

Jornada de Seguridad Informática

InfoSec: Los diez dominios de la Seguridad Informática

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

Agradecimientos

- Universidad CAECE.
- Suplemento de Informática de Clarín.
- Enterprise Risk Management.

Agenda

- Preliminares
- Copyrights
- Introducción, Sun Tzu
- Administración de Seguridad Informática
- Tecnologías de Seguridad Informática
- Servicios de Seguridad Informática

Preliminares

Algunos datos que les conviene
conocer

Preliminares

- Nombre: Donald R. Glass, nunca sabrán que representa la “R”, y no se los pienso decir.
- Altura: 206 cms = 6’ 10”.
- Nunca jugué al basquetbol, ni pretendo hacerlo.
- Mi voz es horrible, así que si no entienden avisen.
- Preguntas y comentarios bienvenidos.
- 216 diapositivas, 390 minutos -> 1.8 min/diap
- Disfruten el paseo...

Copyrights

- Esta presentación esta basada en el Common Body of Knowledge, CBK™ desarrollado por (ISC)².
- La marca CBK™ y el framework de InfoSec utilizado en esta presentación fueron utilizados con permiso de (ISC)². Todos los derechos están reservados por (ISC)² Inc.

Introducción

Alguien a quien escuchar... Sun Tzu

Introducción

“Ganar cien victorias en batallas no es la culminación de la pericia. Someter al enemigo sin luchar es la excelencia suprema.”

Sun Tzu, General Chino – 500 AC

Introducción

“Conoce al enemigo y conocete a ti mismo; en cien batallas no serás nunca derrotado.

Cuando seas ignorante acerca del enemigo, pero te conozcas a ti mismo, tus oportunidades de ganar o perder serán iguales.

Si lo ignoras todo acerca de tu enemigo y de ti mismo, tendrás la seguridad de ser derrotado en cada batalla.”

Sun Tzu, General Chino – 500 AC.

Administración de la Seguridad Informática

Administración de la Seguridad Informática

- Conceptos de Administración de Seguridad
- El proceso de Clasificación de Información
- Implantación de Políticas de Seguridad
- Roles y Responsabilidades
- Administración del Riesgo
- El proceso de Concientización en Seguridad Informática (Infosec Awareness)
- Aspectos legales y éticos de la Seguridad Informática

Administración de la Seguridad Informática

Conceptos de Administración de Seguridad

Seguridad Informática - Definición

- Es responsable de la protección de los recursos informáticos de la compañía.

Estos recursos comprenden todos aquellos que:

- Almacenan,
- Procesan, o
- Transmiten

información corporativa.

...en todas sus formas...

Conceptos de Administración de Seguridad

- The BIG three
 - Confidencialidad
 - Integridad
 - Disponibilidad
- Controles de InfoSec
- Otros conceptos
 - Identificación
 - Autenticación
 - Autorización
 - Responsabilidad (accountability)
 - Privacidad
 - Non-repudiation (validación de identidad)

The BIG three

- Confidencialidad

La información debe ser accedida solo por personal autorizado.

Prevenir el acceso no autorizado a información o datos.

The BIG three

- Integridad

Toda modificación a datos o información es realizada por personas autorizadas utilizando procedimientos utilizados.

Los datos/ información deben ser consistentes, tanto en forma interna como externa.

- Interna: la información es consistente con la existente en sub-entidades.
- Externa: la información es consistente con “el mundo real”.

The BIG three

- Disponibilidad

La información y datos se encuentran disponibles cuando se necesitan.

The BIG three

El opuesto a las BIG three es:

- Revelación (disclosure)
- Modificación (alteration)
- Destrucción (detruction)

Otros conceptos

- Identificación

Forma en la cual los usuarios comunican su identidad a un sistema. Identificación es un paso necesario para lograr la autenticación y autorización.

- Autenticación

Es el proceso por el cual se prueba que la información de identificación corresponde con el sujeto que la presenta.

Otros conceptos

- Autorización

Derechos y permisos otorgados a un individuo (o proceso) que le permite acceder a un recurso del sistema/computadora.

El proceso de Autorización se realiza una vez que se ha logrado la Identificación y Autenticación del usuario.

Otros conceptos

- Responsabilidad (accountability)

Habilidad para determinar las acciones individuales de un usuario dentro de un sistema, y para identificar a dicho usuario. Usualmente este principio esta soportado por logs de auditoría.

- Privacidad

Determina el nivel de confidencialidad y protección de privacidad que se le brinda a un usuario dentro de un sistema.

