
1

## EVOLUCIÓN DE LA CIBERSEGURIDAD

ESCUELA DE COMERCIO
PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

**Figura 1.1—Tríada de ciberseguridad**

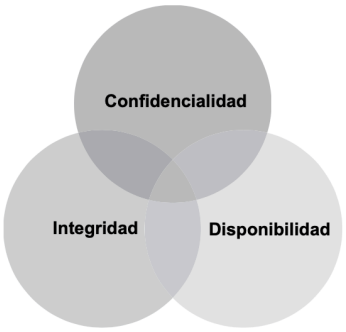
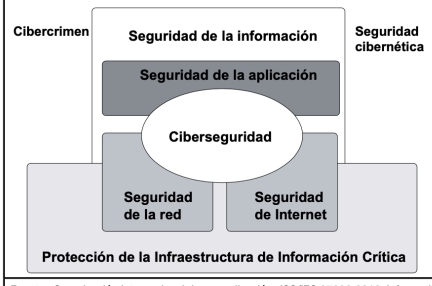



**Figura 1.2—Relación entre la ciberseguridad y otros dominios de la seguridad**




Fuente: Organización internacional de normalización, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Suiza, 2012



2

2

# SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

- La seguridad de la información trata con la información, la ciberseguridad se ocupa de la protección de los activos digitales.
- Protección de activos digitales:
  - Identificar
  - Proteger
  - Detectar
  - Responder
  - Recuperar

3

3

# OBJETIVOS DE LA CIBERSEGURIDAD


La **confidencialidad** es la protección de la información contra el acceso no autorizado o la divulgación

La **integridad** es la protección de la información contra la modificación no autorizada

La **disponibilidad** garantiza el acceso oportuno y confiable al uso de la información y los sistemas

4

4

## RIESGO

- Hay muchas definiciones posibles de riesgo.
- Para los propósitos de este curso, se considerará:
  - Riesgo
  - Amenaza
  - Activos
  - Vulnerabilidad
  - Riesgo inherente
  - Riesgo residual

5

5

## ENFOQUES DE RIESGOS DE CIBERSEGURIDAD

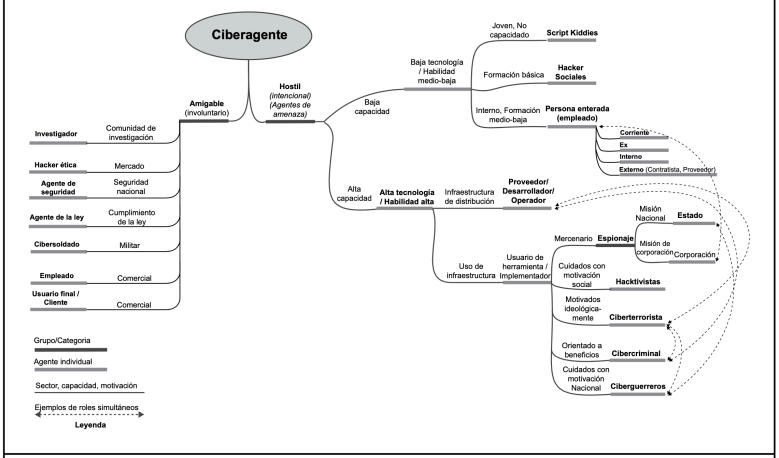
- Ad hoc: un enfoque ad hoc simplemente implementa la seguridad sin una lógica o criterio particular.
- Basado en cumplimientos: también conocido como seguridad basada en estándares, este enfoque depende del cumplimiento de reglamentos o normas para determinar las implementaciones de seguridad.
- Basado en riesgos: la seguridad basada en riesgos depende de la identificación del riesgo único al que una organización en particular se enfrenta.

