RESUMEN DE LOS PPT DE SEGURIDAD INFORMÁTICA

Seguridad de la informacion: medidas preventivas, de deteccion y correccion para proteger la integridad, confidencialidad y disponibilidad de los recursos informaticos.

Seguridad **física**, **lógica** y **administrativa**

Es un aspecto de negocios. Incluye evaluaciones internas y externas.

La **fuga de información** puede ser por **personas** (secretos, cosas que saben) o **sistemas** (datos que hay en ellos)

RRHH

Revision de informacion publica y verificar CV.

- criterios: todo el personal evaluado, controles exhaustivos, niveles estandar.

- beneficios: verificar info, obtener idea del nivel de integridad, prevenir ingreso de no calificados o inmorales.

- acuerdos: confidencialidad, uso de recursos, aceptacion de politicas, auditabilidad, no competencia, **Control de actividades**: rotacion de funciones, vacaciones obligatorias (permite deteccion de fraude), segregacion de funciones (control dual, conocimiento distribuido)

- procedimientos de desvinculacion: manejo de la salida del empleado, borrado de cuentas, reenvio de mail y telefono, cambios en cerraduras, modificacion de contraseñas

Confidencialidad

Informacion accedida solamente por los autorizados. Es la identificación, autenticacion y autorizacion.

- amenazas: ingenieria social, hackers, usuarios descuidados, descargas, trashing

- proteccion: clasificacion de la informacion, control de acceso informatico, encripcion de datos, capacitacion de personal, procedimientos de acceso a la informacion

Integridad

Informacion modificada solo por los autorizados

- amenazas: ingenieria social, actividad de usuarios no autorizados, virus, troyanos, falsas alertas, sitios peligrosos

- proteccion: menor privilegio, segregacion de funciones, procedimientos de control de cambios, verficacion de integridad, antivirus, firewall

Disponibilidad

Es asegurar informacion accesible en tiempo y forma

- amenazas: denegacion de servicios, desastres naturales, acciones humanas, gusanos

- proteccion: seguridad fisica, mecanismos de tolerancia a fallos, plan de contingencia, procedimientos operativos

Responsable de seguridad (ROL): Cumplir con el programa integral de seguridad para garantizar lo anterior, gestionar recursos necesarios para cumplir, determinar prioridades, comunicarse con la alta direccion.

La seguridad de la informacion es de la alta gerencia, NO DE SISTEMAS

Politicas, normas y procedimientos

Politicas (nivel **estratégico**)

Son **breves** y generales, aceptadas por todo el personal. Alineadas con normativas legales y corporativas y deben serlo con la estrategia de negocio.

Deben ser: realizadas y aprobadas por el comité de seguridad de la informacion (compuesto por todas las areas sustantivas), comunicadas a todos los integrantes de la org, escritas en lenguaje claro independiente de la tecnologia, roles definidos para la implementacion.

Contenido: objetivos, alcance, importancia de la SI, proposito de los responsables a nivel gerencial, explicacion de politicas, principios, normas y requisitos, definicion de responsabilidades para la gestion de la SI.

Normativas: definen metas y objetivos, roles, responsabilidades, autoridad, establecen criterios y uniformes de conducta, informan obligaciones y medidas por incumplimiento, informan a terceros definiciones de la org, garantizan el cumplimiento de normas externas.

Estándares, normas y guidelines (nivel **táctico**)

Conjunto de reglas aplicadas a las actividades del manejo de informacio, para protegerla, los recursos y la reputacion de la entidad.

IMPLANTACION

Estándares: especifican el uso uniforme de una tecnologia, define actividades, acciones, reglas, regulaciones.

Normas: recomendaciones, colaboran al cumplimiento de objetivos.

Baselines: definen parametros para un estandar.

Procedimientos (nivel **operativo**)

Conjunto de reglas definidas en el nivel operativo para cumplir las politicas y normas definidas por la organización. Descripción detallada de tareas.

Aspectos legales (si no lo cumple, negligencia)

- **Due diligence**: responsabilidad de entender amenazas y riesgos

- **Due care:** implementar contramedidas para protegerse.

Controles

Reducir los efectos producidos por las amenazas y vulnerabilidades a nivel tolerable por la empresa (datos y activos de la organización)

- **físicos**: guardias, cerraduras, camaras, proteccion, ambientales

- **técnicos**: control de acceso logico, encripcion, identificacion, autenticacion, monitoreo logico

- **administrativos**: politicas, estandares, procedimientos, concientizacion, control de cambios, autorizacion.

CLASIFICACION DE LA INFORMACION

Clasificacion y controles de activos: mantener proteccion de los mismos, se designa un propietario para cada uno, se debe realizar un inventario (protege).

Fundamentos: define niveles de CID (publico, uso interno, confidencial)

Motivos: cuanto invertir en la proteccion, no todos los datos valen igual, no todas las personas deben acceder, aspectos legales y regulatorios. Criterios: valor, vida util, asociacion con personas.

Resultados: info → activo de negocio, gerentes de area → dueños de la informacion, IT → custodio de la informacion, se identifican datos importantes, permite definir controles y costos, asignar roles, compromiso con la seguridad.

Proceso: identificar admin, especificar criterio, clasificacion, especificar excepciones, especificar procesos de desclasificacion y transferencia, programas de concientizacion.

Roles: dueño, custodio, usuario, auditor.

Funciones: gerente, comité, responsible, analista, admin, auditor (de seg)

Areas en la SI

Análisis Forense y Auditoría, Criptografía, Seguridad en el Desarrollo de Aplicaciones, Desarrollo del Programa de Seguridad, Gestión de Riesgo, Gestión del Programa de Seguridad de la Información, Gobierno de Seguridad de la Información, Marco Legal, Modelos y Arquitecturas de Seguridad, Continuidad del negocio y Plan de recupero de desastre, Seguridad en las Operaciones, Seguridad en Redes, Internet y Telecomunicaciones, Seguridad Física, Sistemas y Metodologías de Control de Acceso

Objetivos: gestionar SI, enfocarse en tareas y conocimiento que debe tener el gerente de SI

GESTIÓN DE CAMBIOS

Contar con control sobre modificaciones en operaciones. Algunos cambios pueden corromper un modelo de seguridad. El responsable debe analizar el impacto del cambio antes, modificaciones autorizadas, sin bajar el nivel de seguridad.

GESTIÓN DE LOGS

Registros secuenciales de eventos, compresion, verificar integridad, backup.

GESTIÓN DE ACTIVIDADES

Segregacion de funciones (nadie aprueba su propio trabajo → evita fraude), rotacion de tareas (mas control, reemplazo de funciones), vacaciones obligatorias.

GESTIÓN DE INCIDENTES → identificar desvios en politicas o fallas en controles

Incidente de seguridad (no deseado). Los incidetes ocurren siempre, no hay seguridad 100%.

CSIRT: equipo de respuesta. Puede ser interno o externo, recibe eventos, se encarga de la respuesta, resolucion, seguimieto y reporte.

CONCIENTIZACIÓN

Refuerza el eslabon debil (usuario), no es lo mismo que entrenamiento. Reduce incidentes, mediante coferencias, presentaciones, newsletters, incentivos, recordatorios. Hay que separar a la audiencia:

- management: breve, activos críticos, impacto financiero y legal, definir conceptos(PEP), responsabilidades.

- empleados: claro, derechos y obligaciones, actividades aceptables

- personal tecnico: lenguaje tecnico, estandares, procedimientos, guidelines, manejo de incidentes, funciones, resposabilidades, implicancias en tareas habituales.

Hay que revisar los resultados con monitoreo, observacion, encuestas.

GESTIÓN DE LA SEGURIDAD

Objetivo: proteger activos de información. Debe estar alineada con el negocio, relacionada con el gobierno de la seguridad. Es un proceso cíclico

Normas para la GSI:

- IRAM/ISO/IEC 17799: estandar para la GSI publicado por la organización de la estandarizacio y la comision electrotecnica internacional.