Otros conceptos

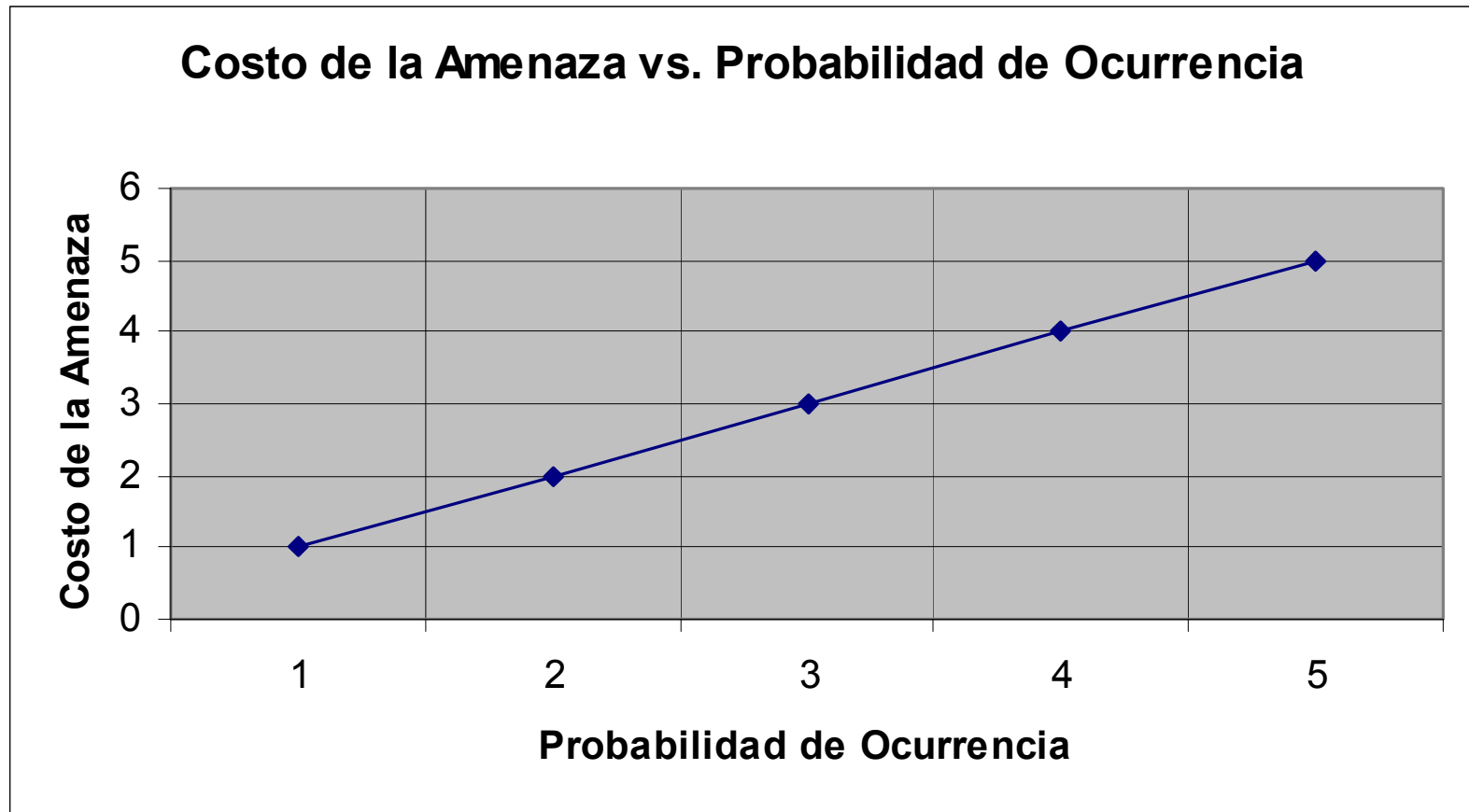
- Non-Repudiation (Validación de identidad)

La utilización de elementos de información única permite validar la autenticidad de una persona (tales como rasgos fisiológicos, certificados de autenticidad, etc.)

Controles de InfoSec

- Reducción de los efectos producidos por las *amenazas de seguridad y vulnerabilidades* a un nivel tolerable por la empresa.
- Estos controles pueden ser:
 - Preventivos
 - Detectivos
 - Correctivos

Controles de Infosec



Administración de la Seguridad Informática

El Proceso de Clasificación de la Información

Clasificación de la Información

Objetivo:

- No todos los datos/ información tienen el mismo valor.
- No todo el mundo puede acceder a toda los datos/ información.
- El costo asociado a la implantación de controles puede ser alto.

Clasificación de la Información

Beneficios:

- Demuestra el compromiso de una organización hacia la seguridad informática.
- Permite identificar que información/ datos son los más importantes para la organización.
- Soporta los conceptos de confidencialidad, integridad y disponibilidad relacionados con los datos/ información.
- Ayuda a identificar que controles corresponden a qué datos/ información.
- Podría ser requerido por aspectos legales, regulatorios u otros.