6

6

# AGENTES DE AMENAZA

**Figura 2.5— Agentes de amenaza de ciberseguridad**



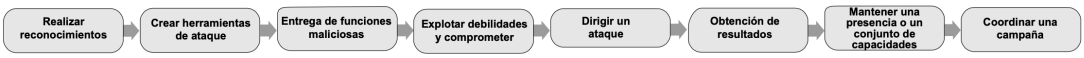

Fuente: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, Enero 2016, Grecia





# PROCESO DE ATAQUE GENERALIZADO

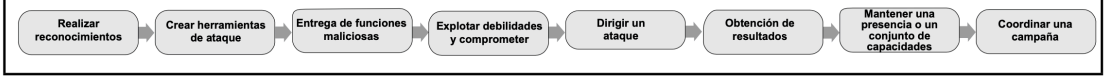
**Figura 2.7—Proceso de amenaza**




- Realizar reconocimientos:
  - Activos
  - Pasivos
- Crear herramientas de ataque:
  - Phishing o ataques selectivos
  - Generar páginas web falsas
  - Crear y operar organizaciones falsas

# PROCESO DE ATAQUE GENERALIZADO

**Figura 2.7—Proceso de amenaza**



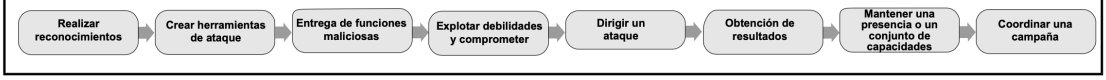

- Entrega de funciones maliciosas:
  - Introducción de malware
  - La colocación de individuos infiltrados
  - La instalación de sniffers
  - Introducción de hardware

9

9

# PROCESO DE ATAQUE GENERALIZADO

**Figura 2.7—Proceso de amenaza**



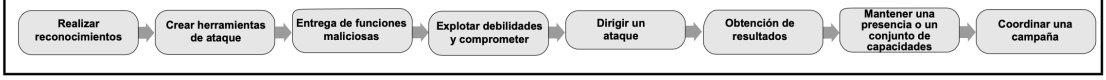

- Explotar debilidades y comprometer:
  - Split tunneling
  - La filtración de datos
  - Explotación de sistemas "multi tenant
  - Lanzando exploits

10

10

# PROCESO DE ATAQUE GENERALIZADO

**Figura 2.7—Proceso de amenaza**



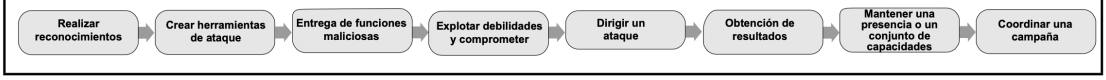

- Dirigir un ataque:
  - Intercepción de comunicaciones
  - Ataques de denegación de servicio
  - Interferencias a distancia
  - Secuestro de sesión

11

11

# PROCESO DE ATAQUE GENERALIZADO

**Figura 2.7—Proceso de amenaza**



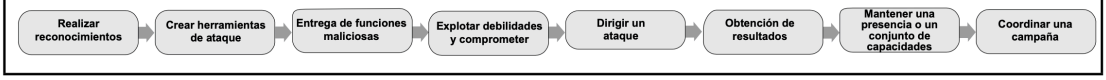

- Obtención de resultados:
  - Obtener acceso no autorizado
  - La degradación de los servicios
  - Crear, corromper o borrar datos críticos
  - Modificar el flujo de control de los sistemas

12

12

# PROCESO DE ATAQUE GENERALIZADO

**Figura 2.7—Proceso de amenaza**




- Mantener una presencia o un conjunto de capacidades:
  - Ofuscando las acciones de adversario
  - Adaptando los ciberataques
- Coordinar una campaña:
  - Ataques de múltiples etapas
  - Ataques internos y externos
  - Ataques generalizados y adaptables

13

13

# MALWARE, RANSOMWARE Y TIPOS DE ATAQUE

- El malware, también conocido como código malicioso, es el software diseñado para obtener acceso a los sistemas informáticos objetivo, robar información o interrumpir las operaciones computacionales.
- Tipos comunes de malware:
  - Virus
  - Gusano de red
  - Troyanos
  - Red de computadoras infectadas con código malicioso (Botnet).

