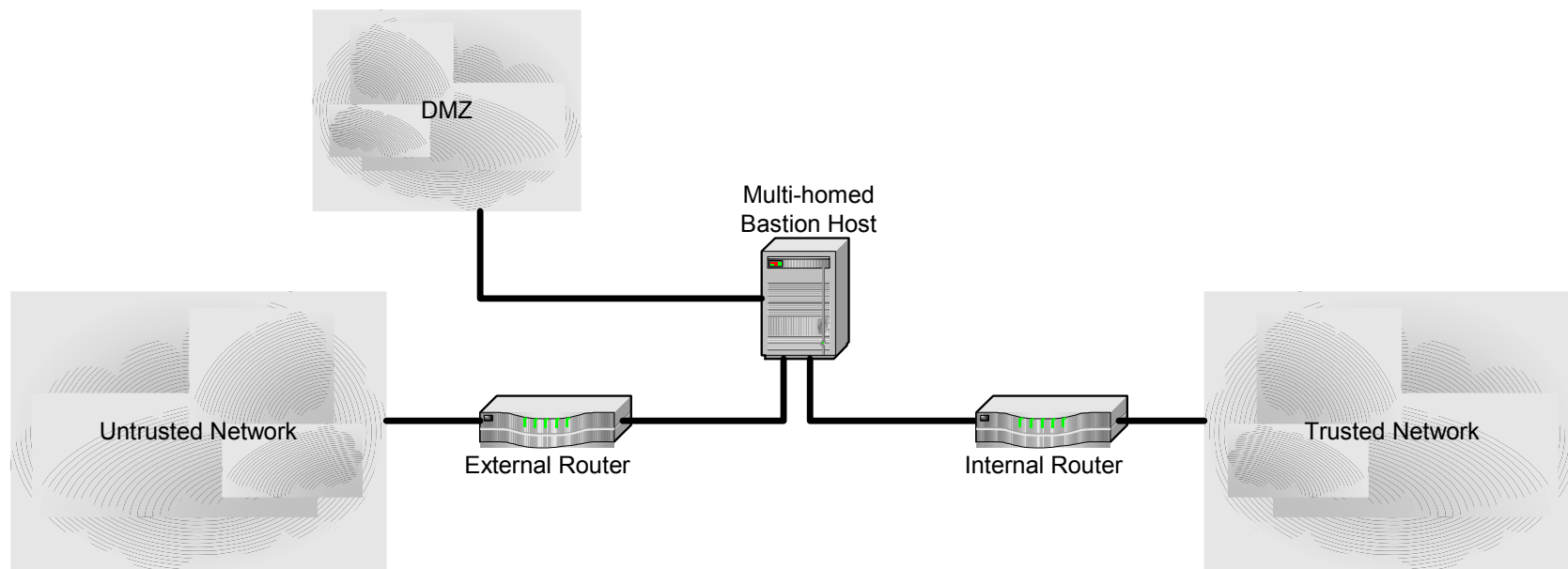


Arquitecturas de Firewalls

- Screened-Subnet Firewalls (with a DMZ)



Redes Privadas Virtuales

Redes Privadas Virtuales

Redes Privadas Virtuales

■ Concepto

- Define un túnel seguro entre dos entes.
- Provee confidencialidad y autenticación.
- Requiere de un sistema de encriptación para operar.
- Se utiliza sobre redes públicas (por ej. Internet).
- Normalmente se define a nivel de capa 3 (Red) o 2 (Enlace de Datos) del modelo de referencia OSI.

Estándares de VPN

- Point-to-Point Tunneling Protocol (PPTP).
 - Conexiones individuales entre cliente y servidor.
 - Designados para sistemas operativos de Microsoft.
 - Capa 2 (Enlace de Datos) del modelo de referencia OSI.
 - Utiliza los servicios de autenticación y encriptación nativos del Point-to-Point Protocol (PPP).

Estándares de VPN

- Layer 2 Tunneling Protocol (L2TP).
 - Combinación de PPTP y Layer 2 Forwarding Protocol (L2F).
 - Conexiones individuales entre cliente y servidor.
 - Capa 2 (Enlace de Datos) del modelo de referencia OSI.
 - Permite el encapsulamiento de múltiples protocolos de red.

Estándares de VPN

■ IPsec.

- Capa 3 (Red) del modelo de referencia OSI.
- Permite la generación y utilización de múltiples túneles en forma simultánea.
- Encripta y Autentica datos IP.
- Provee encriptación, autenticación, control de accesos y no-repudio.
- Define dos protocolos:
 - Authentication Header.
 - Encapsulating Security Payload.

Dispositivos VPN

- Se instalan en el perímetro de la red.
- Encripta el tráfico entre redes o nodos.
- Dos Modos de Operación:

- Modo Túnel.

El paquete IP completo es encriptado y encapsulado dentro de un paquete de IP Sec.

- Modo Transporte.

Solo el área de datos es encriptada, la información de ruteo (direcciones IP) se mantiene visible.

Seguridad de Acceso Remoto

Seguridad de Acceso Remoto

- Conectividad Dial-up, Async y remota a Internet.
 - Digital Subscriber Line (xDSL).
 - Integrated Services Digital Network (ISDN).
 - Wireless Computing.
 - Cable modems.
- Brindar Seguridad a la organización para permitir el tele-trabajo.
 - Asegurar conexiones externas (VPN, SSL, SSH-2).
 - Utilizar Sistemas de Autenticación de Acceso Remoto (RADIUS, TACACS, etc).

Métodos de Seguridad de Acceso Remoto

- Restricción de dirección.

Este procedimiento filtra conexiones no autorizadas basandose en la dirección de red de donde provienen.

- Caller ID.