Clasificación de la Información

- No clasificada
- Sensitiva pero no clasificada
- Confidencial
- Secreta
- Ultra Secreta

Criterio de Clasificación de la Información

- Valor
- Edad
- Vida útil
- Asociación con personas

Clasificación de la Información

Roles

■ Dueño

- Define el nivel de clasificación que le corresponde a la información que le pertenece.
- Revisa los niveles de clasificación periódicamente y realiza los cambios que sean necesarios dentro de la información que administra.
- Delega la responsabilidad de la protección de datos al custodio.

Clasificación de la Información

Roles

- Custodio
 - Ejecuta backups en forma regular de la información que custodia.
 - Ejecuta la restauración de los datos/ información cuando se necesita.
 - Mantiene esos datos/ información respetando la política de clasificación de información.

Clasificación de la Información

Roles

■ Usuario

- Deben seguir los procedimientos operativos definidos en la política de seguridad y aceptar las guías de trabajo definidas.
- Deben hacer lo que este en sus manos para proteger la información clasificada.
- Deben utilizar los recursos asignados solo para fines de negocio.

Administración de la Seguridad Informática

Implantación de Políticas de Seguridad

Implantación de Políticas de Seguridad



Implantación de Políticas de Seguridad

- Declaración de la Alta Gerencia, Política de Seguridad Informática.
 - Reconocimiento de la importancia de los recursos informáticos para el modelo de negocio de la compañía.
 - Declaración de soporte/ apoyo hacia seguridad informática en todas las áreas de la compañía.
 - Compromiso para autorizar y administrar la definición de estándares, procedimientos y normas (guías).

Implantación de Políticas de Seguridad

- Políticas Organizacionales/ Funcionales.
 - Políticas Regulatorias.
 - Políticas Informativas.
 - Políticas Recomendadas.

Implantación de Políticas de Seguridad

- Estándares.

Especifican el uso de una determinada tecnología en forma uniforme.

- Baselines.

Definen parámetros mínimos de configuración en relación a un estándar determinado.

- Normas recomendadas (guidelines).

Guías de recomendaciones mas flexibles que el estándar.

- Procedimientos.

Descripción detallada de tareas a realizar.

Administración de la Seguridad Informática

Roles y Responsabilidades

Roles y Responsabilidades

- Gerencia General

Responsable final por la seguridad informática de la compañía.

- ISSO (Information Systems Security Officer)

Responsable funcional por la seguridad informática de la compañía.

- Dueño

Determina el nivel de clasificación de la información.

Roles y Responsabilidades

- Custodio

Preserva la Confidencialidad, Integridad y Disponibilidad (CID) de la información.

- Usuario/ Operador

Trabaja respetando las políticas, normas y procedimientos definidos.

- Auditor

Evalúa los controles de seguridad informática y presenta recomendaciones a la alta gerencia.

Administración de la Seguridad Informática

Administración del Riesgo

Administración del Riesgo

- Principal objetivo: *mitigar el riesgo*.
- Definición:
 - Identificación.
 - Análisis.
 - Control.
 - Reducción de la pérdida asociada.

Identificación de Riesgos

- Existencia de una amenaza.
- Posibles consecuencias de la concreción de la amenaza.
- Probabilidad de ocurrencia de la amenaza.
- Nivel de confianza en la concreción de la amenaza.

Principios de la Administración del Riesgo

- Realizar un Análisis de Riesgos, incluyendo el análisis de costo-beneficio de los controles implantados y a implantar.
- Implantar, revisar y mantener controles de seguridad informática.

Conceptos de Administración del Riesgo

- Activo.
 - Recurso, producto, proceso, dato, todo aquello que tenga un valor para el negocio de la compañía.
- Amenaza.
 - Presencia de un evento que pueda impactar en forma negativa en la compañía.
- Vulnerabilidad.
 - Ausencia o debilidad de un control.

Conceptos de Administración del Riesgo

■ Activo.

- Recursos
tenidos

■ Amenaza

- Presencia
negativa

■ Vulnerabilidad.

- Ausencia o debilidad de un control.

