Resumen Segundo Parcial Ciberseguridad

Clase 12 - Plan de Continuidad del Negocio y Plan de Respuesta a Incidentes

Plan de Continuidad del Negocio (BCP)

- **Objetivo:** Minimizar el impacto de un incidente de ciberseguridad en la continuidad del negocio.
- **Componentes:**
  - Estrategia general: identificar sistemas y servicios críticos, objetivos de recuperación, procedimientos de recuperación y restauración.
  - Prueba y mantenimiento: realizar pruebas y simulaciones regulares, actualizar el plan periódicamente.
- **Fases:**
  1. Análisis de impacto en el negocio (BIA): identificar procesos y recursos críticos.
  2. Evaluación de riesgos: identificar amenazas y vulnerabilidades.
  3. Desarrollo de estrategias: crear planes de recuperación y restauración, comunicación, continuidad de operaciones y gestión de crisis.
  4. Implementación: instalar medidas de seguridad, implementar sistemas de recuperación de desastres, realizar pruebas.
  5. Prueba y mantenimiento: realizar pruebas y simulaciones regulares, actualizar el plan periódicamente.
- **Métricas:**
  - Tiempo de recuperación objetivo (RTO)
  - Tiempo de punto de recuperación objetivo (RPO)
  - Nivel de servicio (SLA)

Plan de Respuesta a Incidentes (IRP)

- **Objetivo:** Minimizar el impacto de un incidente de ciberseguridad en la organización.
- **Componentes:**
  - Estrategia general: procedimientos para identificar, contener, analizar, erradicar y recuperar incidentes.
  - Equipo de respuesta a incidentes: roles y responsabilidades.
  - Procedimientos detallados: recolección y preservación de evidencia, notificación, comunicación interna y externa.
  - Evaluación y análisis: causas e impacto del incidente.
  - Medidas preventivas: prevenir futuros incidentes.
  - Prueba y mantenimiento: realizar pruebas y simulaciones regulares, actualizar el plan periódicamente.
- **Fases:**
  1. Preparación: establecer procedimientos y recursos para responder a incidentes.
  2. Identificación: detectar y confirmar la existencia de un incidente.
  3. Contención: tomar medidas para contener el incidente.

4. Investigación: investigar la causa y el alcance del incidente.
5. Eliminación: eliminar los efectos del incidente.
6. Recuperación: restaurar sistemas y servicios a su estado normal.
7. Lecciones aprendidas: evaluar el incidente y documentar las lecciones aprendidas.

- **Métricas:**
  - Tiempo de detección del incidente
  - Tiempo de respuesta
  - Tiempo de recuperación
- **¿Por cuál empezar?**
  - Se recomienda implementar primero el BCP y luego el IRP.
  - El BCP aborda riesgos a largo plazo que afectan la continuidad del negocio.
  - El IRP aborda riesgos a corto plazo que interrumpen las operaciones.

Conclusión:

- El BCP y el IRP son esenciales para proteger la organización de incidentes de ciberseguridad.
- El BCP garantiza la continuidad del negocio, mientras que el IRP protege la información y los sistemas críticos.
- La implementación del BCP y el IRP debe realizarse de manera ordenada y siguiendo las mejores prácticas.

Clase 13 - Análisis de Riesgos

Introducción:

- El análisis de riesgos es fundamental para mejorar la seguridad de la información en las organizaciones.
- El Plan Director de Seguridad (PDS) ayuda a reducir los riesgos a niveles aceptables.

Fases para la Gestión de Riesgo:

1. Definir el alcance:

- Establecer el alcance del estudio, considerando el área estratégica o sistema a analizar.
- En este caso, el alcance es "Los servicios y sistemas del Departamento Informática".

2. Identificar los activos:

- Identificar los activos más importantes del departamento, proceso o sistema.
- Utilizar una hoja de cálculo o tabla para mantener un inventario sencillo.