El número de teléfono utilizado para generar la llamada es contrastado contra una lista de números de teléfonos aprobados antes de aceptar la comunicación.

- Callback.

El usuario al iniciar la sesión provee información de autenticación que es utilizada para devolver la llamada y finalizar el establecimiento de la conexión.

Autenticación de Accesos Remotos

- Terminal Access Controller Access Control System (TACACS).
- TACACS+
- Remote Authentication Dial-in User Server (RADIUS).

Autenticación de Accesos Remotos

- Terminal Access Controller Access Control System (TACACS).
 - Protocolo de Autenticación que provee Autenticación de Accesos Remotos.
 - Las contraseñas de los usuarios son administradas en una base de datos centralizada.
 - No permite el cambio de contraseñas, ni la utilización de autenticación de dos factores.
 - Código de dominio público.

Autenticación de Accesos Remotos

■ TACACS+

- Mejoras propietarias de CISCO al protocolo TACACS.
- Mejor sistema de auditoria y contabilidad de accesos.
- Permite el cambio de contraseñas.
- Permite la utilización de autenticación de dos factores.
- Código de dominio público.

Autenticación de Accesos Remotos

- Remote Authentication Dial-in User Server (RADIUS).
 - Protocolo estándar del IETF (Internet Engineering Task Force).
 - Características similares a las de TACACS+
 - RADIUS no soporta:
 - Autenticación de dos-factores.
 - AppleTalk Remote Access Protocol (ARAP).
 - NetBIOS Frame Control Protocol (NBFCP).
 - NetWare Asynchronous Services Interface (NASI).
 - Conexiones a PADs X.25.

Ataques y Abuso de Red

Ataques y Abuso de Red

- Clase A: Acceso no autorizado a servicios restringidos de red mediante la circumbención de controles de acceso.
 - También llamado “abuso de logon”
 - Se trata de usuarios legítimos accediendo a servicios normalmente restringidos a ellos.
 - Usualmente es considerado un ataque interno.

Ataques y Abuso de Red

- Clase B: Uso no autorizado de la red con fines no relacionados con el negocio.
 - Generalmente considerado abuso del sistema.
 - Es difícil marcar una línea que determine claramente que es negocio y que no.

Ataques y Abuso de Red

- Clase C: Moitoreo (Eavesdropping).
 - Intercepción no autorizada del tráfico de la red.
 - Tipos:
 - Monitoreo Pasivo: monitoreo subrepticio de transmisiones no autorizadas, ya sea por el emisor o receptor de la transmisión.
 - Monitoreo Activo: alteración/ modificación de una transmisión con el objetivo de crear un covert signaling channel, o realizar un mapeo de la red en forma activa con el fin de obtener información estructural de la misma (*probing*).

Ataques y Abuso de Red

- Clase D: Negación de Servicios y otras interrupciones de servicios.
 - Objetivo: disponibilidad de la red/ sistema.
 - Normalmente realizado mediante la sobrecarga de una red/ sistema: Slammer.
 - Distributed DoS.

Ataques y Abuso de Red

- Clase E: Intrusiones de Red.
 - Se refiere al uso de accesos no autorizados para penetrar en una red.
 - Normalmente es un ataque externo.

Ataques y Abuso de Red

- Clase F: Probing
 - Es una variante activa de Eavesdropping.
 - Se utiliza para preparar un mapa de la red a atacar.

Ataques de Negación de Servicios

- Buffer Overflow Attack.
- SYN Attack.
- Teardrop Attack.
- Smurf.

Session Hijacking

- IP Spoofing Attack.
- TCP Sequence Number Attack.

Tecnologías de Seguridad Informática

Criptografía

Conceptos de Criptografía

- **Propósito:** Proteger información de forma tal que solo quien esta autorizado pueda leerla y comprenderla.
- En el caso ideal toda persona no autorizada a dicha información nunca podrá sacar provecho de dicha información.
- En el mundo real, el costo (tiempo, recursos) de lectura de dicha información es mayor que el valor que se obtiene de su lectura.

Conceptos de Criptografía

■ Criptografía.

1. Arte de escribir en forma secreta de un modo enigmático (Diccionario General de la Lengua Española Vox).
2. El arte o ciencia de esconder el significado de una comunicación de personas no autorizadas. La palabra criptografía viene del griego, *kryptos* (escondido) y *graphein* (escribir).

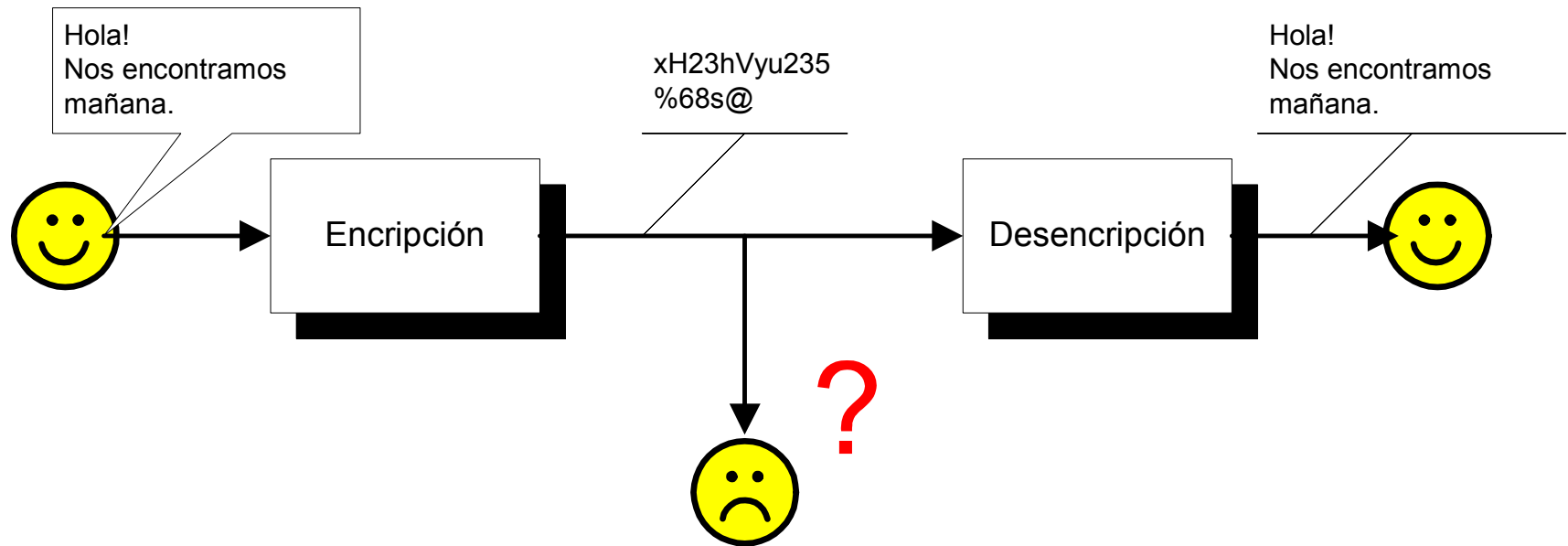
■ Criptoanálisis.