La combinación de **Activo**,
Amenaza y **Vulnerabilidad**
conforman lo que se conoce
como **Triple** en seguridad
informática.

lo que
ía.

en forma

Conceptos de Administración del Riesgo

- Control (implantado).
 - Su función es reducir el riesgo asociado con una amenaza o grupo de amenazas.
- Factor de Exposición (EF).
 - Porcentaje de pérdida sobre el valor del un activo generado por la concreción de una amenaza en dicho activo. Este valor es necesario para el cálculo del SLE.
 - $0\% \leq EF \leq 100\%$

Conceptos de Administración del Riesgo

- Expectativa de Pérdida Individual (SLE).
 - Valor monetario asociado a un evento determinado. Representa la pérdida producida por una amenaza determinada individual.
 - $SLE = \text{Valor Activo (\$)} * EF$
- Tasa de Ocurrencia Annual (ARO)
 - Representa la frecuencia estimada de ocurrencia de un evento, dentro del período de un año.
 - $0 \leq ARO < \infty$

Conceptos de Administración del Riesgo

- Expectativa de Pérdida Anualizada (ALE).
 - Representa la pérdida annual producida por una amenaza determinada individual.
 - $ALE = SLE * ARO$

Análisis de Riesgos

- Cuantificación del impacto de potenciales amenazas al negocio.
- Resultados:
 - Identificación de riesgos.
 - Justificación económica de controles (costo/ beneficio).

Análisis de Riesgos

- Proceso de Evaluación de Activos.
- Análisis Cuantitativo de Riesgos.
- Análisis Cualitativo de Riesgos.
- Selección de Controles.

Proceso de Evaluación de Activos

- ¿Por qué?
 - Es necesario para realizar el análisis de costo/beneficio.
 - Puede ser necesario para determinar pólizas de seguro.
 - Soporta la selección de controles.
 - “Due Care”

Proceso de Evaluación de Activos

- ¿Cómo?
 - Costo inicial y de mantenimiento del activo (licenciamiento, compra, desarrollo y mantenimiento/ soporte).
 - El valor del activo relacionado con la operación y modelo del negocio.
 - El valor del activo establecido por el mercado, y el valor estimado de la propiedad intelectual.

Análisis de Riesgos

- Análisis Cuantitativo de Riesgos.
 - Asigna valores monetarios hard (objetivos) a cada componente de la evaluación de riesgos y a cada potencial pérdida.
- Análisis Cualitativo de Riesgos.
 - Orientado a aspectos soft de la organización: imagen, market share, etc.
 - Puede ser utilizado en forma genérica.

Análisis de Riesgos

| Propiedad | Cantidad | Calidad |
|-----------------------------|-----------------|----------------|
| Análisis costo/ beneficio | Sí | No |
| Costos Hard (\$) | Sí | No |
| Puede ser Automatizado | Sí | No |
| Suposiciones | Pocas | Muchas |
| Cálculos complejos | Sí | No |
| Información requerida | Mucha | Poca |
| Tiempo/ Trabajo involucrado | Mucho | Poco |
| Facilidad de comunicación | Facíl | Difícil |

Selección de Controles

- Análisis Costo/ Beneficio.
 - Costo Control < Valor del Activo
- Nivel de operación manual requerida.
- Características de Auditabilidad y Contabilidad.
- Habilidad de Recupero.
- Proveedor.

Administración de la Seguridad Informática

El proceso de Concientización en Seguridad Informática
(Infosec Awareness)

Security Awareness

- Comprende la concientización general y colectiva del personal de una organización respecto de la importancia de la seguridad informática y de los controles de seguridad.
- Normalmente uno de las áreas de menor consideración... “la cadena se rompe por el eslabón mas débil”... en Infosec → USUARIO
- No es lo mismo que Entrenamiento.

Security Awareness

Beneficios:

- Importante reducción de la cantidad de acciones no autorizadas generadas por el personal de la organización.
- Incremento significativo de la efectividad de los controles implantados.
- Ayuda a evitar el fraude, desperdicio y abuso de recursos informáticos

Security Awareness

Formas de lograr la concientización.

- Presentaciones en vivo o grabadas: conferencias/ presentaciones, video, entrenamiento basado en computadoras (CBT), etc.
- Publicación/ Distribución: newsletters, boletines e intranet.
- Incentivos: premios y reconocimiento por alcanzar objetivos relacionados con la seguridad informática.
- Recordatorios: banners de login, parafernalia de marketing (tazas, lapiceras, mouse pads, etc.).

Administración de la Seguridad Informática

Aspectos legales y éticos de la Seguridad Informática

Computer Crime

- Crímenes cometidos contra una computadora.
- Crímenes cometidos utilizando una computadora.

Computer Crimes

- Denial of Service (DoS), normal o distribuido.
- Robo de Contraseñas.
- Intrusiones a redes.
- Monitoreo no autorizado de emanaciones electromagnéticas (Emanation Eavesdropping).
- Ingeniería Social.
- Contenido de material ilegal (por ej. pornografía).
- Fraude.
- Piratería de software.
- Destrucción o alteración de información.
- Espionaje.
- Terrorismo.
- Uso de scripts de ataque del Internet.
- Dumpster Diving

Computer Crimes

- DDoS contra Y!, Amazon.com y ZDNet (Feb-2000).
- Love Letter (Love Bug), worm liberado por Onel de Guzman en las Filipinas (May-2000).
- Transmisión inadvertida de información personal de clientes por Kaiser Permanente HMO (Ago-2000).
- Kevin Mitnick (1989~1995).
- Morris worm (1988).
- Penetración de la red corporativa de Microsoft (Oct-2000).