- ISO/IEC 27001: para establecer y mejorar un sistema de GSI (SGSI), consistente con la anterior. Es certificable. Involucra:

introduccion: la adopcion debe ser decision estratégica, con apoyo de la alta gerencia. Es un marco referencial, requerimientos legales, comerciales, alineada a la gestion de riesgos.

enfoque: entender requerimientos, establecer politicas y objetivos, implementar y operar controles, manejar riesgos, monitorear desempeño, mejoramiento continuo, todo de la SI

alcance: abarca todos los tipos de org

referencias normativas: ISO/IEC 17799

establecimiento de SGSI: definir alcance y limites, y la politica. Definir la valuacion de riesgos, idenntificarlos (activos, amenazas, vulnerabilidades, impacto (CID)), evaluar opciones de tratamiento: controles, mitigar, aceptarlos objetivamente, eliminar el elemento que lo introduce, transferirlos.

Seleccionar objetivos de control y los controles, obtener aprobacion de la gerencia (por los riesgos residuales), tambien para implementar el SGSI, preparar enunciado de palicabilidad respecto del tratamiento.

- Monitorear y revisar el sgsi: detectar errores, incidentes, violaciones de seguridad, revisar delegacion de tareas, realizar revisiones teniendo en cuenta auditoria e incidentes, evaluar riesgos a intervalos, revisiones gerenciales periodicas, actualizarp lanes de seguridad, registrar eventos y accioens con impacto en el SGI.

- Mantener y mejorar: implementar mejoras, tomar acciones correctivas y preventivas, verificar objetivos cumplidos.

- Documentarlo: politica, alcance, procedimientos, metodologia de evaluacion de riesgos, plan de tratamiento, planeacion y control, aplicabilidad.

- Responsabilidad de la gerencia, auditorias internas: a intervalos planeados para ver si se cumple el estandar y los requerimientos de seguridad, si se implementan de forma efectiva y conforme.

- Mejoramiento de SGSI: correctivo (evitar recurrencia) y preventivo (evitar concurrencia).

La alta gerencia no entiende la necesidad de seguridad, cree que inteferirá con el negocio, no detecta riesgos, cree que la seguridad es costosa.

Depende de la gerencia de sistemas, auditoria, area de SI, de la gerencia de seguridad, consultoria y rrhh.

Responsable:

1) comité de seguridad

2) funcionales: CISO, ISSO.

3) debe conocer el negocio y los procesos.

UNIDAD 2: CONTROL DE ACCESO

El acceso es la transferencia de informacion de un objeto (archivos, docs, impresoras) a un sujeto (usuario, programa, pc). Es otorgar acceso a un sistema o recurso a controlar. Se implementa para asegurar CID.

Pueden ser administrativos, lógicos, físicos

Preventivos, detectivos, etc.

Privacidad: Seguimiento de una persona, anonimidad, profiling (recopilacion de datos), recomendación (privacidad y monitoreo, nivel)

Fases del control de accesos o conceptos : Identificacion, autenticacion y autorizacion

1) Identificacion: diferenciar sujetos. Ej, nombre de usuario, pid. Como comunican su identidad.

2) Autenticacion

Es asegurar que el sujeto es quien dice.

Factores:

a) basada en secretos (conocer): contraseñas.

b) basada en posesion de elementos (tener): tarjeta, token

c) basada en biometricos (ser): huella, voz

d) fuerte: 2 factores diferentes de forma conjunta. Se mitigan por el otro factor las debilidades.

e) basada en hashes: el sujeto informa credenciales (id, pass), el autenticador calcula el hash y compara el que tiene almacenado. El atacante obtendria los hashes. No es necesario almacenar la pass.

a) Basada en secretos

Amenazas: fuerza bruta, analisis de trafico de red, spoofing (autenticacion en objeto falsos), intentar acceder a mecanismos de autenticacion, ej etc/shadow o SAM Database de Windows, bases de datos.

Contramedidas: cuidado con las contraseñas, bloquear cuenta tras intentos, implementar retraso, captchas, cambio periodico, no uso de credenciales anteriores.

b) TOKENS, son generadores de contraseñas que lleva un sujeto.

- estáticos: factor adicional, pass o biometrico. Almacenan clave criptografica. Son usados como tecnica de identificacion en vez de autenticacion, en general. Ej: USB, tarjeta inteligente.

- sincrónicos basados en tiempo: tarjetas y servidor con relojes (tiempo desde la inicializaion), cada cierto tiempo el numero se encripta y se muestra en pantalla, el usuario ingresa su pin con este numero. Ambos tiempos deben coincidir.

- sincrónicos basados en eventos: pass generadas con un evento (sujeto que presione tecla, etc), esto

causa que la tarjeta y servidor avancen al proximo valor de autenticacion. El usuario ingresa su pin en la tarjeta. Luego con esto se geera una nueva pass, enviada al servidor para su verificacion, antes aplicando una funcion criptografica.

- **asincrónicos desafío-respuesta**: genera una cadena de digitos aleatoria y la envia a cliente remoto que intenta acceder a la red. El usuario la ingresa, tambien su pin con la funcion criptografica con una llave almacenada, generando la cotraseña (respuesta) ese resultado se envia al token que hace lo mismo, si el resultado es igual, se autentica.

Amenazas: robo, clonado, ataques a tarjeta de cordenadas con phishing.

Contramedidas: capacitacion, denuncia del token, autenticacion fuerte.

Pueden haber **tarjetas de banda magnética**: baja seguridad, de **proximidad**: mayor alcance de lectura, tiene protocolo, **tarjetas chip con procesamiento** (guardan info confidencial, claves, algoritmos de cifrado) o **sin procesamiento** (se usanpara almacenar datos).

RFID

c) Biométricos:

- retina: con radiacion infrarroja

- iris (iriscode)

- geometria de la mano

- huella dactilar

- firma: **offline** (se parte de firmas **previas**), **online** (requiere **dispositivos digitalizadores,** se dispone de informacion temporal – duracion, posicion, velocidad -, es mejor)

Eleccion de estos: aceptacion del usuario, tiempo de registracion (muestra inicial), tiempo de ingreso, precision, facilidad de implementare, tamaño y manejo de muestras.

Amenazas:

- dispositivos muy sensibles, **error I:** tasa de falsos rechazos

- dispositivos poco sesibles, **error II:** falsas aceptaciones (GRAVE)

la sensibilidad es la interseccion, se llama CER (**crossover error rate**)

Tambien hay tiempo de evaluacion, tasa de procesamiento, exactitud.

3) Autorizacion: definir si tiene acceso a objetos. Ej: listas de control de acceso, control de acceso mandatorio.

4) Trazabilidad: determinar acciones de un usuario dentro de un sistema (logs de auditoria)

5) Privacidad: confidencialidad dentro del sistema

6) No repudio: el sujeto no puede negar que realizo cierta accion. Ej, de origen: no puede negar que envio el mensaje

Clasificación de accesos por centralización:

Gestión de identidades: ingreso a sistemas con única clave, cenntralizar administracion de usuarios y contraseñas, utilizar puerto 389 o 636 (seguro)

- Ventajas: sincronizacion y utilizacion de pass fuertes, ABM de usuarios automatizada, workflows de

aprobacion, disminucion de costos de administracion.

- Desventajas: punto único de entrada, tiempo de desarrollo para sincronizar las aplicaciones.

Acceso simple (SSO): logueo unico para diferentes sistemas, centralización.

- Ventajas: utilizacion de pass fuertes, facilidad de adm.

- Desventajas: punto unico de entrada, dificil de implantar y operar, con la pc desbloqueada se puede acceder a cualquier sistema.

Modelos de control de acceso

- Discrecional (DAC): cada objeto tiene un dueño, se decide qué sujetos acceden a sus recursos, se implementa con listas de control de acceso.

- Mandatorio (MAC): el OS impone sus reglas, uso de labels que posee todo output. Sólo los admin pueden modificar el nivel de sensitividad del objeto.

- Basado en roles (RBAC): asignacion indirecta de permisos, se basa en descripcion de puesto que ocupa en vez de la identidad del sujeto, facilita la segregacion de funciones. Los roles tienen nombres. Es un tipo de MAC.