14

14

## MALWARE, RANSOMWARE Y TIPOS DE ATAQUE

- Tipos específicos de malware:
  - Software espía (spyware)
  - Sistemas de publicidad (adware)
  - Software maligno de petición de rescate (Ransomware):
    - GhostCrypt,
    - SNSLocker
  - Software de registro de tecleado (Keylogger)
  - Rootkit

15

15

## OTROS TIPOS DE ATAQUES

- Además del malware y del ransomware, hay muchos otros tipos de ataques:
  - Amenazas persistentes avanzadas (APT)
  - Puerta trasera
  - Ataque de fuerza bruta
  - Desbordamiento de búfer
  - Cross-site scripting (XSS)
  - Ataque de denegación de servicio (DoS)
  - Ataque de "hombre en el medio"
  - Ingeniería social
  - Phishing
  - Spear phishing / Phishing de Ingeniería Social
  - Spoofing
  - Structure Query Language (SQL) injection
  - Exploit de día cero

16

16

## POLÍTICAS

- Existe un gran número de atributos de políticas recomendables que deben de tenerse en consideración:
  - Las políticas de seguridad deben ser una articulación de una estrategia de seguridad de la información bien definida que capta la intención, las expectativas y la dirección de la gestión.
  - Las políticas deben ser claras y de fácil comprensión para todas las partes interesadas.
  - Las políticas deben ser cortas y concisas, escritas en un lenguaje sencillo.

17

17

## POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

- Aspectos a considerar:
  - Continuidad del negocio y Recuperación ante desastres
  - Gestión de activos
  - Reglas de conducta
  - Adquisición / Desarrollo / Mantenimiento
  - Gestión de proveedores
  - Comunicaciones y Operaciones
  - Cumplimiento
  - Gestión de riesgos

18

18

## POLÍTICA DE CONTROL DE ACCESO

- Esto puede ser medido por indicadores tales como, entre otros:
  - Número de violaciones de acceso que excedan la cantidad permitida
  - La cantidad de interrupciones de trabajo debido a derechos de acceso insuficientes
  - Número de incidentes de segregación de funciones o resultados de auditoría.
- La política de control de acceso debe cubrir los siguientes temas:
  - Ciclo de vida de provisión de acceso físico y lógico
  - Menor privilegio/ privilegio basado en la necesidad de conocer
  - Segregación de funciones
  - Acceso de emergencia

19

19

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

- El objetivo de la política de seguridad de la información del personal incluye:
  - Ejecutar verificaciones de antecedentes regulares de todos los empleados y personas en posiciones clave.
  - Adquirir información sobre el personal clave en puestos de seguridad de la información.
  - Desarrollar un plan de sucesión para todos los puestos clave en seguridad de la información.
  - Definir e implementar procedimientos adecuados para la terminación.

20

20

# POLÍTICA DE RESPUESTA A INCIDENTES DE SEGURIDAD

- Esta política se encarga de la necesidad de responder a los incidentes:
  - Una definición de un incidente de seguridad de información
  - Una declaración de cómo los incidentes serán manejados
  - Requisitos para el establecimiento del equipo de respuesta a incidentes, con roles y responsabilidades
  - Requisitos para la creación de un plan de respuesta a incidentes probado, el cual proporcionará los procedimientos y directrices documentadas para:
    - Criticidad de incidentes
    - Procesos de informes y escalado
    - Recuperación (incluyendo): Los objetivos de punto de recuperación (RPO) y los objetivos de tiempo de recuperación (RTO)

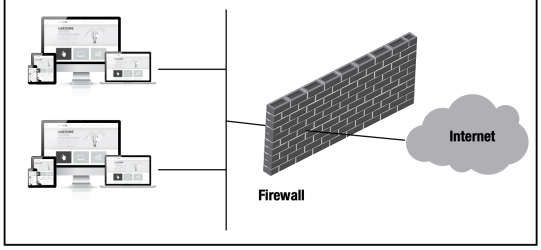
21

21

# FIREWALLS

- Sistema o combinación de sistemas que establece un límite entre dos o más redes, formando típicamente una barrera entre un entorno seguro y un entorno abierto tal como internet.