- El acto de obtener el *texto-plano* o *llave* de un *texto-cifrado* utilizado para obtener información, normalmente valiosa, que fuera originalmente encriptada.

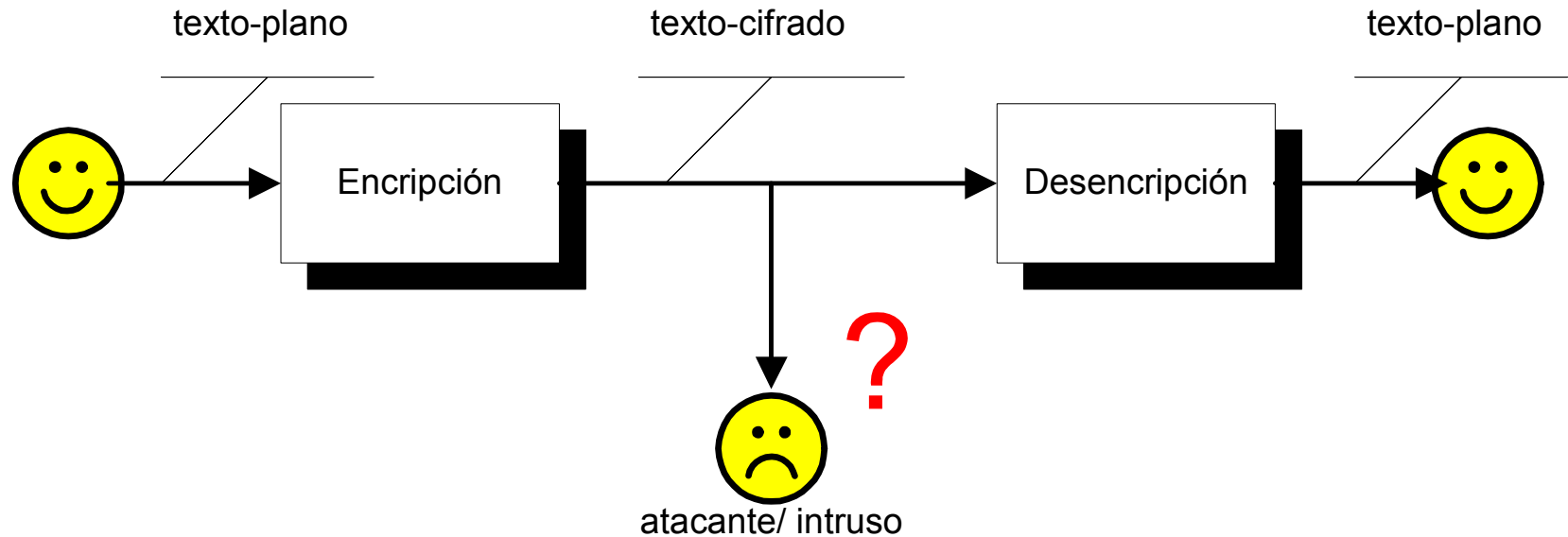
Conceptos de Criptografía

- Criptología.
 - Criptografía + Criptoanálisis.
- Sistema Criptográfico.
 - Conjunto de transformaciones de un espacio de mensaja a un espacio de texto-cifrado.

Conceptos de Criptografía



Conceptos de Criptografía



Operaciones Criptográficas

■ Substitución.

- Sustituir un elemento del alfabeto del texto-plano por uno que corresponde al alfabeto del texto-cifrado.

Texto-plano: DONALD

Texto-cifrado: GRQDOG

A → D D → G ...

B → E E → H ...

C → F F → I ...

Operaciones Criptográficas

- Transposición (Permutación).
 - Permuta los caracteres del texto plano.

Texto-plano: “ESTE ES UN MENSAJE DE PRUEBA!”

Texto-cifrado: “UARSNJUTMEEEEEDBENEASSP!”

E	S	T	E	E	S
U	N	M	E	N	S
A	J	E	D	E	P
R	U	E	B	A	!

Substitución

- Mantiene el mismo patrón de frecuencias del alfabeto original (para caracteres simples, y combinaciones conocidas).
 - Tipo de Ataque: análisis de frecuencias.
- Pueden utilizarse múltiples alfabetos.

Transposición.

- Mantiene el mismo patrón de frecuencias del alfabeto original (para caracteres simples).
 - Tipo de Ataque: análisis de frecuencias.
- Oculta la relación estadística de conjuntos de caracteres.
Ej: ion, the...
- Pueden utilizarse múltiples alfabetos.