- Control de acceso no discreto: util cuando hay mucha rotacion de personal. La autoridad determina a que acceden. Puede estar basado e tareas o roles.

Técnicas de control de acceso:

- Dependiente del contenido: decisiones de acceso se basan en la sensibilidad del dato y su contenido, los cambios e él pueden provocar cambios en las decisiones de acceso, las reglas de acceso son constates. Ej: firewall (app), filtros antispam, antivirus.

- Dependiente del contexto: el sistema toma la decision basada en el estado de una cantidad de variables que forma el contexto. Ej: control de acceso de red (NAC), firewall (red).

- Matriz de relaciones

- RBAC: acceso restringido a reglas, no cuenta la identidad.

Rainbow tables: tablas de hashes precalculados, se usa en cracking local. Compara los hashes de estas contra los que se quieren averiguar.

Hay que implementar seguridad fisica, tiempos de exipracion, politicas que prohiban algunas contraseñas, autenticacion fuerte (2 factores).

Logs: comprende proteccion, compresion, ciclos de rotacion, logs remotos, registros fisicos, contramedidas. Graba en medio de ingreso secuencial.

UNIDAD 3: SEGURIDAD FÍSICA

amenazas: desastres naturales, sistema de suministros, humanas, motivos políticos.

Reglas

Prioridad → vida humana

selección de lugar seguro en diseño y configuracion, asegurar contra acceso no autorizado, equipamiento contra robos, proteger personal e instalaciones, ambiente, defensa de áreas por capas, poner sensores activos (laser, ultrasoido) o pasivos (deteccion de peso, etc)

Controles de acceso: volumen de paso de gente, sistemas de control (tarjetas de acceso, biometricos)

Seguridad ambiental: proteccion electrica, agua, evacuacion, incendios

Seguridad perimetral: iluminacion, rejas, es la primer linea de defensa. Lugar lejano a edificaciones, arboles, arbustos.

Seleccion de ubicación: visibilidad, alrededores, accesibilidad, naturaleza. Ver piso techo y paredes (combustibilidad, altura, permeabilidad), puertas y mantrap (puede tener auntenticacion), ventanas (luz, radiacion, etc)

Seguridad del centro de cómputos: iluminacion, control de acceso fisico, proteccion de incendios, computadorasy servers, comunicaciones y telefonicos, HVAC (heating, vent, air cond)

Energía eléctrica en el centro de cómputos: generadores, problemas de tensión

Agua en el centro de cómputos: que cae, tuberias, valvulas

Dispositivos de vigilancia: camaras, movimiento, monitoreo, grabacion o no, medios de transimision.

Datacenter: acceso a equipamiento, camaras, aire acond, control de acceso local, distribucion.

Backups: inventario, auditoria, cajas ignifugas

Resumen de seguridad física:

• El objetivo fundamental de la seguridad física es proteger la vida humana

• La seguridad física protege desde el perímetro al interior de una empresa

• El datacenter requiere especiales medidas de protección

• La seguridad ambiental incluye iluminación, agua, aire y gas

• Se debe contar con alimentación eléctrica redundante

• Se debe tener en cuenta la detección y supresión de incendios

• Un rápido paseo por una oficina permite estimar el nivel de riesgo

GESTION DE RIESGOS

Se llama IRM, brinda administracion consistente con la id y evaluacion de riesgos y valuacion de activos. Es un proceso continuo.

Requiere dimensionar el proyecto, establecer políticas y armar un equipo de IRM, definir metodologias.

Política

Parte de la politica de gestion de riesgos, alineada con la de SI y con la estrategia de la organización. Definicion del equipo de gestión del riesgo.

Contempla objetivos, definicion de niveles aceptables de riesgo, procesos de análisis y tratamiento de riesgos, metoologias, definicion de roles, indicadores de monitoreo.

Equipo

Garantiza que la organización esta protegida ante los riesgos, con el costo beneficio de los controles.

Conformado por el personal de las áreas representativas.

Propone la politica, redacta procedimientos, analiza y trata riesgos, define metricas, cocientiza y capacita personal, documenta, integra al control de cambios.

Fases del proceso

- **Análisis de riesgos:** analizar ambiente y relacion entre atributos riesgosos. El análisis debe identificar vulnerabilidades (ausencia de control) y amenazas (evento que puede impactar de forma negativa).

- **Evaluación de riesgos**: Asignación de valores a los activos (todo lo de valor para el negocio), frecuencia de ameazas, consecuencias. El repore final puede tener una evaluacion de riesgo o medida.

La **exposicion** es el estado en el que se esta expuesto a pérdidas. El **riesgo** es la pérdida. La **salvaguarda** una medida para reducirlo.

Valor de info = costo de adquisicion + valor del dueño + lo que otro puede pagar.

Etapas de administración del riesgo

- identificación y evaluacion de activos

- análisis de amenazas a los activos

- análisis de vulnerabilidades que puedan concretar amenazas

- evaluación del riesgo y la info recopilada

Los riesgos pueden ser naturales o atropogénicos (humanas, itencionales o no)

Alternativas sobre el riesgo

- **reducción**: salvaguardas, no puede ser cero

- **transferencia**: pago de póliza

- **aceptacion**

- **elminar el elemento** que lo introduce

Cálculos

Riesgo total = amenaza * vulnerabilidades * valor del recurso (se asume si no se implementan contramedidas)

Control gap = RT – RR (reducido)

Riesgo Residual = RT – CG (una vez implementadas el remanente)

Consideraciones de las contramedidas

- costos de adquisicion, diseño, implementación, mantenimiento

- impacto en entorno y compatibilidad

- pryebas

- reparacion, actualizacion

- operación manual

- efectos sobre productividad

- habilidad de recuperacion

Evaluación del riesgo

Determinar impacto de amenazas al negocio. Obtenemos id de riesgos y justificacion de controles

económica (C/B). Hay dos métodos:

Método cuantitativo:

Requiere un plan de procesos muy detallado. Se aplica a activos, amenazas y su riesgo, potenciales perdidas, frecuencia de ocurrencia, controles, prediccion de pérdidas de dinero.

La PSE es una herramienta, se lleva a cabo antes del mismo, ayuda a recopilar elementos para la evaluación.

Ventajas: métricas, cuantificación de los parámetros de la CIA, provee C/B, permite realizar seguimiento, expresado en **lenguaje gerencial**

Desventajas: complejo, necesita mucha info, no está basado en nigún estandar de conocimientos.

Indicadores

- **Exposure Factor**: porcentaje de pérdida sobre el valor de un activo por la concreción de una amenaza.

- **Single Loss Exposure**: perdida por determinada amenaza individual. Valor del activo * EF

- **Annualized Rate Ocurrence:** frecuencia analizada de ocurrencia

- **Annualized Loss Expectancy:** perdida anual por una amenaza. ALE = SLE * ARO

Salvaguardas: desarrollar analisis C/B.

ALE (pre control) – ALE (post control) = valor anualizado del control

Total Cost of Ownership: costos de todos los activos. Ej: licencia, compra, instalacion.

Interrupción producción

Método cualitativo:

- orientado a valores intangibles. Amenazas según juicio, intuición y experiencia. Ej: Delphi, brainstorming, story boards.

Conviene crear listas de amenazas con frecuencia, niveles de exposición, determinar la más representativa, chequear casos con los usuarios, el equipo de analisis de riesgo debe recomendar salvaguardas, elevar informes a gerencia.

Ventajas: sencillo, no hay que saber valor ni frecuencia exacta o impacto en la información ni los costos de recomendaciones de mitigación. Da indicaciones generales de áreas de riesgo significativo.

Desventajas: es subjetivo, el valor hallado puede ser incorrecto, no hay análisis de C/B o mitigación del riesgo ni forma de rastrear avance del plan. No puedo usar herramientas automatizadas.