Figura 3.7—Tráfico enviado a través de un firewall




22

22

# TIPOS DE FIREWALLS

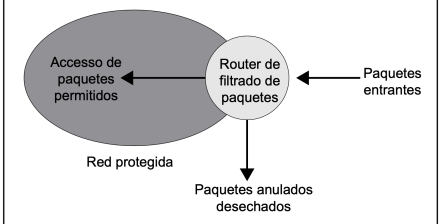
| Figura 3.8—Tipos de Firewall | |
|---|---|
| Primera generación | Un simple router de filtrado de paquetes que examina individualmente los paquetes y aplica reglas basadas en direcciones, protocolos y puertos. |
| Segunda generación | Mantiene registros de todas las conexiones en una tabla de estado. Ésto le permite aplicar reglas basadas en paquetes dentro del contexto de la sesón de comunicaciones. |
| Tercera generación | Opera en la Capa 7 (capa de aplicación) y es capaz de examinar el protocolo usado en las comunicaciones, como el Protocolo de transferencia de hipertexto (HTTP). Estos cortafuegos son mucho más sensibles a actividades sospechosas relativas al contenido del mensaje en sí mismo, no sólo a la información del direccionamiento. |
| Próxima generación | Llamados a veces de Inspección profunda de paquetes (Deep Packet Inspection, DPI), son una versión mejorada de los cortafuegos de tercera generación e incorporan la funcionalidad de Sistema de prevención de intrusiones (IPS) y a menudo son capaces de inspeccionar conexiones SSL (Secure Sockets Layer) o SSH (Secure Shell). |
| Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015 | |

23

23

# FIREWALLS DE FILTRADO DE PAQUETES

**Figura 3.9—Firewall de filtrado de paquetes**




Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

| Figura 3.10—Firewall de filtrado de paquetes | |
|---|---|
| **Ventajas** | **Desventajas** |
| Simplicidad de un “choke point” (cuello de botella) de red | Vulnerable a ataques de filtros no configurados de manera apropiada |
| Minimo impacto en el rendimiento de la red | Vulnerable a ataques de túnel sobre servicios permitidos |
| Poco costoso o gratuito | Todos los sistemas de red privada son vulnerables cuando un router de filtrado de paquete se ve comprometido |

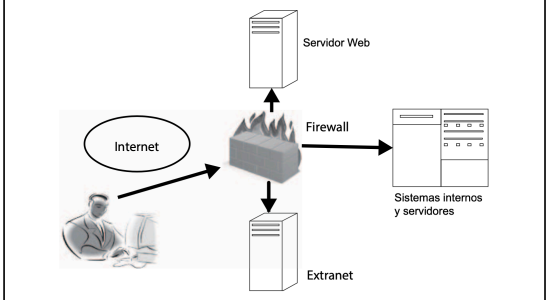
24

24

# IMPLEMENTACIÓN DE FIREWALLS

- Cortafuegos (firewall) de servidor (host) de filtrado (Screened-host Firewall)
- Firewall de base dual (dual-homed firewall)
- Firewall de zona desmilitarizada (DMZ) o firewall de subred proyectada (screened-subnet firewall)

**Figura 3.13—La zona desmilitarizada**




Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

25

25

# ANTIVIRUS Y ANTI-MALWARE

- El anti-malware puede ser controlado a través de diferentes mecanismos, incluyendo:
  - Restricción del tráfico de salida.
  - Políticas y concienciación que preparen a los usuarios a evitar abrir emails sospechosos o archivos adjuntos.
  - Múltiples capas de software anti-malware que usan una combinación de identificación de firmas.

26

26

## SISTEMAS DE DETECCIÓN DE INTRUSIONES

- Las amplias categorías de IDSs incluyen:
  - IDSs basados en la red
  - IDSs basados en host
- Los componentes de un IDS son:
  - Sensores responsables de la recolección de datos.
  - Los analizadores que reciben la información entrante
  - Una consola de administración
- Los tipos de IDS incluyen:
  - Basados en firmas
  - Basados en estadísticas
  - Redes neuronales

27

27

## CIFRADO

- El cifrado es parte de una ciencia más amplia de lenguajes secretos llamada criptografía, la cual es generalmente usada para:
  - Proteger la información almacenada en las computadoras contra la visualización y manipulación no autorizadas
  - Proteger los datos que viajan a través de las redes contra interceptación y manipulación no autorizadas
  - Disuadir y detectar alteraciones accidentales o intencionales de los datos
  - Verificar la autenticidad de una transacción o documento

