TEMA 5

Seguridad del Sistema Operativo

CONTROLES DE ENDURECIMIENTO DEL SISTEMA

(SYSTEM HARDENING) es el proceso de implementación de controles de seguridad.

Los proveedores de computadoras configuran los controles predeterminados para que estén abiertos, lo que permite un uso fácil sobre la seguridad. Pueden existir vulnerabilidades significativas a menos que el sistema esté reforzado. Los controles comunes para el endurecimiento del sistema incluyen:

- Autenticación y autorización.
- Permisos del sistema de archivos.
- Privilegios de acceso.
- Registro y monitoreo del sistema.
- Servicios del sistema.

CREDENCIALES Y PRIVILEGIOS

- Las credenciales de un usuario definen quiénes son y qué permisos tienen para acceder a los recursos dentro del sistema.
- Las contraseñas son el mecanismo estándar para autenticar a un usuario en el sistema.
- En otra forma de limitación de acceso, se pueden asignar privilegios a un usuario en particular.
- Para evitar el mal uso o compromiso, estos deben ser cuidadosamente elegidos y controlados.
- El acceso del usuario también puede estar limitado a través de restricciones de inicio de sesión con respecto a la hora del día, la duración del inicio de sesión, la dirección de origen y el número de intentos de inicio de sesión fallidos.

ENDURECIMIENTO DE PLATAFORMA

El endurecimiento es un proceso que reduce la vulnerabilidad al limitar los vectores de ataque. Un sistema endurecido comprende:

- No almacena datos confidenciales que no se necesitan de inmediato para respaldar una operación comercial.
- Tiene todas las funcionalidades innecesarias deshabilitadas, incluidos puertos, servicios y protocolos que no son necesarios para el uso previsto.
- Utiliza solo contraseñas y cuentas que se han cambiado o deshabilitado. No hay contraseñas predeterminadas o cuentas de invitado.

VIRTUALIZACIÓN

La virtualización brinda a una empresa una oportunidad significativa para aumentar la eficiencia y disminuir los costos en sus operaciones de TI.

VENTAJAS	DESVENTAJAS
Los costos de hardware del servidor pueden disminuir para las compilaciones y el mantenimiento del servidor.	La configuración inadecuada del host podría crear vulnerabilidades que afectan a los hosts e invitados.
Múltiples sistemas operativos pueden compartir la capacidad de procesamiento y el espacio de almacenamiento, reduciendo los costos operativos.	La explotación de vulnerabilidades o un ataque de denegación de servicio podrían afectar a todos los huéspedes anfitriones.
La huella física de los servidores puede disminuir dentro del centro de datos.	Un compromiso de la consola de administración podría otorgar a los invitados acceso administrativo no aprobado.
Un único host puede tener múltiples versiones del mismo sistema operativo, o incluso diferentes sistemas operativos.	Los datos podrían filtrarse entre los invitados si el host no libera y asigna la memoria correctamente.
La creación de copias duplicadas de invitados en ubicaciones alternativas puede respaldar los esfuerzos de continuidad del negocio.	Los protocolos de acceso remoto inseguros podrían dar lugar a la exposición de credenciales administrativas.
Una sola máquina puede alojar una red de varios niveles en un entorno de laboratorio educativo.	Los problemas de rendimiento del propio sistema operativo del host podrían afectar a cada uno de los invitados del host.

RIESGO DE VIRTUALIZACIÓN

En un entorno virtualizado, el anfitrión representa un posible punto único de falla dentro del sistema.

Un ataque exitoso al host podría resultar en un compromiso de mayor alcance e impacto.
Para abordar este riesgo, una empresa a menudo puede implementar y adaptar los mismos principios y mejores prácticas para un entorno de servidor virtualizado que usaría para una granja de servidores. Éstos incluyen:

- Fuertes controles de acceso físico y lógico.
- Prácticas sólidas de gestión de la configuración y endurecimiento del sistema para el host.
- Segregación de red apropiada.
- Fuertes prácticas de gestión del cambio.

SISTEMAS ESPECIALIZADOS

Algunos sistemas y aplicaciones son muy especializados y pueden tener amenazas y riesgos únicos y requieren diferentes tipos de controles.

Los Sistemas especializados incluyen sistemas de control de supervisión y adquisición de datos (SCADA) u otros sistemas de monitoreo o control en tiempo real.

Estos Sistemas operan en entornos especializados que controlan procesos críticos industriales y de fabricación, generación de energía eléctrica, control de tráfico aéreo, comunicaciones de emergencia y sistemas de defensa.