3. Identificar/seleccionar las amenazas:

- Identificar las amenazas a las que están expuestos los activos.
- Considerar amenazas prácticas y aplicadas, como fallos de servidores o daños por agua.
- Usar el catálogo de amenazas MAGERIT v3 como referencia.

4. Identificar vulnerabilidades y salvaguardas:

- Identificar puntos débiles o vulnerabilidades en los activos.
- Considerar vulnerabilidades como sistemas antivirus desactualizados o falta de soporte.
- Analizar y documentar las medidas de seguridad implantadas (salvaguardas).

5. Evaluar el riesgo:

- Calcular el riesgo para cada par activo-amenaza.
- Utilizar criterios cuantitativos o cualitativos.
- Considerar vulnerabilidades y salvaguardas al estimar probabilidad e impacto.

6. Tratar el riesgo:

- Tratar los riesgos que superen un límite establecido (por ejemplo, "4" o "Medio").
- Aplicar una de las cuatro estrategias:
    1. Transferir el riesgo a un tercero (seguro contra fugas de información).
    2. Eliminar el riesgo (eliminar proceso o sistema de alto riesgo).
    3. Asumir el riesgo, siempre justificadamente (alto costo de medidas).
    4. Implementar medidas para mitigarlo (acceso a internet de respaldo).

Conclusiones:

- El análisis de riesgos dentro del PDS ayuda a mejorar la seguridad de la organización.
- Se recomienda realizar este tipo de proyectos de forma aislada o dentro del PDS.

Puntos adicionales:

- El documento proporciona tablas para el cálculo de la probabilidad e impacto.
- Se utiliza una matriz de riesgo para facilitar la evaluación del riesgo.
- Se enfatiza la importancia de considerar vulnerabilidades y salvaguardas.
- Las acciones para tratar los riesgos se integran en el PDS.

Clase 14 - Seguridad en Sistemas Operativos Modernos Parte 1

Introducción:

- Un sistema operativo es un software fundamental que gestiona los recursos de hardware y software de una computadora.
- Es esencial para la seguridad, permitiendo la conexión a internet, la computación en la nube, la IA/ML, el IoT y más.
- Facilita la productividad, la innovación y el acceso a la información.

Seguridad:

- Los sistemas operativos modernos implementan medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas.
- El kernel es el núcleo del sistema operativo y se ejecuta en modo privilegiado, controlando el acceso a los recursos.

Estados privilegiados y no privilegiados:

- Los programas y usuarios operan en diferentes estados de acceso y control.
- El estado privilegiado (modo kernel) permite acceso completo al sistema, mientras que el estado no privilegiado (modo usuario) tiene acceso restringido.
- Esta distinción es crucial para la seguridad, limitando las acciones que pueden realizar los usuarios y programas.

Procesos e hilos:

- Los procesos son unidades de ejecución que gestionan recursos y permiten la ejecución concurrente de tareas.
- Los hilos son unidades de ejecución dentro de un proceso, compartiendo su memoria y recursos.
- La seguridad en procesos e hilos se aborda mediante mecanismos del sistema operativo, prácticas de programación seguras y medidas de seguridad a nivel de aplicación.

Puntos importantes:

- El principio de privilegios mínimos: los programas y usuarios solo deben tener los privilegios necesarios para realizar sus tareas.
- Aislamiento de procesos y memoria: cada proceso tiene su propio espacio de memoria para evitar accesos no autorizados.
- Protección de memoria: impide que un proceso acceda a áreas de memoria no asignadas o privilegiadas.
- Control de acceso: regula el acceso de los procesos a recursos del sistema.
- Sincronización de hilos: garantiza el acceso seguro a recursos compartidos dentro de un proceso.
- Aislamiento de hilos: evita que un hilo malicioso afecte a otros hilos del mismo proceso.

- Seguridad de las bibliotecas compartidas: asegura que las bibliotecas de terceros sean confiables y no contengan vulnerabilidades.