28

28

# ELEMENTOS CLAVE DE SISTEMAS CRIPTOGRÁFICOS

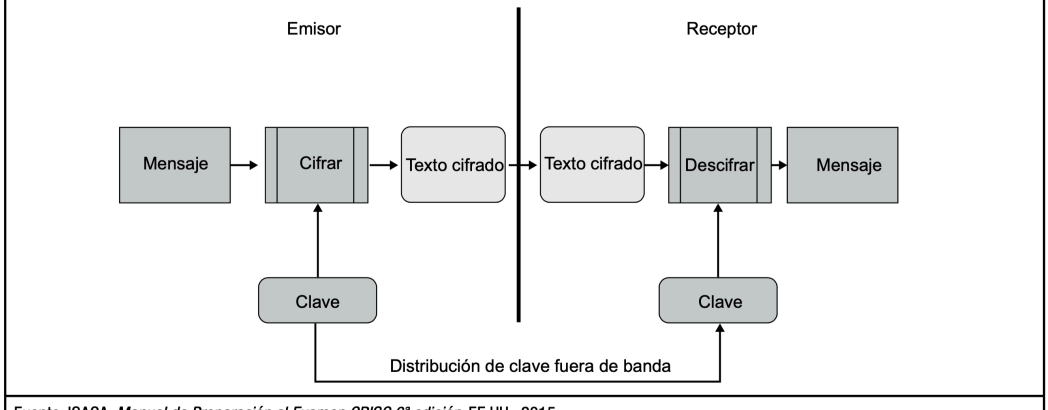
- Los elementos clave de los sistemas criptográficos incluyen:
  - Algoritmo de cifrado
  - Clave de cifrado
  - Longitud de la clave
- Los sistemas criptográficos efectivos dependen de:
  - Fuerza del algoritmo
  - Discreción y dificultad para comprometer una clave
  - No existencia de puertas traseras
  - Incapacidad de descifrar partes de un mensaje de texto codificado
  - Propiedades de un texto plano conocido por un perpetrador

29

29

# CLAVE DE CIFRADO SIMÉTRICA

**Figura 3.15—Criptografía simétrica**



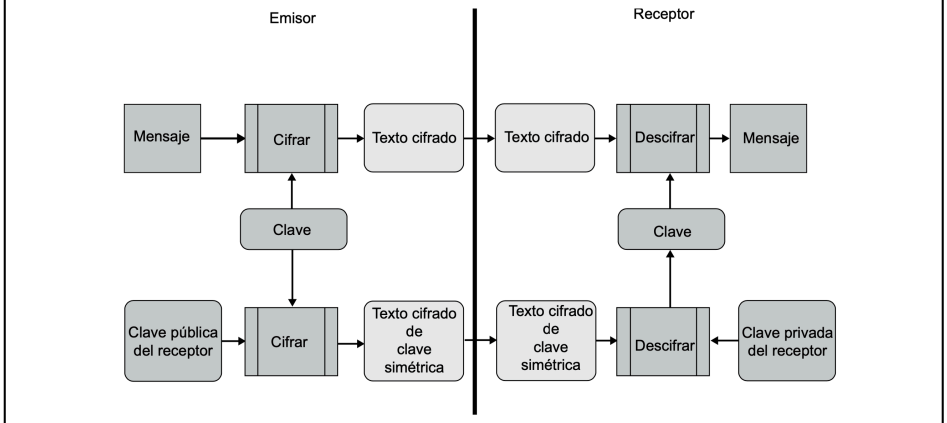

Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

30

30

# CLAVE DE CIFRADO ASIMÉTRICA

**Figura 3.16—Uso de algoritmos asimétricos para respaldar la criptografía simétrica**




Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

31



# FIRMA DIGITAL

- Una firma digital es una identificación electrónica de una persona o entidad creada mediante un algoritmo de clave pública.
- La firma digital es un método criptográfico que asegura:
  - Integridad de los datos
  - Autenticación
  - No repudio

32

## APLICACIONES DE SISTEMAS CRIPTOGRÁFICOS

- Seguridad de la capa de transporte (TLS), las implementaciones actuales:
  - Para criptografía de clave pública.
  - Para cifras simétricas.
  - Para funciones hash de una sola vía.
- Protocolo seguro de transferencia de hipertexto (HTTPS)
- Red privada virtual (VPN)
- IPSec
- Secure Shell SSH
- Extensiones multipropósito seguras de correo de internet (S/MIME)
- Transacción electrónica segura (SET).