Los SCADA, requieren una evaluación de riesgos y amenazas y una mitigación adecuada.

¿WannaCry es un ejemplo de qué tipo de ataque?

- Caballo de Troya
- APTO
- **Secuestro de datos (Ransomware)**
- Suplantación de identidad
- Ingeniería social

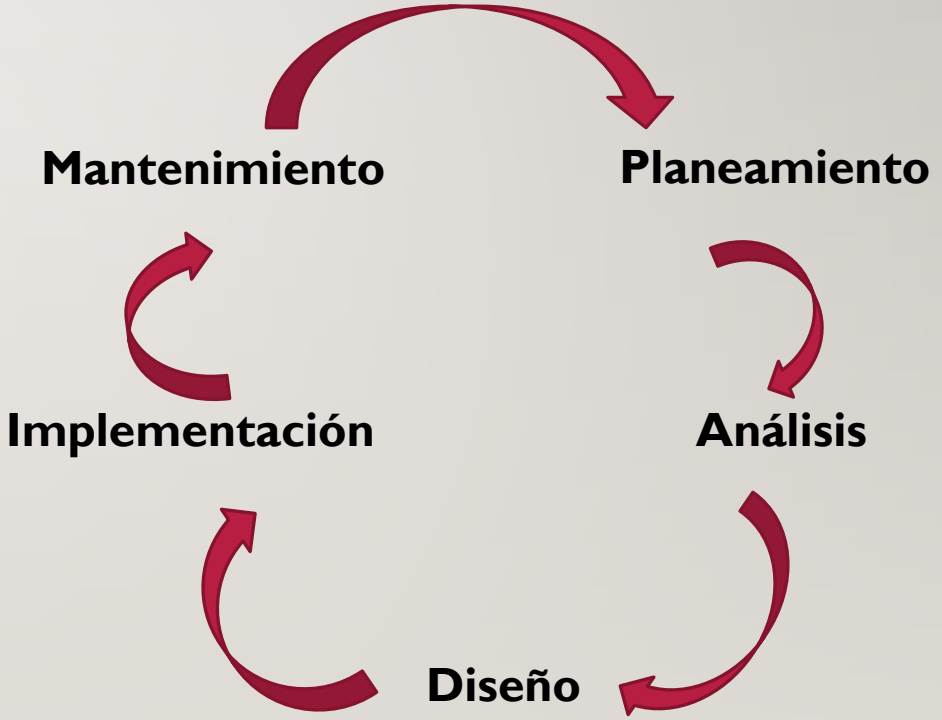
TEMA 6

Seguridad de la Aplicación.

CICLO DE VIDA DEL DESARROLLO DEL SISTEMA (**SDLC**)

El proceso **SDLC** guía las fases de desarrollo o adquisición de un sistema de software. Incluye:

Procesos de TI para gestionar y controlar la actividad del proyecto. Un objetivo para cada fase del ciclo de vida, típicamente descrito con entregables clave, una descripción de las tareas recomendadas y un resumen de los objetivos de control relacionados para una gestión efectiva Pasos incrementales o entregables que sientan las bases para la siguiente fase.



SEGURIDAD DENTRO DE SDLC

No considerar la seguridad en el diseño de un sistema o aplicación es un factor importante que contribuye a las vulnerabilidades de ciberseguridad.

La seguridad es a menudo una ocurrencia tardía, con controles modificados solo después de que las debilidades de seguridad han sido expuestas.

La seguridad y la mitigación de riesgos deben ser criterios de diseño formales en cualquier proceso SDLC, que incluyen:

- Amenaza y evaluación de riesgos del sistema propuesto.
- Identificación e implementación de controles.
- Pruebas de vulnerabilidad y revisión

DIEZ PRINCIPALES RIESGOS DE SEGURIDAD DE APLICACIONES DE OWASP, 2017

- Inyección
- Autenticación rota
- Exposición de datos sensibles
- Entidades externas XML (XXE)
- Control de acceso roto
- Configuración incorrecta de seguridad
- Cross-Site Scripting (XSS)
- Deserialización insegura
- Uso de componentes con vulnerabilidades conocidas
- Insuficiente registro y monitoreo

PRUEBAS SDLC Y FASES DE REVISIÓN

La fase de prueba de SDLC incluye:

- Verificación y validación de que los programas, aplicaciones y controles realizan las funciones para las cuales han sido diseñados.
- Confirmación de que las unidades probadas funcionan sin mal funcionamiento o efectos adversos en otros componentes del sistema.
- Pruebas de vulnerabilidad y control, tomadas desde una perspectiva de seguridad.