Leyes relacionadas

- Leyes de Propiedad Intelectual.
 - Patentes.
 - Copyright.
 - Trade Secrets.
 - Marcas (trademarks).
- Leyes de Privacidad de la Información.
- Leyes específicas.

Investigación

Desafíos:

- Tiempo de investigación reducido.
- Intagibilidad de la información.
- Posible interferencia de la investigación con las operaciones normales del negocio.
- Dificultad para obtener evidencia.

Investigación

Desafíos:

- Datos localizados en el mismo equipo utilizado durante operaciones normales del negocio (data co-mingling).
- En muchos casos un especialista puede ser necesario.
- Locaciones geográficas/ Diferentes jurisdicciones.

Ciclo de vida de la evidencia

- Descubrimiento y Reconocimiento.
- Protección.
- Registración.
- Recolección.
 - Recolección de todos los medios de almacenamientos relevantes.
 - Generación de una imagen del HD antes de desconectar la computadora.
 - Impresión de pantallas.
 - Evitar la destrucción de los equipos (degaussing).

Ciclo de vida de la evidencia

- Identificación (etiquetado).
- Preservación.
 - Protección de los medios magnéticos contra borrado.
 - Almacenamiento en un ambiente adecuado.
- Transportación.
- Presentación ante la corte.
- Devolución de la evidencia a su dueño.

Admisibilidad de la evidencia

La evidencia debe ser/ estar:

- Relevante: relacionada con el crimen bajo investigación).
- Permitida Legalmente: fue obtenida de manera legal.
- Confiable: no ha sido alterada o modificada.
- Identificada: ha sido claramente etiquetada.
- Preservada: no ha sido dañada o destruida.

Conducción de la Investigación

- Comité de investigación:
 - Compuesto por áreas relevantes: IT, Seguridad Informática, Auditoría, RR.HH., Legales...
 - Responsable del planeamiento y ejecución de la investigación.
 - Responsable del establecimiento y definición de los procedimientos relacionados con la investigación.
 - Responsables de determinar si las autoridades locales/ federales/ nacionales deben ser contactadas.
 - Responsables de la recolección inicial de evidencia.

Etica

- “Disciplina filosófica que tiene por objeto los juicios de valor cuando se aplican a la distinción entre el bien y el mal.”
- Códigos de ética:
 - (ISC)²
www.isc2.org/cgi/content.cgi?category=12
 - The Internet Activities Board (IAB), Ethics and Internet (RFC 1087).
www.faqs.org/rfcs/rfc1087.html
 - ISACA
www.isaca.org/codeofethics.htm

Tecnologías de Seguridad Informática

Tecnologías de Seguridad Informática

- Control de Accesos.
- Seguridad en Redes.
- Criptografía.
- Seguridad Operacional.
- Infosec en el desarrollo de aplicaciones.
- Recuperación ante Contingencias.
- Seguridad Física.

Tecnologías de Seguridad Informática

Control de Accesos

Control de Accesos

- Necesario para la preservación de la CID.
- Tipos de controles de accesos:
 - Controles Administrativos: Esta categoría incluye políticas y procedimientos, security awareness, entrenamiento, background checks, estudios de hábitos de trabajo, supervisión, etc.
 - Controles Lógicos y Técnicos: Implica la restricción del acceso a los sistemas y la protección de la información: encriptación, smart cards, ACLs, etc.
 - Controles Físicos: Esta categoría incluye guardias, seguridad física del edificio en general, separación de funciones, back up, etc.

Modelos de Control de Accesos

- Control de acceso Mandatorio.
 - La autorización del acceso de un *sujeto* a un *objeto* depende de *etiquetas (labels)* las cuales indican el nivel de acceso del sujeto en cuestión y la *clasificación o sensibilidad* del objeto.
 - Típicamente utilizado en sistemas militares.
- Control de acceso Discreto.
 - El sujeto, en forma limitada, tiene la autoridad para especificar que objetos son accesibles.
 - Utilizado en ambientes dinámicos.

Modelos de Control de Accesos

- Control de acceso No-discreto.
 - Una autoridad central determina que sujetos pueden acceder a que objetos tomando como base la política de seguridad de la organización.
 - Los controles de acceso pueden estar basados en:
 - el rol del sujeto dentro de la organización (basado en rol),
 - las responsabilidades y tareas desempeñadas por el sujeto en la organización (basado en tareas).
 - Util para organizaciones con un alto nivel de rotación de personal.