Pasos:

- **definición** (niveles de probabilidad de ocurrencia, de impacto, de riesgo)

- **clasificación** de **amenazas** por probabilidad e impacto

- **estimar riesgo**

- estimar **incertidumbre** del proceso

Herramientas automatizadas

Permiten recolectar info, establecer criterios de valoracion, generar graficos, centralizar informacion, facilitar control, simular escenarios, facilitar mejora continua.

Segregación de funciones

Es un control interno básico. Busca que ninguna persona tenga autoridad de ejecutar mas de dos transacciones sensibles que afecten el estado financiero, que ninguna tenga demasiado acceso a un sistema sin controles. Necesita una guía adecuada. Un enfoque basado en riesgos puede hacer que sea manejable para cualquier compañía. Metodología

- Definiciones: entender alcance de transacciones sensibles y los conflictos que existen en los procesos de negocios clave. Presentan mayor riesgo de fraude si hay acceso excesivo. Se determinan umbrales con base en el riesgo e impacto por cada conflicto de segregación. Resulta en una matriz de conflictos indepedente de la aplicación.

- Análisis y pruebas: se utilizan los datos obtenidos para analizar los usuarios con conflictos. Se reconocen los procesamiento de punta a punta, se deben realizar clasificaciones del riesgo. Los resultados pueden ser por usuario o por funcion y muestran gravedad de problemas de los mismos.

- Plan de acción: analiza cada conflicto y busca controles. Al usar mitigación, se debe analizar uno por uno para documentar los ocontroles clave específicos.

- Corrección: el objetivo es la corrección permanente. Remediación: rediseñar y depurar roles, implementar herramientas de segregación para el mantenimiento. Se divide en depuración táctica de los permisos de usuarios (menos tiempo), y en el rediseño de roles (implica muchos cambios)

SEGURIDAD EN REDES DE INFORMACIÓN O DE DATOS

Segun ubicación:

- LAN: espacio geografico limitado, transimision alta, org dueña del medio fisico, utiliza su espacio para ubicar dispositivos. Tasa de errores baja.

- WAN: espacio extenso, velocidades bajas respecto a lan, org alquila el medio, usan satelites, fibras, etc

- MAN: espacio extenso y limitado, velocidad alta respecto a wan, org dueña, interconecta edificios con fibra óptica

Segun uso:

- Internet

- Intranet

- Extranet

Modelo OSI: aplicación, presentacion, comunicación entre host, direcciones, transimision binaria

Modelo TCP/IP: guias de diseño, conectividad extremo a extremo, especifica si los datos deben ir formateados, direccionados, etc. Tiene varias capas.

Internet Protocol (IP): no orientado a conexión, maneja la fragmentacion. Contiene datos del paquete. El direccionamiento IP tiene, de red (parte del camino usado), direccion de host (dispositivo

específico), usa máscara para definir cuántos bits corresponde a cual. No garantiza la llegada.

Transmission Control Protocol (TCP): orientado a conexión, controla los paquetes enviados, retransmite, ordena, maneja varias conexiones entre dos equipos (puertos). Contiene los datos de puerto origen, destino, secuencia, longitud de header, ventana.v Usa control de flujo.

User Datagram Protocol (UCP): No hay controles, pueden llegar los paquetes en cualquier orden.

Address Resolution Protocol (ARP): cada pc y dispositivo de red tiene IP y MAC. Se guarda la relacion. Algunos atacantes pueden modificar la tabla (poisoning).

Reverse ARP: cuando se tiene una MAC y quiero conocer la IP.

Dynamic Host Configuration Protocol (DHCP): la pc puede recibir su ip de forma estatica (config de adaptador de red) o dinámica (el servidor DHCP asigna la IP correcta en el inicio). Facilita la administracion.

Los ataques pueden ser DHCP falsos, pero como contramedida tenemos snooping → asegura que los servidores DHCP asignen IP solo a los sistemas seleccionados (con la direccion MAC). El proxy intercepta los mensajes antes de enviarlos, debe estar entre la red insegura y segura.

Peligros en internet: escenario multiple de informacion, complejidad legal, necesidad de conexión, falta de controles.

Perímetro interno (recursos sensibles a un ataque) y externo (estan los menos sensibles, accessbles desde la red externa por motivos funcionales): para delimitarlo → firewalls, que aislen las redes externas e internas. Ahí se implementan las reglas de acceso.

Diseño: todo el tráfico debe pasarp or ellos, y sólo el autorizado debe poder atravesarlo (definido en la política de seguridad local). Todo lo no explicitamente permitido es prohibido.

Limitaciones: no protege contra ataques que no pasan por el, ej: dial-up, amenazas interas, ataques de contenido malicioso.

Configuracion:

- política restrictiva: lo no permitido, se prohibe.

- política permisiva: lo no prohibido, se permite.

Filtrado

- Packet filters: en capa 3 (IP), aplicable a routers, filtra IP y puerto.

- Circuit Level Gateways: en capa 4 (TCP), filtran sesiones, no individuales. Info viene del gateway.

- Application Level Gateways: en capa 7, se usan como proxy, entienden comandos de los protocolos.

- Stateful multilayer: Filtran en todas, son mas costosos, gran capacidad de análisis y filtrado.

- Packet dynamic filters: maneja los cambios sin reconstruir el firewall

Arquitecturas: controlan acceso desde una red externa considerada insegura

- Gateway de doble conexión (Dual-homed): debe deshabilitarse el routeo IP, los host de red interna e internet se comunican por el gateway, donde se hace el análisis.

- Host protegido (Screened host): brinda servicios a las estaciones a traves de un sistema en la red interna (Bastion), donde se implementan proxies para las apps autorizadas. Se completa agregando filtrados al firewall o router que conecta con la red exterior (de borde)

- Subred protegida (Screened subnet): es la más utilizada, agrega un nivel de seguridad situando una subred entre las redes externa e interna.

Firewalls personales: ideal para dial-up y banda ancha, crea reglas, uso simple, alta proteccion.

Network Address Translation (NAT): permite acceso a internet desde red privada con direccionamiento privado, reduce direcciones publicas, controla el trafico. Puede ser estatico dinamico u overlapping.

Port Address Translation (PAT): el dispositivo que lo realiza escribe por cada conexión el IP de origenn no routeable, el TCP/IP donde se origino la conexión, y con el cual se reemplazo el numero de puerto de origen.

Identificacion de firewalls:

- **Port scanning**: de puertos abiertos y filtrados

- **Firewalking:** relevamiento de ACL, requiere un agente en la red interna

- **Banner Grabbing:** lectura de los de los servicios que corren en un equipo.

Atravieso de firewalls:

- tunelizar datos por puertos habilitados

- abrir la conexión desde el interior de la red (Es mas probable)

Sistemas de Deteccion de Intrusos (IDS): responsable del monitoreo de sistemas para obtener evidencia relacionada con una intrusion o abuso de recursos. Se implanta y mantiene el IDS y los procesos relacionados, se crea el CSIRT.

Indicadores generales: modificacion de sw y configs, bajo rendimiento inusual, cuelgues, ausencia de logs, de archivos determinados, etc.

Clasificación

- basada en donde obtiene los datos:

Network-Based (NIDS): reside en segmentos de red discretos, monitorea el trafico de red en ese segmento, appliance de red con un NIC en modo promiscuo. De intrusos en la red.

Host-Based (HIDS): Es de intrusos en el equipo, utiliza agentes que residen en cada host, monitorea los log, detecta anomalías solo dentro de esa pc. Verificacion de integridad: puede utilizarse en los hids porque detectan cambios, automarizan la verificacion y dan opciones de dteccion de alteraciones. Para individuales, md5, sha1

- basada en cómo detecta intrusiones:

Knowledge Based (signature): base de datos de intrusiones conocidas, baja la cantidad de falsos positivos y tiene alarmas estandarizadas. Es intensivo con la utilizacion de recursos y no siempre descubre ataques originales.

Behavior Based: utiliza algoritmo de aprendizaje para determinar conductas normales (es dinámico), no depende de un OS. Alta tasa de falsos positivos porque el comportamiento puede no ser muy estatico.

Protocol Anomaly Based: deteccion de mal uso de TCP/IP, se basa en RFC o en el uso tradicional de los headers.

