.
- Se clasifica la muestra obtenida.
- Posteriormente, en la etapa de análisis, se analizan los paquetes obtenidos para determinar posibles compromisos de seguridad.

Muestreo de Tráfico

SEKUREIT
CONSULTORES EN SEGURIDAD INFORMATICA

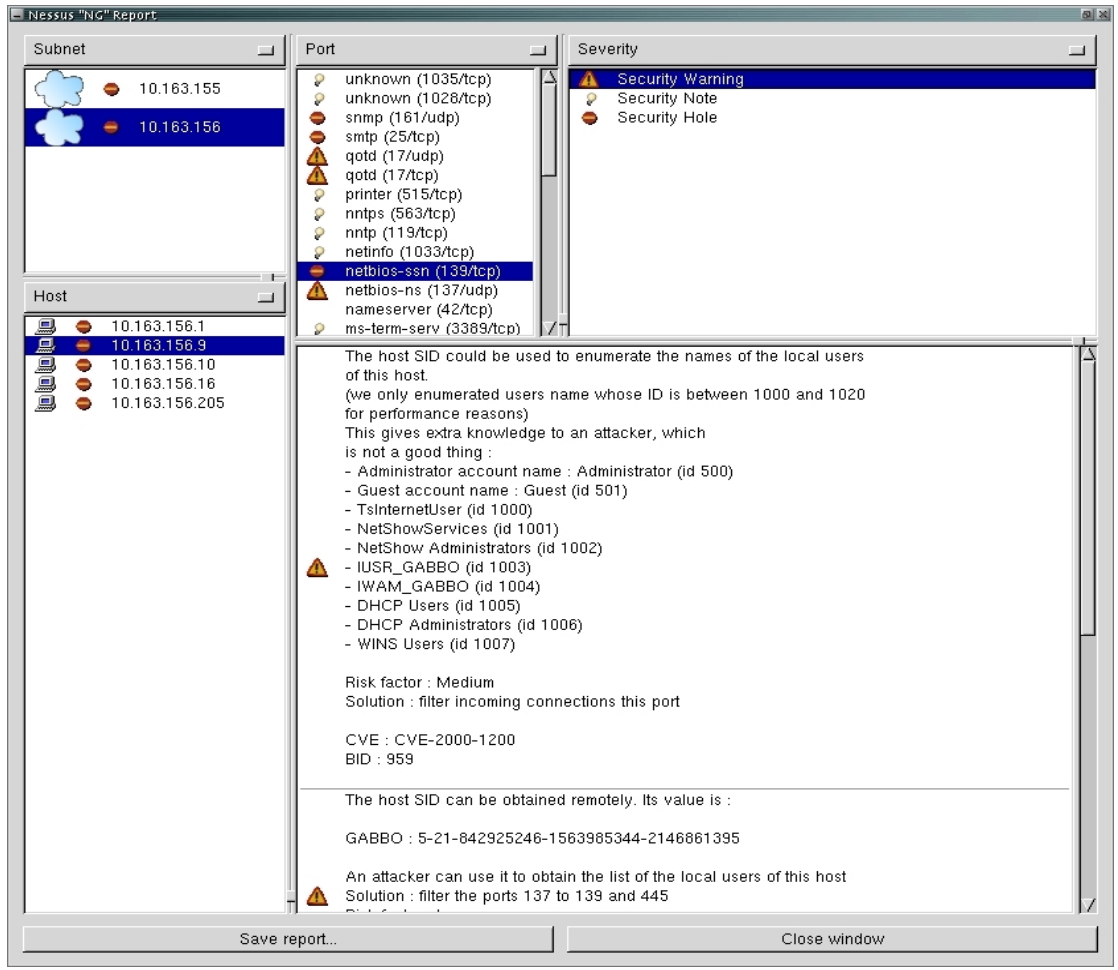


Detección de Vulnerabilidades

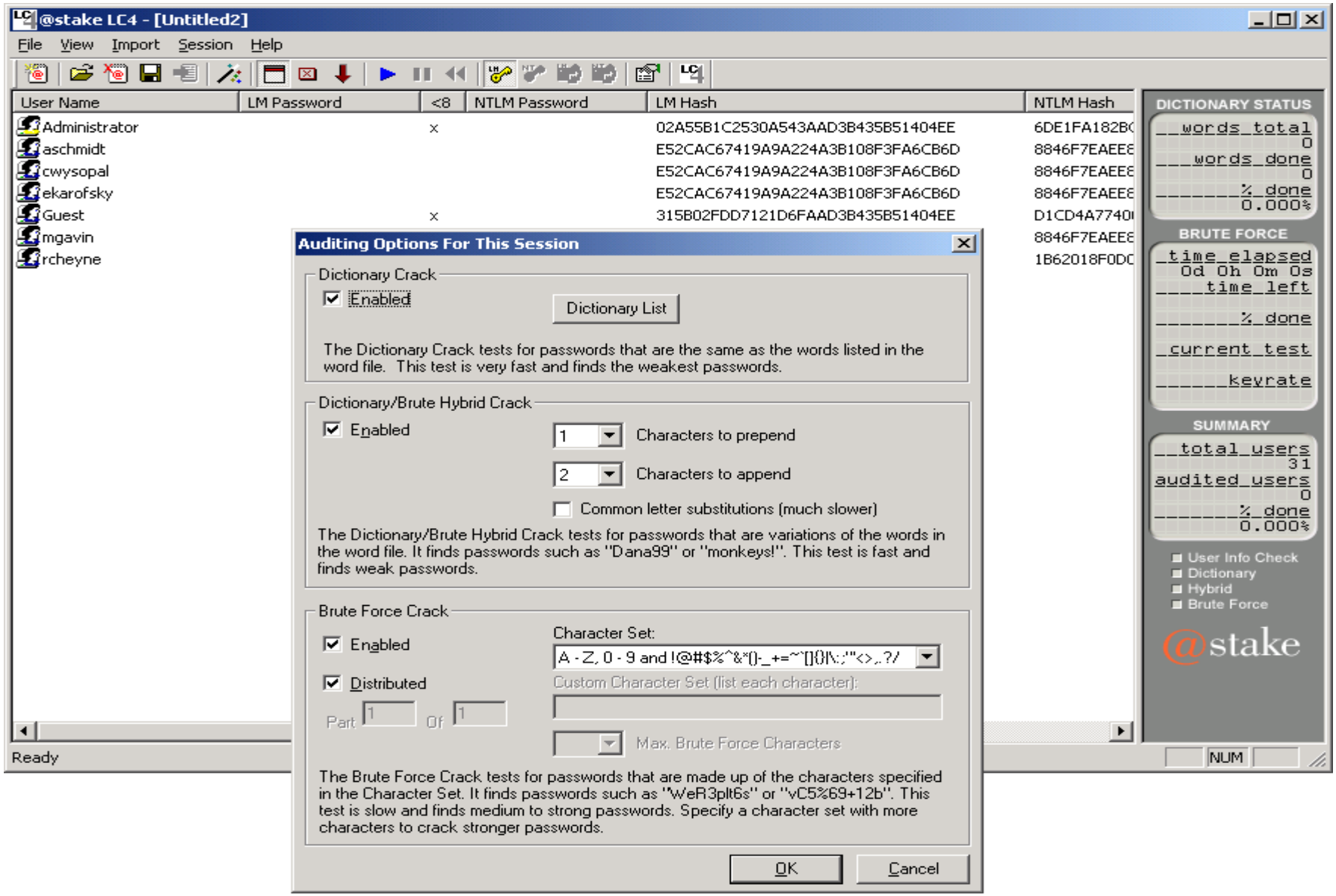
Se realiza en dos partes:

- Detección automatizada:
  - Se utilizan varias herramientas para la detección automática de vulnerabilidades.
- Detección manual:
  - En base a las vulnerabilidades reportadas por las herramientas, se prueba su posible explotación.

Detección de Vulnerabilidades



Rompimiento de Contraseñas



Análisis y Pruebas Adicionales

Durante la etapa de análisis se incluyen las siguientes actividades:

- Análisis de Vulnerabilidades.
- Análisis de Bitácoras.
- Análisis de Tráfico.
- Análisis de Permisos y Control de Acceso.
- Análisis de Políticas y Procedimientos de Seguridad.