Clase 15 - Seguridad en Sistemas Operativos Modernos Parte 2

Introducción:

- La seguridad en los sistemas operativos es crucial para proteger la información y los recursos de los usuarios.
- Los sistemas operativos modernos implementan diversas medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Conceptos fundamentales:

- **Estados privilegiado y no privilegiado:** Los programas y usuarios operan con diferentes niveles de acceso y control al sistema.
- **Procesos e hilos:** Unidades de ejecución que permiten la gestión eficiente de recursos y la ejecución concurrente de tareas.
- **Memoria:** Almacena datos e instrucciones de forma temporal para el funcionamiento del sistema.
- **Sistemas de archivos:** Organizan y almacenan los datos en un dispositivo de almacenamiento persistente.
- **Virtualización:** Permite crear entornos informáticos virtuales independientes dentro de un solo computador físico.
- **Hipervisores:** Software que gestiona los recursos del computador físico y los asigna a las máquinas virtuales.
- **Principios de diseño de seguridad:** Directrices para crear sistemas operativos más seguros y confiables.

Aspectos de seguridad:

- **Aislamiento:** Proteger cada componente del sistema para evitar accesos no autorizados.
- **Control de acceso:** Limitar quién puede acceder a los recursos del sistema y qué acciones pueden realizar.
- **Protección de datos:** Cifrar y proteger los datos confidenciales.
- **Actualizaciones de seguridad:** Aplicar actualizaciones regularmente para corregir vulnerabilidades.
- **Monitoreo y registro:** Vigilar la actividad del sistema para detectar anomalías.

Consideraciones adicionales:

- Amenazas potenciales a las que está expuesto el sistema operativo.
- Requisitos de seguridad específicos que debe cumplir.
- Facilidad de uso para los usuarios legítimos.

Clase 16 - Seguridad en Sistemas Operativos Modernos Parte 3

Introducción a la virtualización:

- La virtualización permite crear entornos informáticos aislados ("máquinas virtuales") dentro de un solo computador físico.
- Los hipervisores son el software que gestiona los recursos del computador físico y los asigna a las máquinas virtuales.

Aspectos de seguridad en la creación de entornos virtualizados:

- **Elección del hipervisor:** Seleccionar uno con historial de seguridad probado y actualizaciones regulares.
- **Configuración segura del hipervisor:** Habilitar autenticación fuerte, deshabilitar servicios innecesarios y aplicar las últimas correcciones de seguridad.
- **Aislamiento de las máquinas virtuales:** Aislarlas entre sí y del servidor host para evitar que un ataque en una afecte a las demás.
- **Protección de datos:** Cifrar y proteger los datos almacenados en las máquinas virtuales.
- **Gestión de identidades y accesos:** Implementar un sistema IAM para controlar el acceso a las máquinas virtuales y a los recursos del servidor host.

Aspectos de seguridad en la operación de entornos virtualizados:

- **Monitoreo y registro:** Monitorear los entornos virtualizados para detectar actividades sospechosas y registrar todos los eventos de seguridad.
- **Actualizaciones de software:** Aplicar las últimas actualizaciones de seguridad al hipervisor, a las máquinas virtuales y al software que se ejecuta en ellas.
- **Pruebas de penetración:** Realizar pruebas de penetración regulares para identificar y corregir las vulnerabilidades de seguridad.
- **Capacitación del personal:** Capacitar al personal sobre los riesgos de seguridad de la virtualización y las mejores prácticas para mitigarlos.

Herramientas de seguridad para entornos virtualizados:

- Análisis de vulnerabilidades
- Detección de intrusiones
- Prevención de intrusiones
- Protección de datos

Principios fundamentales de diseño de seguridad:

- **Principio de mínima confianza:** Ningún componente debe tener más privilegios de los necesarios.
- **Defensa en profundidad:** Implementar múltiples capas de seguridad para proteger el sistema.
- **Falla segura:** Diseñar el sistema para que en caso de fallo se encuentre en un estado seguro.