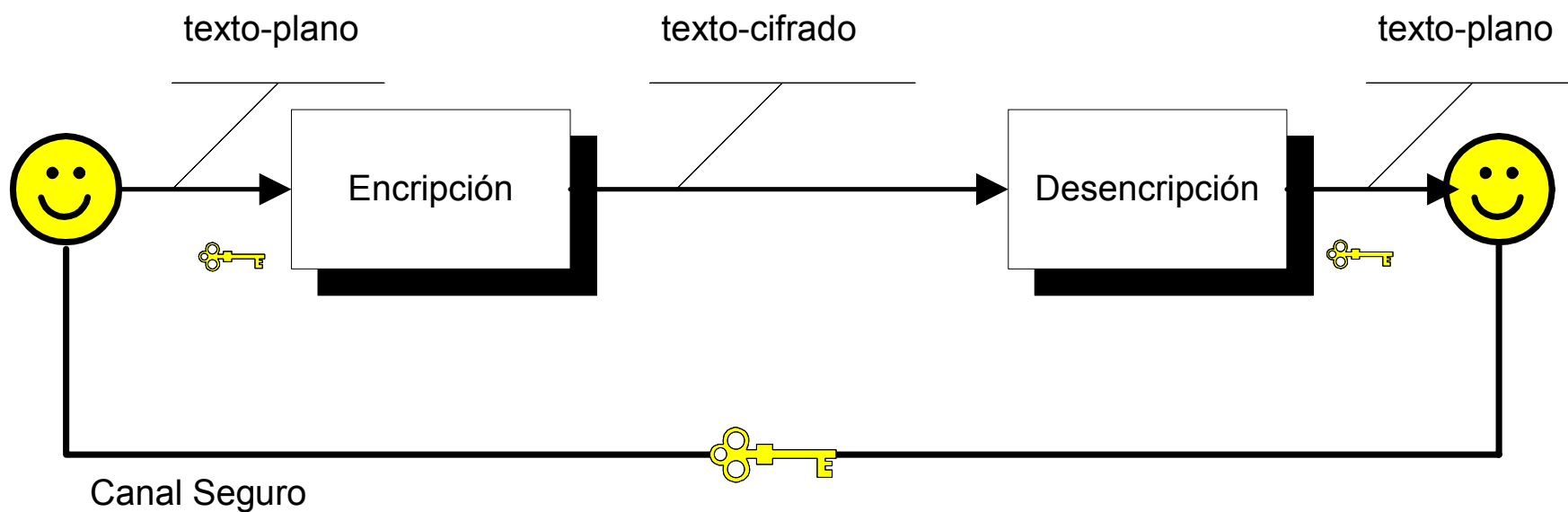
Componentes de un sistema Criptográfico

- Algoritmo de encriptación.
- Algoritmo de desencriptación.
- Llave de encriptación/ desencriptación.

Sistemas Criptográficos

- Sistemas Simétricos (de llave privada).
 - Ambas partes (emisor y receptor) comparten la misma llave de encriptación/ desencriptación.
 - Requiere de un canal seguro para poder compartir la llave.
- Sistemas Asimétricos (de llave pública).
 - Dos llaves.
 - Llave pública, utilizada para encriptar.
 - Llave privada, utilizada para desencriptar.

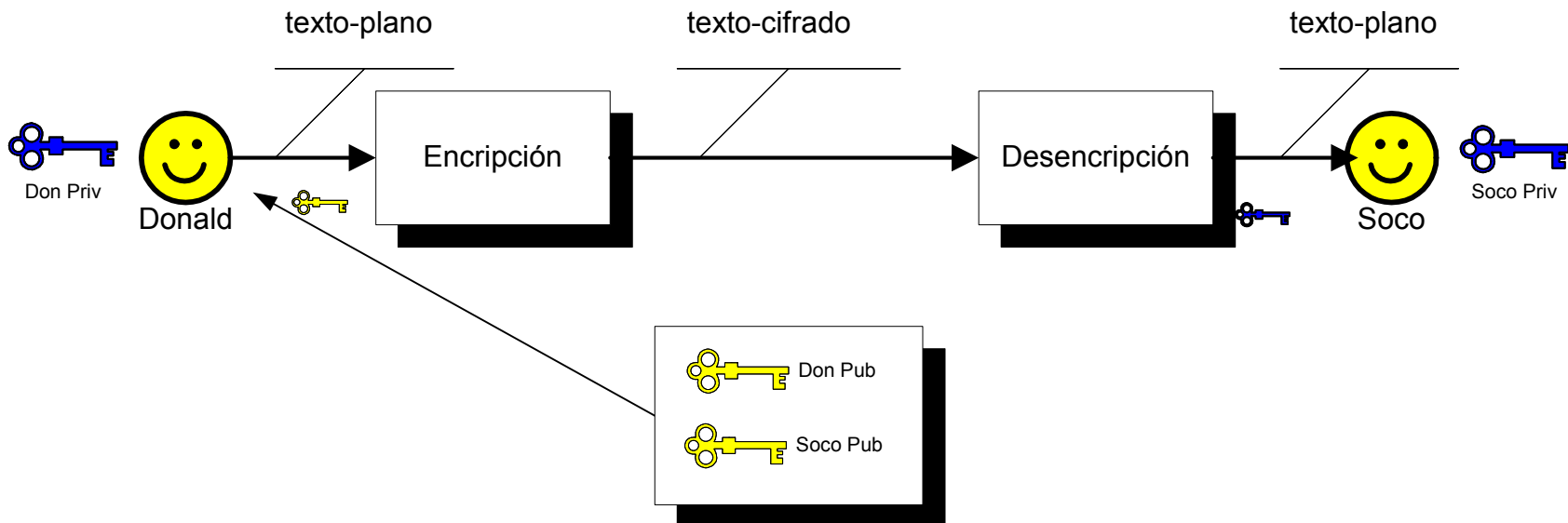
Criptografía Simétrica



Criptografía Simétrica

- Data Encryption Standard.
 - En uso desde 1976.
 - Bloques de 64 bits.
 - Llave de 56 bits.
 - Otras opciones: Triple DES.
- Advanced Encryption Standard: Rijndael.
 - Seleccionado como reemplazo del DES desde Oct-2000.
 - Bloques de: 128, 192 o 256 bits.
 - Llave de: 128, 192 o 256 bits.