Análisis de Vulnerabilidades

En base a los datos obtenidos, se determina la posibilidad de:

- Intrusiones
- Fugas de información
- Ataques de denegación de servicio
- Puntos de falla únicos
- Propagación de código malicioso (virus, gusanos, troyanos, etc.)

Análisis de Vulnerabilidades

Las vulnerabilidades se clasifican en:

- De bajo riesgo, solo implican la fuga de información de menor importancia.
- De medio riesgo, pueden ocasionar el mal funcionamiento o interrupción temporal de los servicios.
- De alto riesgo, pueden ocasionar el *compromiso total* de los sistemas.

Análisis de Bitácoras

A partir de las bitácoras de los servidores se determina:

- Registro detallado de eventos de seguridad.
- Indicios de actividad sospechosa o rastros de compromisos anteriores.
- Posibles fallas de hardware o del software del sistema.
- Interrupciones abruptas en el funcionamiento de los sistemas.

Análisis de Tráfico

De la muestra de tráfico se determinan:

- Estadísticas de tráfico
- Tráfico susceptible de intercepción
- Posibles fugas de información
- Actividad sospechosa
- Puntos de falla únicos (*cuellos de botella*)

Análisis de Control de Acceso

En esta parte se analizan:

- Permisos en directorios y recursos compartidos
- Uso de contraseñas fuertes
- Listas de control de acceso en dispositivos de red
- Reglas de filtraje de paquetes en los cortafuegos.

Políticas y Procedimientos

Las políticas y procedimientos de seguridad deben incluir:

- Políticas de uso adecuado de los recursos.
- Políticas de privacidad.
- Políticas de asignación de privilegios.
- Planes de contingencia.
- Planes de recuperación.

Análisis de Políticas

Se analizan las políticas y procedimientos de seguridad para determinar:

- Su aplicación y seguimiento.
- Su pertinencia respecto a la situación actual del sistema de información.
- Si existe normas respecto a su cumplimiento.

Reporte Final

El reporte final incluye:

- Información detallada de las vulnerabilidades encontradas y los potenciales problemas de seguridad que pueden darse.
- Recomendaciones para prevenir tales problemas:
  - Actualizaciones
  - Procedimientos
  - Herramientas

Programa de Inducción

- Objetivos:
  - Los empleados reconocen su responsabilidad en la protección de los activos informáticos de la organización.
  - Entienden el valor de la seguridad informática.
  - Reconocen potenciales violaciones y saben a quien contactar.
  - El nivel de conciencia respecto a la SI permanece alto entre los empleados.

Programa de Inducción

- Diseño del programa:
  - Plantear una estrategia
  - Determinar necesidades de la organización
    - Evaluar necesidades
    - Incorporar resultados de revisiones
  - Desarrollar un plan de inducción y adiestramiento
    - Identificar audiencias, delimitar ámbito, establecer prioridades, comprometer a la admon.

Programa de Inducción

- Desarrollar material de inducción:
  - Aspectos de políticas y guias
    - El programa es dependiente de la política
    - Revisar aspectos legales y contractuales !!
  - Aspectos de infraestructura y logística
    - Capacitación in-situ o externa
    - Inducción a distancia o basada en web
  - Fuentes: Advisories, websites de seguridad, revistas, etc.

Certificaciones

- (ISC)2 CISSP, SSCP
- GIAC GSE
- CompTIA Security+
- ISACA CISM, CISA
- SCP SCNP, SCNA
- CERT CCSIH
- Cisco CCSP
- Microsoft MCSA, MCSA

Certificaciones $(ISC)^2$

- $(ISC)^2$ *Internet Information System Security Certification Consortium*
  - Certificación CISSP – “Reconoce el dominio de un estándar internacional de seguridad informática y entendimiento de un cuerpo común de conocimiento (CBK)”
  - Certificación SSCP – Se enfoca en prácticas, roles y responsabilidades tal como se han definido por expertos en la industria de SI.