33

33

## INFRAESTRUCTURA DE CLAVE PÚBLICA

- Elementos clave de la infraestructura son los siguientes:
  - Certificados digitales
  - Autoridad de certificación (CA)
  - Autoridad de registro

34

34

## RIESGOS Y PROBLEMAS DE REDES LAN

- El riesgo asociado con el uso de redes de área local incluye:
  - La pérdida de integridad de datos
  - La falta de protección de los datos
  - La exposición a actividades externas
  - Infección por virus y gusanos
  - Revelación indebida de datos causado por disposiciones de acceso general
  - La violación de las licencias de software
  - El acceso ilegal simulado
  - Escucha de información
  - La suplantación del usuario
  - Destrucción de los datos de registro y de auditoría

35

35

## TECNOLOGÍA INALÁMBRICA

- Las redes inalámbricas sirven como mecanismo de transporte entre dispositivos, y entre dispositivos y las redes alámbricas tradicionales.
- Las redes inalámbricas son muchas y diversas, pero frecuentemente son categorizadas en cuatro grupos basados en su rango de cobertura:
  - WANs
  - LANs
  - Redes inalámbricas de área personal (WPANs)
  - Redes inalámbricas ad hoc

36

36

## PROTECCIÓN EN REDES INALÁMBRICAS

- Los principales riesgos asociados:
  - El email puede ser interceptado y leído o modificado.
  - Hackers pueden reemplazar las credenciales de un usuario con información falsa.
  - Una persona no autorizada puede acceder a una red inalámbrica no segura y usar sus recursos.

37

37

## PUERTOS Y PROTOCOLOS

- Un puerto es una conexión lógica.
- La designación de un puerto es la forma en que un programa cliente especifica a un determinado programa servidor cuál es el equipo.
- Numeros de protocolo y servicios de misiones:
  - Los puertos reconocidos
  - Los puertos registrados
  - Los puertos dinámicos y/o privados
- Considerar aspectos de tunelización

38

38

## REDES PRIVADAS VIRTUALES (VPN)

- Al diseñar una VPN, es importante asegurar que la VPN puede transportar todos los tipos de datos de manera segura y privada a través de cualquier tipo de conexión.
- Los tipos comunes de tunelización incluyen:
  - Protocolo de túnel punto a punto (PPTP)
  - Protocolo de túnel de capa 2 (L2TP)
  - VPN Capa de sockets seguros
  - VPN IPSec

39

39

## VOZ SOBRE PROTOCOLO DE INTERNET (VOIP)

- Los usuarios a menudo esperan que todas las comunicaciones de voz sean confidenciales.
- Cualquier dispositivo VoIP es un dispositivo IP; por tanto, es vulnerable a los mismos tipos de ataques que cualquier otro dispositivo IP.
- Un hacker o virus podrían potencialmente dejar indisponibles las redes de datos y de voz de forma simultánea en un sólo ataque.
- Las redes VoIP poseen una serie de características que necesitan de requisitos de seguridad especiales.

40

40

## ACCESO REMOTO

- El acceso remoto basado en TCP/IP Internet es un método rentable que permite que las organizaciones aprovechen las infraestructuras de red pública y las opciones de conectividad disponibles.
- Las organizaciones deberían ser conscientes de que usar VPN para permitir el acceso remoto a sus sistemas puede crear agujeros en su infraestructura de seguridad.
- El tráfico cifrado puede esconder acciones no autorizadas o software malicioso que puede ser transmitido a través de dichos canales.