Criptografía Asimétrica (de llave pública)



Criptografía Asimétrica (de llave pública)

- Utiliza un par de llaves relacionadas.
- Condiciones:
 - La llave pública no puede descifrar el mensaje que encripta.
 - Idealmente, la llave privada no se puede derivar de la llave pública.
 - Un mensaje encriptado con una llave puede ser descifrado con la otra llave asociada.
 - La llave privada es mantenida privada.

Criptografía Asimétrica (de llave pública)

- RSA (Rivest-Shamir-Addleman).
 - Basado en la dificultad de factorizar un número N , producto de dos números primos grandes.
- Diffie-Hellman Key Exchange.
 - Se utiliza para intercambiar llaves en forma segura.
- El Gamal.
 - Extiende a DH habilitando la encriptación y el manejo de firmas digitales.

Comparación de longitud de llaves

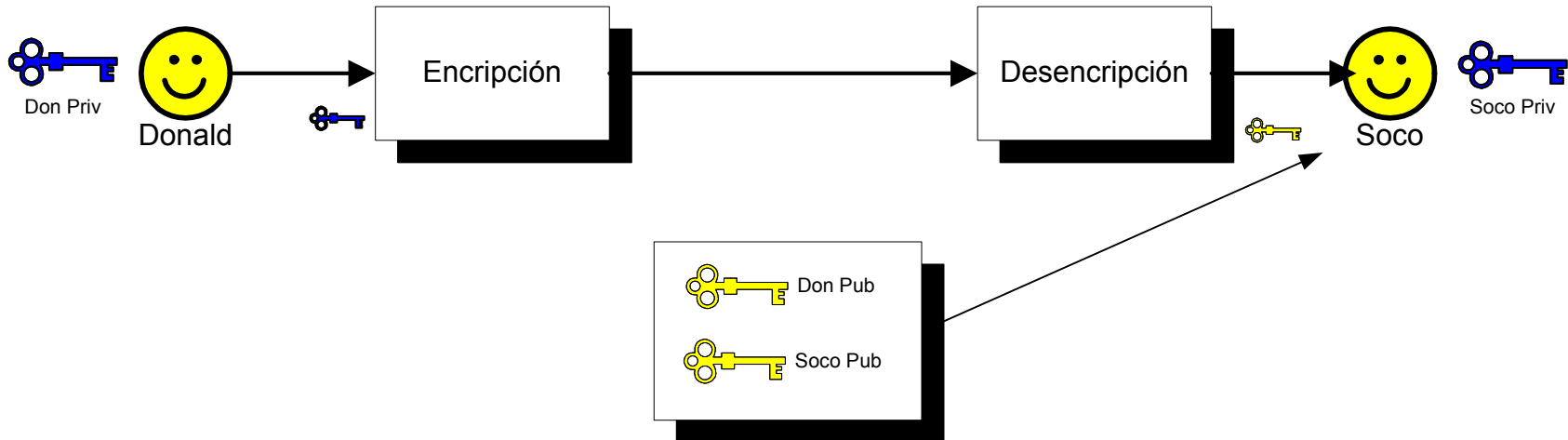
Asimétrico	Simétrico
512	64
1792	112
2304	128

bits

Firmas Digitales

- A fin de asegurar la autenticidad del mensaje que se esta enviando, este se puede firmar en forma digital.
- Un message digest (MD) es generado utilizando una función hash (de un solo sentido).
- Este MD es encriptado con la llave privada del emisor y anexado al mensaje original.
- El destinatario al recibir el mensaje, recalcula el MD y lo compara contra el recibido (previamente descriptado con la llave pública del emisor),

Firmas Digitales



Ataques Criptográficos

- Fuerza bruta.
- Texto-Plano conocido.
- Texto-Plano elegido.
- Solamente Texto-Cifrado.
- Texto-Cifrado conocido.
- Otros...

Tecnologías de Seguridad Informática

Seguridad Operacional

Seguridad Operacional

- Seguridad Operacional refiere al acto de comprender las vulnerabilidades y amenazas de las operaciones de los centros de cómputo/ computadoras con el objetivo de dar soporte a dichas actividades que son las que permiten que los sistemas funcionen adecuadamente.
- Este dominio se concentra en aquellos controles que permiten proteger el *hardware*, *software* y los *medios de almacenamiento de datos*.

Controles de Operaciones

- Protección de Recursos.
- Controles de Hardware.
- Controles de Software.
- Controles de Entidades-Privilegiadas.
- Controles de Medios.
- Controles de Acceso Físico.

Protección de Recursos

- Hardware.
 - Comunicaciones.
 - Medios de almacenamiento.
 - Sistemas de Procesamiento.
 - Computadoras stand-alone.
 - Otros dispositivos (impresoras, faxes, etc).

Protección de Recursos

- Software.
 - Librerías de Programas y código fuente.
 - Software propietario o de proveedores.
 - Sistemas Operativos y Utilidades de los sistemas.

Protección de Recursos

- Datos.
 - Backups.
 - Archivos de usuario.
 - Archivos de contraseñas.
 - Directorios del sistema operativo.
 - Logs del sistema y rastros de auditoría.