Si el IDS detecta un ataque bloquea la ip, genera logs, etc.

Herramientas de evasion: sidestep, admutate, etc.

Honeypots: simula realidad, disuade, puede tener distintos niveles de interaccion.

- diseño: definir tipo, qué releva, acuerdo con ISP, responsible, herramientas de análisis.

Ventajas: recolecta pocos datos de mucha utilidad, no hay falsos positivos, minimos recursos, atacantes internos y externos.

Desventajas: fuentes potenciales de riesgo, si no son atacados no tienen utilidad

Deben integrarse con el sistema, pueden estar alrededor del firewall o en la DMZ.

DMZ: zona desmilitarizada, es donde se establece el perimetro.

Conexiones remotas a escritorio

- VNC: cliente/servidor, basado en envio de pixels, no es seguro por defecto

- SSH: sistema linux, openssh

- Terminal Server: microsoft, RDP, puede usar TLS.

- Citrix: cliente/servidor

VPN: extension de red local a traves de una red publica, utiliza protocolos de comunicación, encriptacion, encapsulamiento. Puede generarse en capa 2 o 3. Funciona en modo transporte (protege dato del paquete IP), o tunel (paquetes IP completos). Es de bajo costo, accesible yescalable, pero sobrecarga al cliente y depende de medios no fiables.

Estándar IPSec – Internet Protocol Security (de seguridad para capa 3): Es adaptable a Ipv4 y v6. Añade cifrado y autenticacion.

Componentes: arq, protocolos, mecanismos de cifrado y aut.

Protocolos:

- Autentication Header (AH): autenticacion e integridad, pero no confidencialidad.

- Encapsulating Security Payload (ESP): confidencialidad

- ISAKMP: intercambio de claves para cifrado y autenticacion de AH y ESP. Incluye Internet Key Exchange, utiliza Diffie-Hellman.

En modo transporte protege el dato del paquete IP, en túnel el paquete completo.

Domain Name Service (DNS): resuelve nombres a las direcciones IP. Puede haber Spoof definiendo

otro servidor DNS. Se puede usar DNSSec.

Protocol Seguro (https): cifrado

WLAN: soporta buena transferencia de datos (velocidad), movilidad, cambios en oficinas sin gastos extra. Tiene access point (AP)

LAN: autenticacion (solo los autoriados), encriptacion, seguridad de la administracion (solo los autoricados pueden configurar AP), usa un SSID distinto al default.

WEP: claves, basado en RC4, codifica comunicación entre cliente y AP.

WPA: generada en forma dinamica para cada usuario. Usa TKIP.

Ataques de red:

- acceso no autorizado a servicios restringidos (interno)

- uso no autorizado de la red con fines no relacionados con la organización

- monitoreo (intercepcion no autorizada del trafico de red)

- denegacion de servicio e interrupciones

- intrusiones de red (ataque externo)

Tecnologías de trasmisión

- CSMA: cada equipo monitorea en forma continua, cuando el medio esta libre ocmieza la transimision. Si no es verificada, se asume colisión y se retransmite.

- CSMA/CD: opera como el anterior, y si detecta nueva señal mientras transmite envia bloqueo y notifica a todos de la colision, espera un tiempo y despues retransmite.

- Polling: primaria (consulta a secundaria si tiene datos), si tiene le permite transmitir, si es autorizada. Se usa en mainframe.

- Token-Passing: solo si recibe token puede trasmitir, cada estacion lo mantiene un tiempo. No hay colisiones, es bueno para redes de uso intensivo. Se puede calcular ttiempo hasta la proxima., se usa en token ring.

Un dispositivo lan sirve para interconectar redes, y extender la red local, aislar problemas.

Dominio de colision: los nodos estan en el mismo dominio de colision cuando acceden al medio

Dominio de mensaje: estan en el mismo dominio de broadcast si uno envia un mensaje y el resto lo recibe

VLAN: independientes dentro de una red fisica, proveen seguridad.

XDSL: provee transmision de datos de alta velocidad.

Conmutacion de circuitos: trafico constante, demora fija, orientado a conexión, sensible a la perdida de conexión, orientado a voz.

Conmutacion de paquetes: por rafagas, variable, desconectado, a perdida de datos, orientado a datos.

Frame Relay: WAN de alta performance, no tiene correccion de errores.

ATM: ancho de banda muy grande, baja demora, requiere medio fisico de alta velocidad, se usa en redes backbne

VoIP: combina diferetes tipos de datos, permite integrar redes de voz y datos, costo beneficio bueno.

Direccionamiento de red

- Host: nombre de pagina
- Direccion de internet (IP)
- Direccion de hardware (MAC)

CRIPTOGRAFIA

Para garantizar confidencialidad, integridad y autenticidad, que la lea solo el autorizado.

Seguridad incondicional (teorica): sistema seguro frente a atacante con recursos iilimitados. La computacional es con limitados. La seguridad probable, no se puede demostrar su integridad pero el sistema no fue violado.

Criptografia clasica (Secreto del algoritmo)

- transposicion: dispersion de shannon (permitar caracteres sin modificarlos)
- sustitucion: se sustituyen por otros caracteres, puede la distribucion estar en el criptograma.

Cifrados

- monoalfabetico: u alfabeto desplazado y transformado. Se usan tablas de frecuencia, se aprovecha la redundancia.
- polialfabético: hay una periodicidad. Metodo de kasiski: buscar cadenas de caracteres repetidos, el mcd es el periodo. Indice de coincidencia: si los textos cifrados correspoden con suustituciones simples.
- por homófonos: palabras de igual sonido, asignar mas a los mas frecuentes
- poligrámico: playfair (analisis de diagramas reconstruyendo matriz), hill (ataques no por fuerza bruta pero si con texto plano conocido)

Informacion: depende de la ingenieria, empresa, etc.

Entropia: medida de incertidumbre acerca de una variable aleatoria y el numero de bits de informacion.

Un codificador optimo usa el menor numero posible de bits.

El secreto criptografico perfecto si el texto cifrado no da info del mensaje.

Distancia de unicidad: bloque de texto cifrado minimo para intentar éxito en busqueda dde la clave. Criptograma mas largo (+ info) es mas facil de atacar

Criptosistemas modernos

Segun tratamiento del mensaje:

Cifrado en flujo: telefonia movil, internet, wlan

El espacio de las claves es igual o mayor que el de los mensajes. Las claves deben ser equiprobables, la secuencia de clave se usa una sola vez y luego se destruye. El algoritmo se aplica a un elemento de informacion mediante un flujo de clave aleatoria y de mayor longitud que el mensaje. Se hace bit a bit.

La secuencia de bits debe enviarse en un canal inseguro. Si fuese infinita desbordaria la capacidad del canal. Si fuese seguro se mandaria el mensaje directamente.

La técnica usa vectores de inicializacion (aleatoreidad). Usa XOR conn período alto.

Ventajas: alta velocidad, resistente a errores (cifrado independiente del elemento)

Desventajas: baja difusion de elementos, pueden alterarse por separado

Cifrado en bloque:

El mensaje se agrupa en bloques antes de aplicar un algoritmo a cada uno con la misma clave. El bloque **pequeño** facilita ataques por estadisticas, el **grande** lentitud del tratamiento del dato (poco rendimiento)

Ventajas: difusion de elementos, no se pueden introducir bloques extraños sin detectarlos.

Desventajas: baja velocidad de cifrado (hay que leer todo el bloque antes), puede tener errores de cifrado que se propagan a todo el bloque.

- **clave pública**: exponenciacion / suma o producto (firma digital, clave)

- **clave secreta**: cifrado propio en una sesion en internt o red, o local

Espacio de mensajes y criptogramas

Requisitos de un criptosistema:

Algoritmo de cifrado y descifrado rápido y fiable, se debe poder transmitir informacion por una linea de datos, almacenarlos o transferirlos, no debe existir retardo debido al cifrado o descifrado, la seguridad del sistema debera residir en el secreto de la clave solamente, no en las funciones. Fortaleza: imposibilidad de romper el cifrado, o encontrar una clave secreta a través de una pública.