Dominios CISSP

- Son cubiertos los diez dominios siguientes:
  - Metodologia y sistemas de control de acceso
  - Desarrollo de sistemas y aplicaciones
  - Planeación de continuidad del negocio
  - Criptografia
  - Leyes, investigación y ética
  - Seguridad de operaciones
  - Seguridad física
  - Modelos y arquitectura de seguridad
  - Prácticas de administración de la seguridad
  - Seguridad de telecomunicaciones, redes e Internet

Dominios SSCP

- Son cubiertos los siete dominios siguientes:
  - Controles de acceso
  - Administración
  - Auditoria y monitoreo
  - Riesgo, respuesta y recuperación
  - Criptografia
  - Comunicaciones de datos
  - Código malicioso

GIAC Security Expert

- GIAC – *Global Information Assurance Certification, SANS.*
- Abarca un conjunto de habilidades tales como:
  - Auditoria
  - Detección de intrusos
  - Manejo de incidentes
  - Cortafuegos y seguridad perimetral
  - Forensia
  - Técnicas de hackers
  - Seguridad en Windows y Unix
- Se evalua a través de diferentes tareas (*assignaments*)

CompTIA Security+

- CompTIA – *Computing Technology Industry Association*.
- Se evalua:
  - Dominio del área de seguridad informática
  - Dos años de experiencia profesional
- Tópicos cubiertos en el examen:
  - Conceptos generales
  - Seguridad de comunicaciones
  - Seguridad de infraestructura
  - Bases de criptografia
  - Seguridad operacional/organizacional

ISACA CISM, CISA

- ISACA – *Information System Audit and Control Association*
  - CISM – Certified Information Security Manager
    - Planeación de la seguridad informática
    - Administración de riesgos
    - Administración del programa de SI
    - Administración de respuestas de SI
  - CISA – Certified Information Security Auditor

SCP SCNP, SCNA

- SCP – *Security Certified Program*
  - SCNP – Security Certified Network Professional
    - Diseño e implementación de IDS
    - Tráfico de red
    - Análisis de vulnerabilidades
    - Diseño e implementación de cortafuegos
    - Seguridad de ruteadores
    - Seguridad de sistemas operativos
    - Conocimiento avanzado de TCP
    - Bases de seguridad en redes
  - SCNA – Security Certified Network Architect
    - VPNs, criptografia, PKI, autenticación biometrica, etc.

CERT CCSIH

- CERT – *Computer Emergency & Response Team*
  - *CCSIH Certified Computer Security Incident Handler*
  - *Requerimientos:*
    - *Cuatro cursos obligatorios:*
      - *Creación de un CSIRT*
      - *SI para staff técnico*
      - *Administración de CSIRTs*
      - *Manejo de incidentes avanzado*
    - *Curso optativo:*
      - *Forensia*
      - *Detección y análisis de intrusiones*
      - *Auditorias y evaluaciones de seguridad*
    - *Tres años de experiencia, carta de recomendación, examen.*

Cisco CCSP

- CCSP – *Cisco Certified Security Professional*
  - *Prerrequisitos: CCNA o CCIP*
  - *Examenes:*
    - *Securing Cisco IOS Networks*
    - *Cisco Secure PIX Firewall Advanced*
    - *Cisco Secure Intrusion Detection System*
    - *Cisco Secure VPN*
    - *Cisco SAFE Implementation*

Microsoft MCSA, MCSE

- MCSA – *Microsoft Certified System Administrator*
  - *Core: (3 examenes)*
    - *Sistemas operativos cliente*
    - *Redes*
  - *Especialización en seguridad (2 examenes)*
    - *Implementación y administración de seguridad en redes de Windows 2000.*
    - *Instalación, configuración y administración de ISSA Server 2000 o CompTIA Security+*
- *MCSE – Microsoft Certified Security Engineer*
    - *Sistema operativo cleinte (1 examen)*
    - *Redes de windows (3 examenes)*
    - *Diseño de seguridad (1 examen)*
    - *Especialización en seguridad (2 examenes)*

Gracias por su atención

http://www.sekureit.com