Controles de Hardware

- Mantenimiento de Hardware.
- Cuentas de usuario de mantenimiento.
- Control de puertos de diagnóstico.
- Control físico del hardware.
 - Terminales y estaciones de operación.
 - Gabinetes o armarios en dónde se almacenen datos.
 - Data centers de Servidores y Comunicaciones.
 - Pools de modems y cuartos de cableado de telecomunicaciones.

Controles de Software

- Administración del sistema anti-virus.
- Prueba de software (software testing).
- Utilidades del sistema (system utilities).
- Almacenamiento seguro de software/ datos.
- Controles de Backup.

Controles de Entidades Privilegiadas

- El acceso a entidades privilegiadas, también conocido como *funciones de operación privilegiadas* se define como el acceso especial o extendido a recursos informáticos que se le otorga a operadores y administradores de los sistemas.
- Clases de entidades privilegiadas:
 - Comandos del sistema.
 - Parametros del sistema.
 - Programa de control del sistema (Control Program Management).

Controles de Medios

- Controles de Seguridad de Medios.
 - Registro de uso de medios (logging).
 - Control de accesos a los medios.
 - Eliminación/ borrado. Destrucción apropiada de medios.
- Controles de viabilidad de medios.
 - Etiquetado.
 - Trato (uso, transporte de los medios).
 - Almacenamiento.

Controles de Acceso Físico

- Hardware.
 - Control del equipamiento computacional y de comunicaciones.
 - Control de los medios de almacenamiento.
 - Control de reportes y logs impresos.
- Software.
 - Control de los archivos de backup.
 - Control de las aplicaciones de producción.
 - Control de datos/ información sensible/ crítica.

Controles de Acceso Físico

- Personal.
 - Personal del departamento de IT.
 - Personal de limpieza.
 - Personal de mantenimiento del sistema de A/C.
 - Personal de empresas de servicios contratado.
 - Consultores, proveedores y personal temporario.

Monitoreo y Auditoría

- Monitoreo.
 - Detección de Intrusos.
 - Penetration Testing.
 - Análisis de Violaciones de seguridad.
- Auditoría.
 - Auditorías de Seguridad/ IT.
 - Interna.
 - Externa.
 - Registros de Auditoría (Logs).

Amenazas a la seguridad Operacional

- Pérdida Accidental.
 - Errores u omisiones en inputs de operadores.
 - Errores de procesamiento de transacciones.
- Actividades Inapropiadas.
 - Contenido Inapropiado.
 - Desperdicio/ Uso indebido de recursos corporativos.
 - Sexual/ Racial Harassment.
 - Abuso de privilegios o derechos.

Amenazas a la seguridad Operacional

- Operaciones ilegales y Ataques intencionales.
 - Monitoreo (eavesdropping).
 - Fraude.
 - Robo.
 - Sabotaje.
 - Ataques externos.

Tecnologías de Seguridad Informática

Infosec en el desarrollo de aplicaciones

Infosec en el desarrollo de aplicaciones

- Separación de Ambientes.
- Proceso de Administración de Cambios.
- Testing.
- Controles de Aplicaciones.

Separación de Ambientes

- Ambiente de Desarrollo.
- Ambiente de Pruebas.
- Ambiente de Producción.

Proceso de Administración de Cambios

- Es el proceso responsable del seguimiento y aprobación de los cambios que se realicen en un sistema (hardware. Software).
- Para InfoSec lo importante es que dichos cambios no alteren, en forma negativa, el nivel de seguridad existente. Adicionalmente, es parte de la Administración de Cambios el mantenimiento de la documentación relacionada.

Proceso de Administración de Cambios

- Procedimientos básicos:
 1. Solicitar un nuevo cambio.
 2. Catalogar el cambio solicitado.
 3. Agendar cuando se realizará el cambio.
 4. Implantar el cambio solicitado.
 5. Reportar el resultado de la implantación a todas las partes interesadas.

- Estos procedimientos solo refieren a la generación de un cambio en ambiente de producción.

Testing

- Antes de que cualquier cambio llegue a la etapa de solicitud de implantación, debe haber sido puesto a prueba.
- Aspectos a Testear:
 - Funcionalidad.
 - Seguridad.
 - Compatibilidad.

Controles de Aplicaciones

- Exactitud (accuracy).

La información/ datos ingresados a las distintas aplicaciones deben ser exactas. No debe haber diferencias entre lo que se *tiene* que ingresar y lo que se *ingreso*.

- Seguridad.

Preservar la CID.

- Consistencia.

La información/ datos deben ser consistentes.

Controles de Aplicaciones

Exactitud (accuracy).

- Preventivos:
 - Revisión de datos, formularios, pantallas personalizables, chequeos de validez, etc.
- Detectivos:
 - CRC, totales de hash, comprobaciones de razonabilidad.
- Correctivos:
 - Backups, reportes de control, etc.

Controles de Aplicaciones

Seguridad.

- Preventivos:
 - Firewalls, clasificación de datos, encriptación, separación de ambientes, etc.
- Detectivos:
 - IDS, logs de auditoría.
- Correctivos:
 - Respuesta ante emergencias.

Controles de Aplicaciones

Consistencia.

- Preventivos:
 - Diccionario de datos, estándares de programación, DBMS.
- Detectivos:
 - Controles de comparación, reconciliación.
- Correctivos:
 - Comentarios en programas, controles en base de datos.