Sistemas de clave secreta

Son criptosistemas **simétricos,** existe una única clave (comparten emisor y receptor) y con esta se cifra y descifra. La seguridad es mantener la clave en secreto. La debilidad es gestionarla mal o distribuirlas mal (porque no se puede asegurar mandarla de forma segura), no tiene firma digital aunque sí se puede autenticar el mensaje. Se utiliza porque es alta la velocidad de cifrado, el algoritmo es no lineal entonces lo unico es fuerza bruta, y con claves pequeñas se obtienne seguridad.

Sistemas de clave pública

Son criptosistemas **asimétricos**. Cada usuario tiene un par de claves, una pública y otra privada. Lo que se cifra con una se descifra con la otra. La seguridad es qué tan dificil es saber la clave privada a partir de la pública. Usan funciones unidireccionales con trampa.

No se puede comprobar la autenticidad del emisor si cuando se transmite el mensaje está protegido, entonces se usa llave privada en origen.

Cifrado simétrico: autenticacion parcial, sin firma digital, alta velocidad, uso en mucha información, claves de longitud pequeña, vida corta y número elevado.

Cifrado asimétrico: autenticacion total, firma digital, velocidad baja, uso en firma e intercambio de clave de sesion, longitud grande, vida larga, numero reducido.

No repudio: Se suma a integridad y confidencialidad. Asociado a la aceptacion de un protocolo de comunicación.

Tipos de ataques

- Fuerza bruta
- Analíticos: algoritmos
- Estadísticos: debilidades del diseño
- Implementación: no ataco el algoritmo, sino como fue implantado.
- COA: inteta desencriptar el texto directamete
- KPA: intenta hacerlo conociendo parte del texto plano.
- CPA: obtiene texto cifrado correspondiente a uno plano conocido.
- CCA: obtiene texto plano correspondiente a uno cifrado predeterminado

Algoritmos de hash: para generar salidas univocas de la enntrada. La salida debe tener tamaño fijo sin immportar la entrada. Tiene unidireccionalidad, compresion, facil de calcular, difusion. Se usa en contraseñas, firma digital, integridad, autenticacion.

En la firma digital se aplica clave privada en un hash, se comprueba descifrando con la clave publica y al mensaje se aplica el hash, si es lo mismo es íntegro.

Esteganografía: comunicar un mensaje ocultando la informacion para que pase desapercibida, puede cambiarse la extension y ser muy dificil de detectar. Puede además estar encriptada.

SEGURIDAD EN DESARROLLO DE SISTEMAS

Hay inseguridad porque los profesionales no saben de programacion, y al revés, hacen mucho enfasis en la funcionalidad. La comunidad lanza sistemas vulnerables y luego aplica parches.

Los proyectos fracasan por poca participacion del usuario, requerimientos u objetivos poco claros, falta de recursos, etc.

Comité de control de cambios: cambio analizado, probado, autorizado y documentado, no deben

afectar negativamente.

-Hay que tener un control de versionado y poder hacer rollback.

- Segregar funciones (arma matriz, carga incompatibles, identifica usuarios, arma plan de acción correctivo)

- Monitorear aplicaciones (definir qué eventos registrar, distintos niveles de login, cómo y donde registrarlos, monitorear usos indebidos y tener evidencias). Hay que loguear todo esto.

Firewall de BD: políticas de auditoria, de seguridad, firmas, scanner de vulnerabilidades, verificar permisos de BD, monitoreo y bloqueo de transacciones, nnotificaciones.

Buffer overflow: si el espacio de memoria es menor que lo ocupado los bytes se copian en memoria no reservada que puede tener estructuras de control del OS. Hay que revisar la variable, analizar código fuente, ver si hay anormalidades cuando se ejecuta. En los heap-based puede ser por mallocs, en los stack-based revisar los datos y su tamaño.

En el testeo estático se analiza el código, en el dinámico se ejecuta.

Técnicas de ataque:

- condicion de carrera

- revelacion de info

- fuzzing

- ingeniería inversa

- análisis de protocolos

- búsqueda de vulnerabilidades conocidas

OWASP

1) inyección: el atacante envia mensajes que explotan la sintaxis del intérprete, puede causar denegación de servicio, o modificació en los datos. Usar una API segura y validar valores de entrada o white list. Puede pasar con SQL o LDAP.

2) pérdida de autenticacion y gestion de sesiones: man in the middle para usar una sesion y saber datos

3) secuencia de comandos en sitios cruzados: el atacante envia cadenas de texto con comandos que explotan el intérprete. También hay que validar valores de entrada o white list y usar bibliotecas de sanitización

4) referencia directa insegura a objetos: un atacatnte puede estar como usuario autorizado en el sistema, modifica un valor de un parametro por otro para el cual el usuario no está autorizado. Hay que utilizar referencias indirectas para otorgar permisos e incluir comprobacion extra para las directas.

5) configuracion de seguridad incorrecta: accede a cuentas por defecto, paginas sin uso, etc para obtener acceso no autorizado. Hay que tener seguridad en capas y buena arquitectura.

6) exposicion de datos sensibles: roban claves en transito o del navegador del usuario Hay que aplicar algoritmos de cifrado para datos sensibles y asegurar que las claves se almacenan con un algoritmo diseñado para ellas.

7) ausencia de control de acceso a las funciones: por usuarios anonimos legítimos en el sistema, que cambian la url o parametros a funciones con privilegios. Hay que tener gestion de accesos y permisos, accesos cerrados por defecto.

8) **Falsificacion de peticiones en sitios cruzados:** http falsificadas y engaña a la victima. El usuario debe estar auntenticado. Utilizar un cookie o token oculto.

9) **Uso de componentes con vulnerabilidades conocidas:** el atacante identifica un componente debil. Hay que idetificar todo esto y revisar seguridad y politicas, agregar capas de seguridad.

10) **Redirecciones y reenvíos no validados:** enlaces a redirecciones y engaña a las victimas. Hay que prohibir el uso de redirecciones o reenvíos, y si se utiliza que no lo haga el usuario.

ANÁLISIS FORENSE

Es adquirir, prservar, obtener y presentar datos procesados electronicamente y almacenados informaticamente. Los puntos de pericia los determina el perito y genera informes si puede hacerlo. La **evidencia digital** puede ser: **repetible**, **integra** (saber si fue modificada), **recuperable** (aun borrada), contiene **metadatos**. Es **transportable**.

Pedido desde juzgado, elaboracion, secuestro de evidencia (permite relacionar eventos, puede ser real o digital), copias, cadena de custodia, análisis, reporte.

Desventajas: puede ser **modificada**, falta de cuidados en conservacion, trabajo con medios originales, falta de RRHH y equipamiento.

Hay que saber cómo se crea, falsifica, integridad, etc.

Sólo el profesional debe tener acceso al manejo de la evidencia, documentar todo, mantener la cadena de custodia y las acciones no deben cambiarla. La evidencia se puede ocultar con renombrado, alteracion de ubicación, compactado, encriptado, esteganografia.

Regla de la exclusión: obtenida en violacion de cualquier procedimiento técico o legal, es anulada.

Cadena de custodia: registro del pasaje de persona a otra, ubicación fisica a otra, registro de testigo, contacto con evidencia.

Adquisición de evidencia por **método directo**: requiere un bloqueador de escritura pero es el más fácil.

Adquisicion por **método indirecto**: permite hacerlo sin apertura, pero es más lento.

Procedimiento forense

Consiste en organizar el caso, examinar documentacion, controlar la cadena de custodia, elegir adquisicion y realizarla, verificar integridad, ver si hay archivos renombrados, enncriptados, etc. Hay que realizar busqueda de frases, de imagenes, la cache de internet, verificar evidencia, completar informe y guardar el material procesado.

AUDITORÍA

Es un control selectivo, lo compone un grupo independiente al proceso a auditar. Evalua eficiencia de los sectores y obtiene evidencias, con cursos de accion alternativos.

Aparte de detectar errores es para evaluar la eficiencia de un organismo. Determina alternativas para mejorar la organización Un **error** no es intencional, una **irregularidad** sí.