Identificación y Autenticación

- Identificación.
 - Refiere al acto de proveer credenciales que permitan determinar la identidad de un sujeto.
- Autenticación.
 - Refiere a la comprobación de las credenciales recibidas con el objetivo de determinar si el sujeto es quien dice ser.
- Autorización.
 - Refiere a la determinación de los permisos de acceso de un sujeto identificado y autenticado sobre un objeto.

Identificación y Autenticación

- Tipo 1: Algo que conoces.
 - Tipo 2: Algo que tienes.
 - Tipo 3: Algo que eres (físicamente).
-
- Autenticación de dos factores (two-factor) refiere a la utilización de dos tipos de identificadores para la realización de la autenticación.

Algo que conoces

- Caso ideal: *“one-time password”*
- Contraseña estática: aquel que se mantiene durante cada sesión de logon.
- Contraseña dinámica: aquella que cambia cada vez que el usuario se identifica.
- Passphrase: secuencia de caracteres, usualmente de mayor longitud de la permitida para un contraseña. Esta passphrase se utiliza para determinar un contraseña virtual

Algo que tienes

- Tokens.
- Smart Cards.
- Llaves.
- Etc...

Algo que eres

- Sistemas Biométricos.
 - Método automatizado de identificación o autenticación de un sujeto vivo basado en aspectos fisiológicos o de comportamiento.
 - Identificación → uno-a-muchos.
 - Autenticación → uno-a-uno
 - Tipos.
 - Huellas digitales, Retina, Iris, Cara (estructura de la cara del sujeto), geometría de la Mano, Voz.
 - Dinámica de la firma a mano alzada.

Single Sign-On (SSO)

- Disminuir la cantidad de log-on a diferentes sistemas.
- Centralizar la administración de usuarios/ contraseñas.
- Ventajas:
 - Utilización de contraseñas fuertes.
 - Facilidad de administración/
- Desventajas:
 - Punto único de entrada.
- Ejemplo: Kerberos

Tecnologías de Seguridad Informática

Seguridad en Redes

Seguridad en Redes

- Sistemas de Detección de Intrusos.
- Firewalls.
- Redes Privadas Virtuales.
- Remote Access.
- Ataques y Abuso de Red.

Sistemas de Detección de Intrusos

Sistemas de Detección de Intrusos

- Detección y Respuesta a Intrusiones
 - Responsable por el monitoreo de sistemas con el objetivo de obtener evidencia relacionada con una intrusión o con abuso de los recursos informáticos.
 - Implantación y mantenimiento de los Sistemas de Detección de Intrusos (IDS) y los procesos relacionados.
 - Creación del Computer Incident Response Team (CIRT).

Sistemas de Detección de Intrusos

- Computer Incident Response Team (CIRT)
 - Análisis ante la notificación de un evento.
 - Respuesta ante un incidente, si el análisis determina que lo amerita.
 - Definición de los procedimientos de escalamiento de incidentes.
 - Resolución, seguimiento post-incidente, y reporte a las áreas/ individuos pertinentes.

Sistemas de Detección de Intrusos

- Principio:

“El comportamiento de un intruso dentro de un sistema o red difiere de aquel de un usuario autorizado, esta diferencia es cuantificable y se puede medir de tal forma de facilitar la comparación”.

Sistemas de Detección de Intrusos

Clasificación

- Basada en dónde se obtiene los datos:
 - Network-based
 - Host-based
- Basada en cómo detecta intrusiones:
 - Knowledge-based (Signature-based)
 - Behavior-based (Statistical anomaly-based)

Sistemas de Detección de Intrusos

- Network-based
 - Normalmente reside en segmentos de red discretos.
 - Monitorea el tráfico de red en el segmento en donde fue instalado.
 - Usualmente es un appliance de red con un NIC trabajando en modo promiscuo.

Sistemas de Detección de Intrusos

■ Host-based

- Utiliza pequeños programas (agentes), los cuales residen en cada host.
- Monitorea los archivos de log del sistema.
- Solo detecta anomalías dentro de la misma computadora