41

41

## SEGURIDAD DE LOS DATOS

- La información usada por una organización puede tener un valor e importancia variables.
- La clasificación de datos funciona mediante el etiquetado de los datos con los metadatos basados en una taxonomía de clasificación.
- La información del negocio pertenece en última instancia al responsable de los procesos del negocio.

42

42

## SEGURIDAD DE LOS DATOS

- Al clasificar los datos, se deben considerar los siguientes requisitos:
  - Acceso y autenticación
  - Confidencialidad
  - Privacidad
  - Disponibilidad
  - Propiedad y distribución
  - Integridad
  - Retención de datos
  - Auditabilidad.

43

43

## SEGURIDAD DE BASE DE DATOS

- Las bases de datos son vulnerables a riesgos, incluyendo:
  - Actividades no autorizadas por parte de usuarios autorizados
  - Infección o interacción con malware
  - Problemas de espacio
  - Daño físico
  - Fallos de diseño
  - Corrupción de datos
- La seguridad de bases de datos se alcanza mediante una serie de medidas.

44

44

## INVESTIGACIONES

- Se incluye la recopilación y análisis de las evidencias con el objetivo de identificar al autor de un ataque o del uso o acceso no autorizado.
- La evidencia de un delito informático existe en forma de archivos de logs, marcas de tiempo de archivos, contenido de la memoria, etc.
- La cadena de evidencia contiene esencialmente información respecto a:
  - Las personas que han tenido acceso
  - Los procedimientos que se siguieron para trabajar con la evidencia
  - Garantías de que el análisis se basa en copias que son idénticas a la evidencia original.

45

45

## ANÁLISIS FORENSE

- La informática forense incluye actividades que involucran la exploración y aplicación de métodos para recolectar, procesar, interpretar y usar evidencias digitales que ayuden a sustanciar si ha ocurrido un incidente.
- Hay 4 consideraciones principales en la cadena de eventos en lo que respecta a las pruebas de análisis forense digital:
  - Identificar
  - Preservar
  - Analizar
  - Presentar

46

46

## ELEMENTOS DEL ANÁLISIS FORENSE

- Protección de datos
- Adquisición de datos
- Generación de imágenes
- Extracción
- Entrevistas
- Normalización

47

47

## ELEMENTOS DEL ANÁLISIS FORENSE

- Presentación de informes:
  - Describir con precisión los detalles de un incidente.
  - Ser comprensible para los encargados de tomar decisiones.
  - Ser capaz de resistir al escrutinio legal.
  - Ser inequívoco y no estar abierto a una interpretación errónea.
  - Ser fácilmente referenciado.
  - Contener toda la información necesaria para explicar las conclusiones alcanzadas.
  - Ofrecer conclusiones, opiniones o recomendaciones válidas cuando sea necesario.
  - Ser creado en el momento oportuno.

48

48

## ELEMENTOS DEL ANÁLISIS FORENSE

- Análisis de tráfico de red.
- Análisis de archivos de registro:
  - Herramientas de reducción de auditoría
  - Herramientas de detección de tendencia/varianza
  - Herramientas de detección de firma de ataques
- Herramientas de análisis forense digital:
  - Ordenador
  - Memoria
  - Dispositivo móvil
  - Red

49

49

## ELEMENTOS DEL ANÁLISIS FORENSE

- Cronogramas
- Anti análisis forense:
  - Borrar de forma segura los datos
  - Sobrescribir metadatos
  - Prevenir la creación de datos
  - Cifrado de los datos
  - Cifrado de los protocolos de red
  - Ocultar datos en el espacio de inactividad o en otros lugares no asignados
  - Ocultar datos o archivos dentro de otro archivo (esteganografía)

50

50

# TECNOLOGÍA MÓVIL: RIESGOS, AMENAZAS Y VULNERABILIDADES

- Aplicaciones móviles:

Figura 6.5—OWASP: Las diez principales vulnerabilidades de seguridad móvil en 2016

| | | | |
|---|---|---|---|
| M1–Uso inadecuado de la plataforma | M2–Almacenamiento inseguro de datos | M3–Comunicación insegura | M4–Autenticación insegura |
| M5–Criptografía insuficiente | M6–Autorización insegura | M7–Calidad del código del cliente | M8–Manipulación del código |
| | M9–Ingeniería inversa | M10–Funcionalidad extraña | |