Tecnologías de Seguridad Informática

Recuperación ante Contingencias

Recuperación ante Contingencias

- Business Continuity Plan (BCP).
 - Define las acciones a tomar en los casos en que una determinada contingencia inhabilite algún área de operaciones o tecnología.
 - Permite recuperar las operaciones críticas definidas **del negocio**.
 - Incluye el DRP.
- Disaster Recovery Plan (DRP).
 - Define las acciones a tomar en los casos en que una determinada contingencia inhabilite el centro de cómputos.
 - Permite recuperar las operaciones críticas definidas **de IT**.

Recuperación ante Contingencias

- La prioridad número 1 de la recuperación de contingencias es:

La gente siempre esta primero.

Contingencias

- Eventos Naturales.
 - Huracanes, inundaciones, terremotos, incendios.
 - Interrupción de servicios básicos (electricidad, comunicaciones, etc).
 - Incendios, explosiones o derramamiento de toxinas.
- Eventos desatados por personas.
 - Sabotage, bombardeo u otros ataques intencionales.
 - Huelgas, accidentes.
 - Errores.

Business Continuity Plan

Etapas

- Definición de Alcance e Inicio del Plan.
- Evaluación del Impacto en el Negocio (Business Impact Assessment – BIA).
- Desarrollo del Plan.
- Aprobación e Implantación del Plan.
- Prueba y Mantenimiento del Plan.

Roles y Responsabilidades

- Alta Gerencia.
 - Inicia el proyecto, da la aprobación final y apoya la iniciativa a lo largo de todo su ciclo de vida.
- Gerencia de Unidades de Negocio.
 - Identifican y priorizan los sistemas/ operaciones críticas del negocio.
- Comité de BCP.
 - Dirige los procesos de planificación, implantación y prueba del BCP.
- Unidades Funcionales:
 - Participa en la implantación y las pruebas del plan.

Evaluación del Impacto en el Negocio

Objetivos.

- Priorización en base a la criticidad de los procesos/ sistemas.
- Estimación de tiempo máximo de tolerancia (Maximum Tolerable Downtime).
- Requerimientos de Recursos.

Evaluación del Impacto en el Negocio

Tareas.

- Obtención del material necesario para realizar el análisis.
- Desarrollo de una evaluación de vulnerabilidades.
- Análisis de la información obtenida.
- Documentación y reporte de resultados y recomendaciones.

Definición de la Estrategia de Continuidad

- Recursos Informáticos.
 - Hardware, software, comunicaciones, aplicaciones, datos.
- Locaciones.
 - Locaciones alternativas para equipamiento y personal.
- Personal.
 - Cada persona asignada al BCP tendrá funciones específicas para llevar a cabo la ejecución del plan en forma exitosa.
- Equipamiento y suministros.
 - Papel, formularios, A/C, equipamiento de seguridad específico, etc.

Disaster Recovery Plan

Objetivos

- Proteger a la organización de fallas generales de los servicios de información.
- Minimizar el riesgo generado por la demora en la provisión de servicios.
- Garantizar la confianza de los sistemas de backup a través de pruebas y simulaciones.
- Minimizar la toma de decisiones del personal durante una contingencia.

Procesos del DRP

- Planificación de la continuidad del procesamiento de datos.
 - Acuerdos de ayuda mutua.
 - Servicios de Suscripción.
 - Hot Site.
 - Warm Site.
 - Cold Site.
 - Centros múltiples.
 - Service Bureaus.
- Mantenimiento del Plan.

Testeo del Plan

- Checklist.
 - Copias del plan son distribuidas a las gerencias para su revisión.
- Seguimiento estructurado (structured walk-through).
 - Gerentes de las áreas afectadas se reúnen para revisar el plan.
- Simulación.
 - Todo el personal de soporte se reúne en una sesión de práctica.

Testeo del Plan

- Prueba en Paralelo.
 - Los sistemas críticos son ejecutados en el sitio alternativo.
- Interrupción completa.
 - Todos los sistemas en producción son interrumpidos. Se procede a ejecutar el plan en condiciones reales.

Equipos de Trabajo

- Equipo de Recuperación.
 - Responsable de ejecutar los procedimientos de recuperación ante la declaración de un desastre.
- Equipo de Salvatage.
 - Responsable de volver el sitio primario a sus niveles operativos normales.
- Equipo de Reanudación de Operaciones.
 - Responsable de volver las operaciones al sitio primario.
 - No siempre es un equipo adicional.

Otros aspectos a considerar

- Relación con grupos externos (emergencias, policia, bomberos, etc).
- Relaciones con empleados.
- Fraude y crímenes.
- Desembolsos financieros.
- Relaciones con los medios de prensa/ tv/ radio.

Importante!!

- Ambos planes, BCP y DRP, deben mantenerse actualizados.
- El personal responsable debe estar preparado para entrar en contingencia.
- Toda la compañía debe conocer y entender los objetivos de los planes.
- Pruebas periódicas de los planes, BCP y DRP, deben realizarse. Estas deberían estar a cargo de entidades independientes a las áreas involucradas: Auditoría Interna o Consultores Externos.

Tecnologías de Seguridad Informática

Seguridad Física

Seguridad Física

- Seguridad Física comprende...
 - ...los elementos involucrados en la selección de un sitio seguro, su diseño y configuración,
 - los métodos para asegurar una instalación contra acceso no autorizado,
 - los métodos para asegurar el equipamiento contra robos dirigidos a ellos y a la información que contienen,
 - las medidas de seguridad y ambientales necesarias para proteger el personal, las instalaciones y los recursos asociados.

Amenazas

- Interrupción en la provisión de servicios informáticos – Disponibilidad.
- Daño físico – Disponibilidad.
- Revelación no autorizada de información – Confidencialidad.
- Pérdida de control del sistema – Integridad.
- Robo (físico) – Confidencialidad, Integridad y Disponibilidad.