La fase de revisión de SDLC incluye:

- Procesos de revisión de código que varían de procesos informales hasta recorridos formales.
- Revisión del equipo o inspecciones de código.

Tenga en cuenta que la seguridad debe ser una parte integrada de cualquier proceso de revisión.

ENTORNOS DE DESARROLLO Y PRUEBA

Se deben usar entornos de desarrollo, prueba y producción separados durante SDLC para minimizar un compromiso o una configuración incorrecta que se introduce o conecta en cascada a través del proceso.

Se deben utilizar diferentes controles de acceso (credenciales) entre estos diferentes entornos.

Tenga en cuenta que, si los datos de producción se utilizan en el entorno de prueba, la información de identificación privada o personal debe cambiarse para que la información confidencial no se divulgue inadvertidamente.

ENFOQUES DE DESARROLLO AGILE Y DEVOPS

Agile permite que los proyectos de desarrollo de software se construyan de manera más flexible e iterativa. Esto permite una respuesta más rápida a los cambios que ocurren durante un proyecto. También facilita las pruebas de seguridad en las primeras etapas del proceso de desarrollo.

El desarrollo y las operaciones de TI (DevOps) combinan los conceptos de **desarrollo ágil**, **infraestructura ágil** y **operaciones flexibles**. DevOps divide grandes proyectos en entregas más pequeñas y más manejables y múltiples implementaciones. Estas implementaciones más pequeñas pueden depurarse más fácilmente durante el proceso de desarrollo.

AMENAZAS ADICIONALES

Los profesionales de la seguridad deben ser conscientes de una variedad de amenazas. Se debe tener en cuenta las siguientes amenazas:

- Canal encubierto: transfiere información entre sistemas de forma ilícita, utilizando la infraestructura existente.
- Condición de carrera: accede a redes sin autorización, utilizando vulnerabilidades de procesamiento de operaciones.
- Esteganografía: oculta mensajes, imágenes o archivos dentro de otro archivo similar.

PROTOCOLO DE APLICACIÓN INALÁMBRICA (WAP)

Los protocolos WAP (Wireless Application Protocol) llevan contenido de Internet a dispositivos móviles inalámbricos.

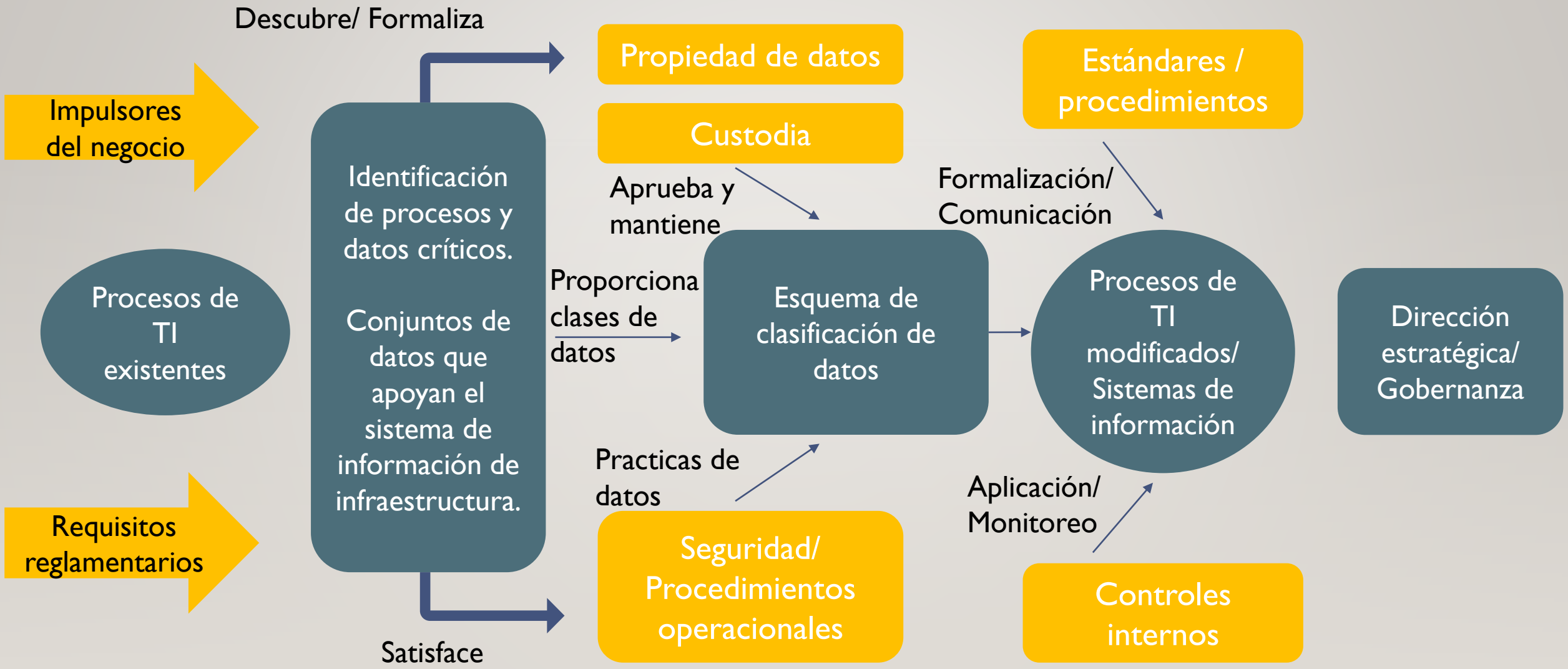
WAP es compatible con la mayoría de las redes inalámbricas y es compatible con todos los sistemas operativos diseñados específicamente para dispositivos de mano y algunos teléfonos móviles.