Hay que evaluar el área administrativa, sistemas, procedimientos, procesos de datos, seguridad, integridad y confidencialidad, aspectos legales, todos los tipos de riesgos.

La auditoria informatica revisa y evalua controles, sistemas, participa del procesamiento de datos para poder obtener informacion en forma segura y confiable, se basa sobre la integridad y confidencialidad

de la información.

El informe del auditor no es garantia, pueden haber irregularidades en el sistema de control, por eso hay que analizar los riesgos de auditoria por no haberlos detectado. Disminuyen con las evidencias.

Riesgos:

- **inherentes**: errores o irregularidades significativos antes de considerar los sistemas de control. Lo determina el entorno y la calidad de los recursos.

- **de control**: incapacidad de detectar errores por parte de estos sistemas. Ayuda a mitigar el riesgo inherente.

- **de deteccion**: que los procesos seleccionados no los detecten.

Procesos de auditoría

Consiste en identificar las afirmaciones y evaluar su importancia, reunir evidencia y analizarla, formular un reporte.

- **Planificación**: como encarar, puede ser **estratégica** (reunir conocimiento del ente desde el primer contacto) o **detallada** (cada componente en particular, para los programas de trabajo).

- **Ejecución**: cumplimentar procedimientos detallados en los programas de trabajo → tareas, selección dem uestra, deadline, etc

- **Evaluación**: de las evidencias y se emite el informe.

Procedimientos de auditoría dependen del tipo de evidencia que quiero obtener. Puede ser de cumplimiento de controles, o sustantivos (De la validez de los controles)

Auditoría externa

Acreditar que cierta información es real. Su objetivo es adecuar políticas, normas y procedimientos, evaluar la gestion de áreas de la empresa con relacion a las normativas y buenas prácticas. El sujeto debe ser un profesional **independiente.** El producto final, informes donde se identifica el estado de situacion y puede sugerirse tomar ciertas acciones. Revisa estados contables. En general lo solicita alguna autoridad de control como el BCRA.

Auditoría interna

Es un mecanismo de control selectivo e independiente del área en revisión. Debe informar las normas, si se cumplen congtroles internos, y promover la eficiencia en lo operativo. El sujeto puede no ser un profesional y es un empleado de la orgaización. El producto final, un informe analítico detallado con observaciones y sugerencias para mejorar el control interno, con conclusiones indicando plazos y responsabilidades de los planes de acción. Debe optimizar el costo beneficio.

El auditor participa en interna y externa. Responsabilidades:

Revision de sistemas en desarrollo: examen, participacion en fase de prueba, verificacion de tareas.

Revisión de datacenters: estructura, backup, redes, prácticas, recupero de desastres.

Revisión de aplicaciones contables

Evaluacion de controles para asegurar integridad de los resultados de procesamiento y mantener programas y archivos, prevenir que los errores sean detectados, asegurar confiabilidad de salidas y que se procesen solo las transacciones autorizadas, que los controles sean aplicados y probar los resultados del procesamiento, también evaluar la efectividad del sistema con los objetivos, lógica de la aplicación,

controles que ejecute el usuario.

Los **auditores no especializdos** recolectan y analizan datos, prueban controles, investigan inconsistencias. El profesional emite juicio a traves del informe del auditor.

Dictamen: informe donde el auditor expresa conclusión o no. Es **significativo** y **razonable** (margen de error)

ETHICAL HACKING

Necesidad de conocer el nivel de seguridad identificando puntos débiles, que se cumplan regulaciones, leyes y normativas, obtener info para la gestión de la seguridad a traves de un proceso de gestion de riesgos. Los procesos de evaluacion deben ser fundamentales en la estrategia de seguridad. Peor que tener debilidades es desconocerlas.

Las evaluaciones de seguridad permiten conocer el estado del sistema, identificar falta de controles. No es solucion integral, requiere combinarse con otros y no ser independientes, son ideales en un proceso continuo.

Deben ser periódicas y autorizadas legalmente.

Comercializacion de servicios: Como cliente hay que solicitar explicaciones a los proveedores mucho antes, asi podemos evaluar si conviene.

Contratacion: Suele requerir una cuota de confianza, debe informar al cliente el proceso y metodologias que va a usar, con buenas prácticas.

Common Vulnerability Scoring System (CVSS)

Captura caracteristicas, severidad de vulnerabilidades. Permite priorizar riesgos.

EVALUACIONES

Sobre sistemas y redes:

VS Y VA: alertar configuraciones incorrectas, falta de parches

Vulnerability Scanning: carácter no intrusivo, interno y externo, automático, poca o ninguna inteligencia profesional.

A) **Vulnerability Assessment**: a lo anterior le agrega verificaciones manuales para eliminar falsos positivos (aca hay profesionales).

B) Penetration test: para confirmar existencia de la amenaza.

Lo hace personal calificado, determiina qué puede hacer un intruso. Comprueba la seguridad, el desenvolvimiento del equipo de deteccion y respuesta, etc

Metodología del EH:

- **Reconocimiento**: recolectar informacion sin interactuar directamente (**sniffing**) o sí (**ing social**)

- **Escaneo**: previo al ataque, scanners, network mappers.

Tipos de escaneo: **red** (determina equipos activos y direcciones IP, OS y servicios), **puertos** (TCP abuertios, apps instaladas), **vulnerabilidades** (conocidas)

- **Obtencion de acceso**: penetracion, codigo exploit sobre sistema, dispositivo, engaño

- **Mantenimiento de acceso**: el atacante quiere apropiarse, instala troyanos, manipula cosas, asegura

acceso reiterado (Exclusivo)

- Eliminación de rastros.

El proceso consiste en discutir necesidades con el cliente, firmar un NDA, hacer el test, analizar resultados, hacer los reportes y presentarlos.

Entregables

- Informe: es confidencial, se entrega e mano, contiene info general de la evaluación. Es resumen ejecutivo, tiene vulnerabilidades, detalle de las pruebas, herramientas, técnicas, recomendaciones, clasificacion de problemas e info que lo pueda hacer repetible.

- Workshop (opcional): Es técnico y ejecutivo, presenta los resultados obtenidos en el proceso de evaluación, asesora con distintas alterativas.

C) Auditoría informática

Sobre software:

Testing de aplicaciones

Auditoría de código fuente.

El hacker ético simula u ataque real, lo que haría un intruso. Es experto en informática, con habilidades sociales. Las áreas de explotación son OS, código propio, apps, configuraciones. Los **ataques** son por **actividad** (pasivo o activo), **ubicación** (interno o externo), por **naturaleza** (técnico o no).

- Fases: reconocimiento, escaneo, acceso, mantenimiento, eliminación.

Las evaluaciones de seguridad deben estar presentes en toda organización.

Malware y botnets: Se propagan por internet o medios extraibles. Utilizan técnicas de **ocultación** como packers, binders y ofuscación (cambiar variables, flujo – mas lento - , insertar código corrupto).

LEGISLACIÓN INFORMÁTICA

Habeas data: derecho de quien figura en una bd de conocer la info y de pedir modificacion. Garantiza intimidad. Son datos personales o sensibles como opinniones, raza, salud. Sólo pueden ser recolectados por ley. Los antecedentes penales, sólo por autoridades públicas. Salud → secreto profesional.

Datos

Puede pedir que borren los datos, y el respinsable debe garantizar su seguridad y confidencialidad. No puede registrar datos en archivos que no sean integros y seguros. Es titular, usuario y responsable. No se puede transmitir a paises sin proteccion. El tratamiento de datos personales es ilicito si la persona no lo consiente, a menos que sea informacion tributaria, DNI, sea para el ejercicio de poderes del estado o se obtenga de lugares públicos. Hay que informar para qué y si es obligatorio o no decirlo.

DNPDP: es el órgano de control que tiene a su cargo el registro de las bases de datos, es el que recibe denuncias y se fija si la BD cumple con la ley.

Incorpora documentos (actos o hechos sin importar el soporte), firma y suscripción (firma digital), e instrumento privado y cerficiado.