51

51

# TECNOLOGÍA MÓVIL: RIESGOS, AMENAZAS Y VULNERABILIDADES

- Riesgo físico:
  - Localización del dispositivo basado en el seguimiento de la antena (celda) a la que se conecta.
  - Capacidad remota de eliminación de los datos y apagado
  - Capacidad de bloqueo remoto de la tarjeta SIM
- Riesgo organizacional.
- Riesgo técnico:
  - Monitorización de actividades y Recuperación de datos

52

52

# TECNOLOGÍA MÓVIL: RIESGOS, AMENAZAS Y VULNERABILIDADES

ESCUELA DE COMERCIO PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

- Conectividad de red no autorizada

| Figura 6.7—Riesgo de conectividad no autorizada[80] | |
|---|---|
| **Vector** | **Riesgo** |
| Email | Transmisión de datos cuya complejidad varía entre baja a alta (incluyendo archivos de gran tamaño) |
| SMS | Transmisión de datos simples, instalaciones de comando y control limitadas (comando de servicio) |
| HTTP get/post | Vector de ataque genérico para la conectividad, comando y control basado en el navegador |
| Socket TCP/UDP | Vector de ataque de bajo nivel para la transmisión de datos sencillos a complejos |
| Exfiltración DNS | Vector de ataque de bajo nivel para la transmisión de datos cuya complejidad varía entre baja a alta, cuyas posibilidades de detección son lentas pero difíciles |
| Bluetooth | Transmisión de datos cuya complejidad varía entre baja a alta, instalación de comando y control basado en el perfil, vector de ataque genérico para las proximidades |
| WLAN/WiMAX | Vector de ataque genérico para comando y control completo del objetivo, equivalente a la red cableada |

53

53

# TECNOLOGÍA MÓVIL: RIESGOS, AMENAZAS Y VULNERABILIDADES

ESCUELA DE COMERCIO PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

- Suplantación de la visita web.
- Fuga de datos confidenciales:
  - Identidad
  - Credenciales
  - Archivos de localización
- Almacenamiento no seguro de datos confidenciales.
- Transmisión no segura de datos confidenciales.
- Dirigido por vulnerabilidades.

54

54

## NUBE Y COLABORACIÓN DIGITAL

- Riesgos de computación en la nube:
  - Pérdida de gobierno
  - Bloqueo
  - Fallos en el aislamiento
  - Cumplimiento
  - Compromiso de la interfaz de gestión
  - Protección de datos
  - Eliminación incompleta o insegura de datos
  - Infiltrado malicioso

55

55

## NUBE Y COLABORACIÓN DIGITAL

- Riesgos de aplicación en la nube.
- Beneficios de la computación en la nube:
  - Impulso de mercado
  - Escalabilidad
  - Rentabilidad
  - Actualización oportuna y eficaz
  - Auditoría y evidencia

56

56

## MEDIOS SOCIALES

- Las empresas usan las redes sociales para aumentar el reconocimiento de la marca, las ventas, los ingresos y la satisfacción del cliente.
- El riesgo asociado a una presencia en las redes sociales corporativas incluye:
  - Introducción de virus/software malintencionado (malware) a la red de organización
  - Información errónea o engañosa publicada a través de una presencia fraudulenta.
  - Derechos de contenido poco claros.
  - Insatisfacción del cliente
  - Mala administración de las comunicaciones electrónicas.

57

57

## MEDIOS SOCIALES

- Riesgos asociados al uso de medios sociales por parte del empleado incluyen:
  - Uso de cuentas personales
  - Difusión de imágenes o información por parte de los empleados
  - Uso excesivo de redes sociales por parte de los empleados
  - Acceso a las redes sociales por parte de los empleados a través de dispositivos móviles proporcionados por la empresa.

58

58

ESCUELA DE COMERCIO

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

MÓDULO 5

# FUNDAMENTOS DE CIBERSEGURIDAD

**Prof. Mg. Rafael Mellado S.**
rafael.mellado@pucv.cl
COM3162 – Sistemas de Información 2
Escuela de Comercio

59

59