Los micro navegadores tienen archivos de tamaño pequeño que pueden acomodar las limitaciones de poca memoria de los dispositivos portátiles y las limitaciones de bajo ancho de banda de una red inalámbrica de dispositivos portátiles.

TEMA 7

Datos de Seguridad

PROCESO DE CLASIFICACIÓN DE DATOS



REQUISITOS DE CLASIFICACIÓN DE DATOS

Al clasificar los datos, se deben cumplir los siguientes requisitos:

- Acceso y autenticación
- Privacidad
- Disponibilidad
- Propiedad y distribución
- Integridad
- Retención de datos
- Auditabilidad
- Una vez que se ha asignado la clasificación de datos, se pueden establecer controles de seguridad, incluidos el cifrado, la autenticación y el registro.
  Las medidas de seguridad deberían aumentar a medida que se incrementa el nivel de sensibilidad o criticidad de los datos.

CLASIFICACIÓN DE DATOS

- Es importante que una organización entienda la sensibilidad de la información que posee.
- Los datos deben clasificarse en función de su sensibilidad y el impacto de la liberación o pérdida involuntaria.
- La clasificación de datos debe definirse en una política que proporcione la definición de diferentes clases de información y su manejo y protección.
- Mantenga los niveles al mínimo, use niveles de descripción claros. Se debe reclasificar la información de acuerdo a las necesidades del negocio y sus regulaciones legales.
- Definir niveles en la política.

CONTROLES DE BASE DE DATOS

Las bases de datos se pueden proteger individualmente con un control similar a las protecciones aplicadas a nivel del sistema. Los controles específicos que se pueden colocar a nivel de base de datos incluyen:

- Autenticación y autorización de acceso.
- Los controles de acceso limitan o controlan el tipo de datos a los que se puede acceder y qué tipos de acceso están permitidos (solo lectura, lectura y escritura o eliminación).
- Registro y otro monitoreo transaccional.
- Encriptación y controles de integridad.
- Copias de seguridad.

VULNERABILIDADES DE LA BASE DE DATOS

Las bases de datos son vulnerables a muchos riesgos, que incluyen:

- Actividad no autorizada por usuarios autorizados.
- Infecciones o interacciones de malware.
- Problemas de capacidad.
- Daño físico.
- Defectos de diseño.
- Corrupción de datos

SEGURIDAD DE LA BASE DE DATOS 1/2

La seguridad de la base de datos se puede aumentar mediante las siguientes acciones:

- Cifrado de datos confidenciales en la base de datos.
- Uso de vistas de bases de datos para restringir la información disponible para un usuario.
- Protocolos seguros para comunicarse con la base de datos.
- Aplicación de controles de acceso basados en contenido.
- Restringir el acceso a nivel de administrador.
- Indexación eficiente para mejorar la recuperación de datos.

SEGURIDAD DE LA BASE DE DATOS 2/2

La seguridad de la base de datos se puede aumentar mediante las siguientes acciones:

- Copias de seguridad de bases de datos (Completo, Diferencial, Incremental).
- Copias de seguridad de diarios de transacciones (diario, periódico, remoto).
- Integridad referencial.
- Integridad de la entidad.
- Validación de entrada.
- Campos de datos definidos (esquema).
- Restricciones de acceso a la red en capas o segregación.