No se regula el spam, ya es ilegal según habeas data.

Ley de firma digital

La firma digital debe ser susceptible de verificacion por terceros. Regula la creacion y alcances de la

firma, crea un ente administrador para otorgar licencias habilitantes.

Debe ser vigente, verificada, y certificado reconocido por un certificador licenciado.

La infraestructura es el conjunto de leyes, normativa, etc que permite que las entidades se identifiquen de manera segura al realizar transacciones en redes. Equivale a PKI. Participan el ente licenciante que otorga las licencias, las autoridades certificantes (AFIP, ANSES, que son proveedores de servicios de certificacion) y autoridades de registro que validan la identidad de los suscriptores.

La firma **electrónica** no es firma digital si no tiene todos los requisitos o si es desconocida debe acreditar validez.

Certificado digital

Documento digital firmado digitalmente, debe ser emitido por certificador, responder a estandares, contenner datos que permitan verificarse. No es válido si se usa para distintos fines, esta vencido o revocado. Debe contener identidad del propietario, clave pública, entidad que lo firma, numero de serie, algoritmo, fecha.

Ley de confidencialidad: siempre que sea secreta, tenga valor comercial, etc

Ley de propiedad intelectual: objetos → obras cientificas, literarias, etc. El titular es el autor, herederos, los que la traducen con permiso o modifican, personas contratadas en el desempeño de funciones laborales.

La explotacion incluye los contratos de licencia de uso. Se puede tener una copia de salvaguarda.

Vigencia: durante su vida y 70 años mas, despues es dominio publico. Sin herederos, 15 a quien la edite autorizadamente. Colaboracion y obrras póstumas → muerte del ultimo coautor. Cualquiera puede publicar hasta 1000 palabras.

BCP Y DRP

Hay que considerar integridad y confidencialidad en los procedimientos. La disponibilidad se afecta primero. Luego de daños en recursos tangibles, hay menos capacidad operativa.

La **continuidad del negocio** deberia formar parte del programa de seguridad, de las decisiones de negocio y del proceso de gestión de cambios.

Business Continuity Plan (BCP): describe cómo una org va a responder ante un evento para garantizar que no haya demoras o cambios inaceptables.

Tiene en cuenta personal, procesos alternnativos, lugares, equipamiento, configuraciones.

Protege vidas, reduce impacto, recupera la opratoria normal, provee respuesta ante situaciones de emergencia. Prepara a la organización para continuar, especialmente en lo **crítico**, con alcance global, no solo IT. Incluye al DRP.

Planes que lo componen

OEP: para la vida

CCP: distribucion de reportes al perosnal en desastres

BRP: recupero de operaciones de negocio en desastres. Puede incluir el retorno de funciones criticas.

CSP / IT CP : aplicaciones criticas o redes de procesamiento

CIRP: detectar y limitar consecuencias de ataques informáticos

COOP: funciones esenciales y estratégicas en un sitio alternativo durante 30 dias como mucho (sustentar)

DRP: recupero de capacidades en sitio alternativo, a largo plazo.

Disaster Recovery Plan (BCP): Minimizar efectos de un desastre para que todo vuelva a la normalidad rápido, se pone en marcha luego de ocurrido el desastre y es de IT.

Etapas

- política de continuidad: integrar requerimientos, definir objetivos, alcance, aprobacion de alta gerencia.

- BIA: identificar funciones y recursos criticos, amenazas, riesgos

- identificacion de controles preventivos: implementar y mitigar riesgos

- desarrollo de estrategias de recupero: procesos de negocio, edificios, etc.

- desarrollo de BCP: documentar procedimientos, soluciones, roles, respuestas

- mantenimiento del BCP: integrar en el proceso de control de cambios, asignar responsabilidades, actualizar plan y distribuirlo.

- prueba del BCP: y mejora, entrenamiento de empleados

Roles y responsabilidades: definir un comité de BCP que interactue con gerencia para que haga todo lo anterior. Debe estar integrado por familiarizados con actividades de los departamentos y experiencia en planes.

- alta gerencia: inicia, aprueba, apoya

- comité: dirige, implanta, prueba. Son unidades de negocio, gerencias, ti, seguridad, comunicaciones, legales.

- gerencia de unidades de negocio: identifica y prioriza operaciones

- coordinador del comité

- unidades funcionales: participa en planificar, e implantacion y prueba.

Hay que desarrollar politica de continuidad y plan de proyecto (mapeo de objetivos, recursos ,tareas, puntos de control, costos)

BIA

Plantear los peores casos. Evaluar nivel de criticidad. Se realiza al comienzo del BCP para determinar mayor pérdida económica. Determinar funciones que necesitan seguir operando y tiempo de caida tolerado. Considerar legales y regulaciones, reputación. Esto es parte del impacto.

Hay que recolectar circuitos, procesos. Se prefiere lo preventivo ante que los reactivos.

Medidas preventivas: redundancia, UPS, backup, proteger medios de almacenamiento, empleo de materiales fuertes de construccion, etc. Buscan reducir la probabilidad de que ocurra. El recupero es cuando ya ocurrio, el equipo debe comprender los pasos.

DRP Centros de cómputos

- **Hot Site**: Pertenece a la org, listo para operar en horas, faltan datos actuales y usuarios. Se prueba anualmente, es costoso. Soporta interrupciones cortas o largas. Es un servicio de suscripcion, no un sitio redundante. Los backup deben ser comprobados siempre enn el hot site para ver que lo pueda interpretar.

- **Warm Site**: como el anterior sin equipammiento costoso (no tanta redundancia), es un sitio de procesamiento y algunos periféricos. Puede operar durante un tiempo aceptable.

- **Cold Site**: brinda el entorno básico o la infraestructura. Puede tomar semanas que esté listo así que requiere más esfuerzo. No se prueba.

Acuerdos reciprocos con empresas

Mobile sites: trailer o acoplado con energia y sistemas

Sitios redundantes: configurado igual que el primero, pertenece a la org. No operan hasta que se interrumpa el primario.

Backup: debe contarse ocn clasificacion de info, cada propietario debe definir necesidad de backup, los custodios son responsables de que se cumpla. Deben haber ormas sobre la información a resguardar, lugares, responsables.

Puede ser de **hardware** con dispositivos redundantes o de **software** con copias de resguardo.

Puede ser **full** con todos los archivos modificados o no, es más simple, **incremental** con modificados desde la ultima copia full o incremental, marca los copiados, insume menos tiempo y recursos, **diferencial** copia los creados o modificados desde la ultima pero no lo marca como copiado, insume más tiempo en backup pero menos en restaurarse, que el anterior. No deben mesclarse los dos ultimos.

Un **desastre** es cualquier evento que inhabilite a la org de hacer funciones criticas.

Hay que tener un entorno operativo lo mas pronto posible, cada gerente debe notificar a su personal.

Los datos criticos deben estar **onsite** en caso de no desastres y **offsite** en caso de desastre o catástrofe.

Pueden contratar servicios de almacenamiento externo, pero ver disponibilidad, mecanismos de control de acceso que tiene, etc

Backups

- **Electronic vaulting:** periodico. El **tape** es manual.

- **Remote**: solo transmite el log de transaciones, es util para BD dañadas o perdidas.

- **HSM**: resguardos online continuos, combina tecnologias de almacenamiento con otros mas baratos.

- **SAN**: varios sistemas de almacenamiento en red.

Cada depto puede tener su BCP y DRP, integrado con los otros. Puede ser realizado por personal propio o externo, debe definir funciones de los equipos, comunicación, tareas del equipo de estimacion de daños que actua primero y decide si activa BCP. El BCP se prueba una vez por año. En las pruebas hay que considerar tiempo.

Puede hacerse una **simulacion** donde se reunen todos, una **prueba en paralelo** donnde se desplaza el sistema al sitio secundario, o **interrupcion completa**.

Puede el BCP dejar de ser vigente según cambios en infraestructura, modificaciones de HW, etc. Hay que integrar siempre el BCP al proceso de gestion de cambios y considrarlo en decisiones directivas.