Principales causantes de daño físico**

1. Temperatura.
2. Gases.
3. Líquidos.
4. Organismos.
5. proyectiles
6. Movimiento
7. Anomalías de Energía

** Fighting Computer Crime, Donn B. Parker

Controles Administrativos

- Planificación de los Requerimientos de las Instalaciones.
 - Selección de un sitio seguro para la instalación.
 - Diseño de un sitio seguro para la instalación.
- Administración de la Seguridad en Instalaciones.
 - Rastros de Auditoría.
 - Procedimientos de Emergencia.

Controles Administrativos

- Controles de Personal.
 - Revisiones pre-contratación.
 - Seguimiento continuo de empleados.
 - Revisiones post-contratación.

Controles técnicos y físicos

- Requerimientos de Control de la Instalación.
 - Guardias.
 - Perros.
 - Cercas.
 - Iluminación.
 - Cerraduras.
 - CCTV.

Controles técnicos y físicos

- Controles de Acceso a Instalaciones.
 - Tarjetas de Acceso.
 - Tarjetas con foto incorporada.
 - Tarjetas codificadas digitalmente.
 - Lectores de proximidad (wireless).
 - Dispositivos biométricos.

Controles técnicos y físicos

- Detección de Intrusos y Alarmas.
 - Detección de Intrusos Perimetral.
 - Sensores Fotoeléctricos.
 - Switches de contacto secos.
 - Detectores de Movimiento.
 - Patrones de onda.
 - Capacitancia.
 - Detectores de sonido.
 - Sistemas de Alarma.

Controles técnicos y físicos

- Control de Inventario.
 - Control físico de PCs
 - Control de laptops.
- Requerimientos de Almacenamientos de Medios.
 - Acceso físico a los medios.
 - Controles ambientales.
 - Inventario de contenido.
 - Auditorías de uso.
 - Reuso del medio y Remanencia de datos.

Test de Seguridad Física: Paseo por la oficina

- Comprobar que:
 - Información confidencial o sensitiva de la compañía no se encuentra sobre escritorios o en lugares de acceso público (por ej. impresoras).
 - Las estaciones de trabajo se encuentren desconectadas de la red (logged off) y apagadas.
 - Las oficinas se encuentren cerradas con llave.
 - Las puertas de las salidas de emergencia (escaleras) se encuentren cerradas
 - Escritorios y armarios se encuentren cerrados.
 - Diskettes, tapes de datos, CDs se encuentran debidamente guardados.

Servicios de Seguridad Informática

Servicios de Seguridad Informática

- Evaluación de Riesgos y Revisiones de Clasificación de la Información.
- Estudios de Penetración.
- Evaluación de Vulnerabilidades.
- Auditoría de Sistemas.

Evaluación de Riesgos y Revisiones de Clasificación de la Información

- Evaluación de procesos de información críticos para el negocio de la empresa.
- Identificación de la exposición.
- Revisión de la clasificación de los datos en la organización
- Comprobación de la existencia de controles costo-eficientes sobre los riesgos descubiertos.

Estudios de Penetración

- Los Estudios de Penetración proveen al cliente de una radiografía de la seguridad existente en su red y hosts mediante la prueba exhaustiva de intentos de intrusión internos y externos. Utilizando técnicas de “hackers”, se evalúa el nivel de riesgo al que esta expuesta la compañía mediante el análisis detallado de las vulnerabilidades encontradas y el nivel de éxito de los intentos de intrusión ejecutados.
- Los Estudios de Penetración deben ser realizados utilizando metodologías probadas de administración de riesgo y programas de trabajo específicamente diseñados para cada escenario definido.
- Estos servicios resultan en recomendaciones detalladas de tipo técnico, procedural y estratégico que permiten a la compañía aumentar su seguridad, minimizando riesgos.

Estudios de Vulnerabilidad

- Permiten determinar cual es el nivel de riesgo al que la compañía se encuentra sujeta sobre la base de un análisis exhaustivo de las vulnerabilidades existentes en su infraestructura tecnológica.
- Estas evaluaciones deben ser realizadas utilizando metodologías de administración del riesgo y programas de trabajo desarrollados especialmente para estos estudios.
- La utilización de herramientas automatizadas que mejoran la eficiencia del proyecto a la vez que permiten reducir sus costos es altamente recomendada para este tipo de servicios.

Auditoría de Sistemas – Controles Generales

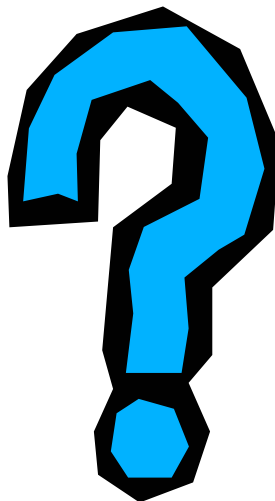
- Evaluaciones exhaustivas de la función de Sistemas de Información en general, las operaciones y los controles asociados.
- Recomendaciones basadas en los resultados para aprovechar oportunidades de mejoras y eficiencia en las operaciones.

Auditoría de Sistemas – Revisión de Aplicaciones

- Revisión pre-implantación.
 - Estas revisiones proporcionan un acercamiento rentable a la evaluación de controles y a la mejora de la seguridad de la aplicación antes de que la misma sea puesta en ejecución en ambiente de producción.

Auditoría de Sistemas – Revisión de Aplicaciones

- Revisión post-implantación.
 - Abarcan tanto sistemas nuevos como sistemas modificados que se encuentran ya en ambiente de producción.
 - Aseguran que los sistemas estén funcionando según lo previsto.
 - Resuelven objetivos de negocio previstos.
 - Verifican que la seguridad y otros controles generales que rodean las aplicaciones sean adecuados.



Muchas Gracias

Donald R. Glass CISSP, CISA, MCSE, MCSE+I, CNE

dglass@emrisk.com

<http://www.emrisk.com>