- **Separación de privilegios:** Las tareas críticas deben ser realizadas por diferentes componentes con diferentes privilegios.
- **Menor superficie de ataque:** Minimizar la cantidad de código e interfaces expuestas.
- **Protección contra errores de software:** Diseñar el sistema para que sea resistente a errores de software.
- **Cifrado:** Cifrar los datos confidenciales tanto en reposo como en tránsito.
- **Gestión de identidades y accesos:** Implementar mecanismos sólidos para la gestión de identidades y accesos.
- **Monitoreo y registro:** Registrar los eventos de seguridad y monitorear los registros para detectar actividades sospechosas.
- **Actualizaciones y parches:** Mantener el sistema actualizado con los últimos parches de seguridad.

Controles de Acceso:

- Conjunto de medidas y mecanismos para limitar y regular el acceso a los recursos informáticos.
- Objetivo: proteger la información confidencial, prevenir el uso no autorizado de recursos y mantener la integridad del sistema.

Mecanismos de control de acceso:

- **Autenticación:** Verificar la identidad de un usuario o entidad.
- **Autorización:** Determinar los permisos que tiene un usuario o entidad para acceder a un recurso del sistema y qué acciones puede realizar sobre él.
- **Listas de Control de Acceso (ACL):** Estructuras de datos que asocian permisos a usuarios o grupos para recursos específicos.
- **Tablas de Control de Acceso (MAC):** Tablas mantenidas por el sistema operativo que especifican los permisos de acceso para cada recurso y usuario/grupo.
- **Módulos de Control de Acceso (MAC):** Componentes del sistema operativo que implementan la lógica de control de acceso.

Modelos de control de acceso:

- **Control de acceso basado en listas de control de acceso (ACL):** Asocia permisos específicos a usuarios o grupos para recursos individuales o grupos de recursos.
- **Control de acceso basado en roles (RBAC):** Asigna permisos a los usuarios en función de sus roles dentro de la organización.
- **Control de acceso basado en atributos (ABAC):** Permite definir permisos basados en una combinación de atributos del usuario, el recurso y el entorno.

Implementación en sistemas operativos comunes:

- **Windows:** Utiliza ACL y RBAC principalmente.

- **Linux:** Utiliza principalmente RBAC y SELinux (Security Enhanced Linux).
- **macOS:** Similar a Windows, utiliza ACL y RBAC.

Métodos de control de acceso:

- **Controles de acceso a la red (NAC):** Firewalls y VPNs para restringir el acceso a los recursos de la red.
- **Control de acceso a aplicaciones:** Mecanismos de autenticación, autorización y control de datos en aplicaciones.

Importancia de los controles de acceso:

- **Protección de información confidencial.**
- **Prevención del uso no autorizado de recursos.**
- **Mantenimiento de la integridad del sistema.**
- **Cumplimiento de regulaciones de seguridad.**

Conceptos fundamentales de seguridad:

- **Separación de dominios:** Aislar secciones del sistema para limitar el alcance de ataques o fallos.
- **Aislamiento de procesos:** Ejecutar cada aplicación en su propio espacio de memoria para evitar interferencias.
- **Encapsulación de recursos:** Proteger los recursos del sistema mediante mecanismos de control de acceso.
- **Mínimo privilegio:** Asignar solo los permisos necesarios a usuarios y procesos.

Implementación en sistemas operativos modernos:

- **Control de acceso basado en roles (RBAC):** Permisos según el rol del usuario.
- **Listas de control de acceso (ACL):** Especificar acceso y acciones permitidas.
- **Sandboxes:** Ejecutar aplicaciones en entornos aislados.
- **Cuentas de usuario limitadas:** Restringir acceso a funciones administrativas.

Beneficios:

- **Protección contra malware y ataques.**
- **Minimización de daños.**
- **Mejora de la confiabilidad.**
- **Cumplimiento de normativas.**