Sistemas de Detección de Intrusos

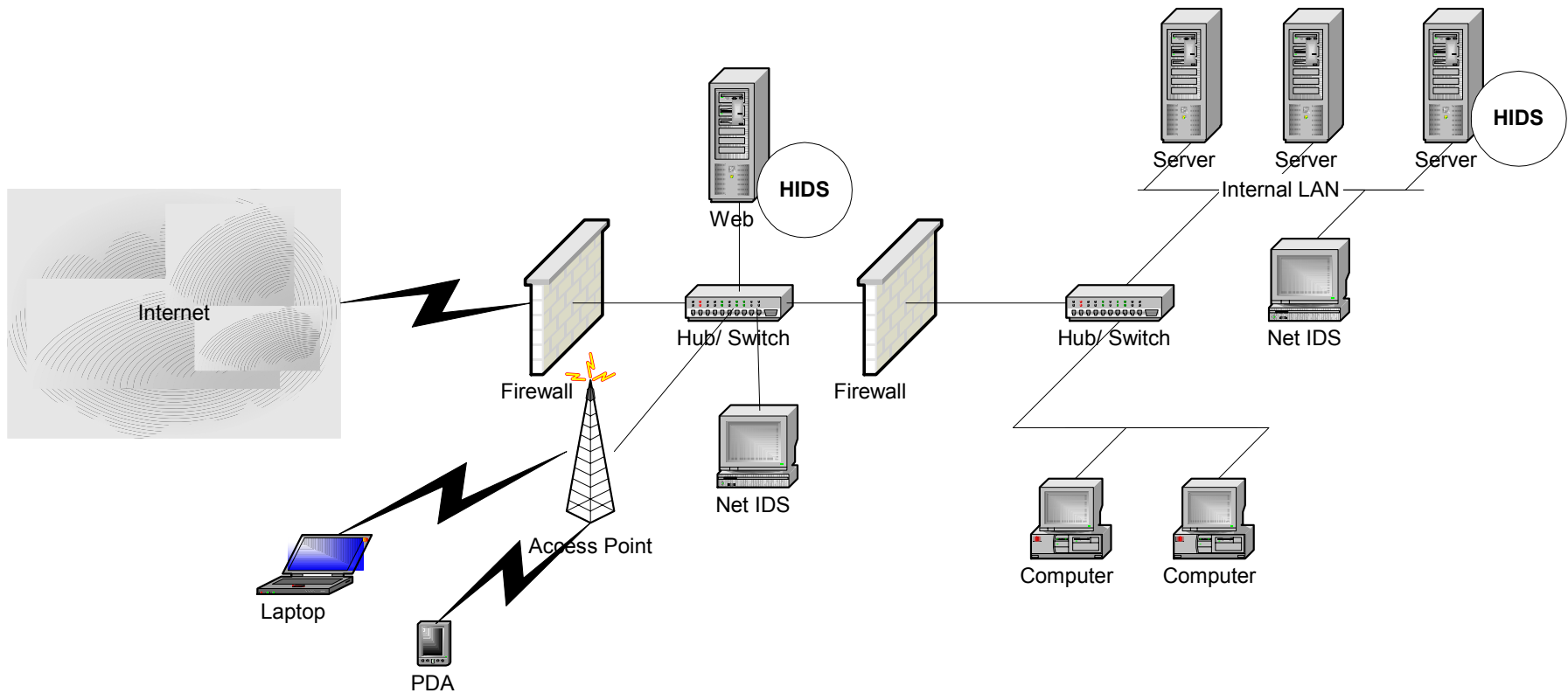
- Knowledge-based
 - Base de datos de intrusiones conocidas (firmas).
 - Ventajas:
 - Baja cantidad de falsos-positivos.
 - Alarmas estandarizadas.
 - Desventajas:
 - Intensivo en cuanto a la utilización de recursos.
 - Ataques nuevos, únicos u originales no siempre son descubiertos.

Sistemas de Detección de Intrusos

■ Behavior-based

- Utiliza un algoritmo de aprendizaje para determinar que se considera una conducta “normal”.
- Ventajas:
 - Se adaptan dinámicamente a nuevos ataques.
 - No dependen de un sistema operativo en particular.
- Desventajas:
 - Alta tasa de falsas alarmas (falsos-positivos).
 - El comportamiento del sistema puede no ser lo suficientemente estático.

Sistemas de Detección de Intrusos



Firewalls

(cortafuegos)

Firewalls

- Principios de Diseño:
 - Todo el tráfico de adentro hacia fuera, y viceversa debe pasar a través del Firewall.
 - Solamente el tráfico autorizado, definido en la Política de Seguridad Local debe poder pasar por el Firewall.
 - El Firewall debe ser inmune a penetraciones.

Firewalls

- Limitaciones:
 - Un Firewall no protege contra ataques que no pasan por el mismo.
Ej: líneas dial-up.
 - Un Firewall no protege contra amenazas internas.
 - Un Firewall no pretege contra ataques de contenido malicioso.

Firewalls - Regla de Oro

- Todo aquello que no fue explícitamente permitido, es prohibido.

Firewalls

Bastion Host:

- Es un sistema identificado como un punto crítico de seguridad.
- Es el equipo que, indefectiblemente, será atacado.

Tipos de Firewalls

- Firewalls de Filtrado de Paquetes (Screening router).
 - Primera generación de Firewalls .
 - Capas 3 (Red) y 4 (Enlace de Datos) del modelo de referencia OSI.
 - Utiliza direcciones de red (IP) y números de puertos.

Tipos de Firewalls

- Firewalls de Capa de Aplicación (Proxy Server).
 - Segunda generación de Firewalls.
 - Capa 7 (Aplicación) del modelo de referencia OSI.
 - Actua como un intermediario (proxy) entre la un host localizado red externa (insegura) y otro dentro de la red interna (segura).
 - Uso intensivo de recursos, degrada la performance de la red.

Tipos de Firewalls

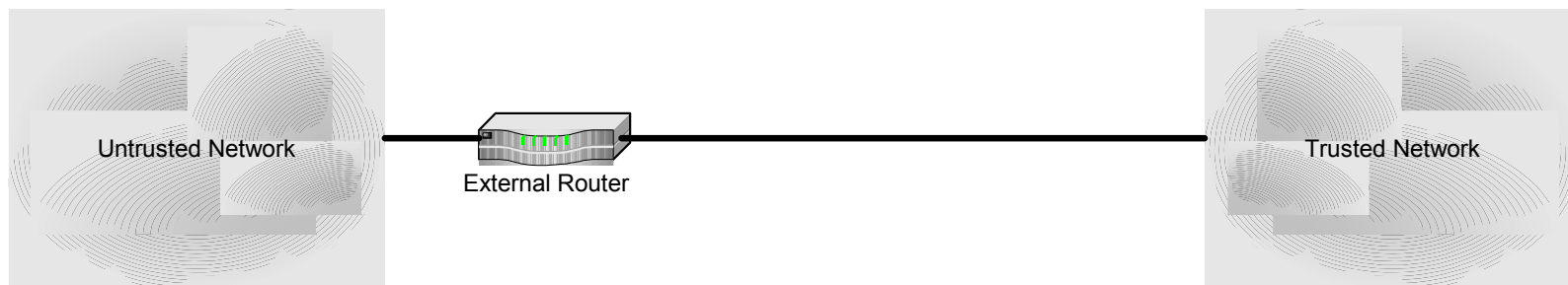
- Firewalls de Inspección de Estados (Stateful Inspection).
 - Tercera generación de Firewalls.
 - Los paquetes de datos son capturados por un motor de inspección que opera en la capa de red..
 - Todas las capas del modelo de referencia OSI.

Tipos de Firewalls

- Firewalls de Filtrado Dinámico de Paquetes.
 - Cuarta generación de Firewalls.
 - Permite la modificación de las reglas de seguridad del firewall como respuesta a determinados eventos.
 - Mayormente utilizado para proveer soporte limitado a UDP. Por un período corto de tiempo el firewall recuerda todos los datagramas UDP que cruzaron el firewall y, así decide si permite o no el paso de nuevos datagramas.

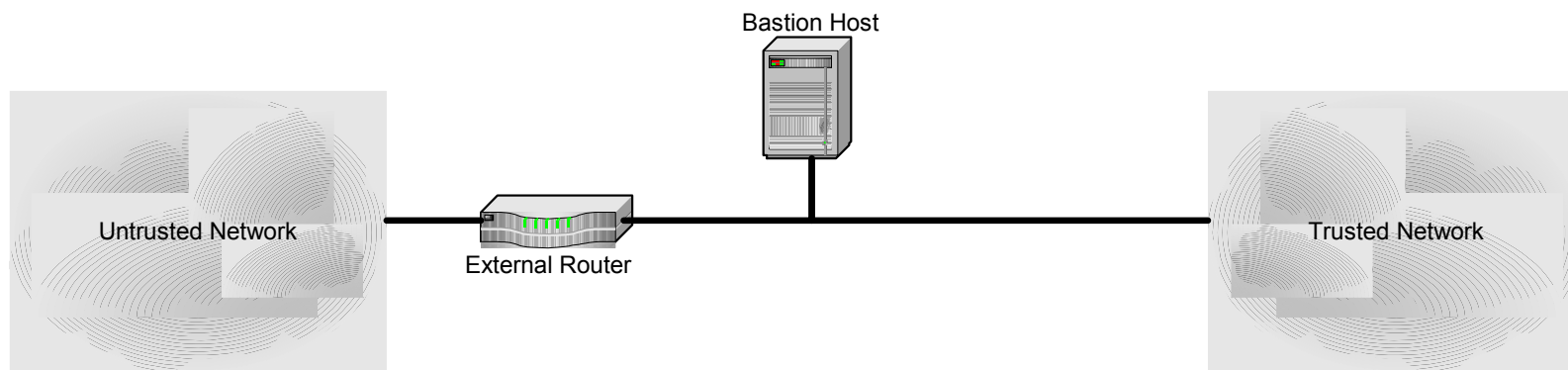
Arquitecturas de Firewalls

- Packet-Filtering Routers



Arquitecturas de Firewalls

- Screened-Host Firewall Systems



Arquitecturas de Firewalls

- Dual-Homed Host Firewall

