Seminario de Seguridad Informática con énfasis en hacking ético.

joseroberto.rivas@itservicesin.com

503-78876717

CLASE 004 28/Febrero/2021

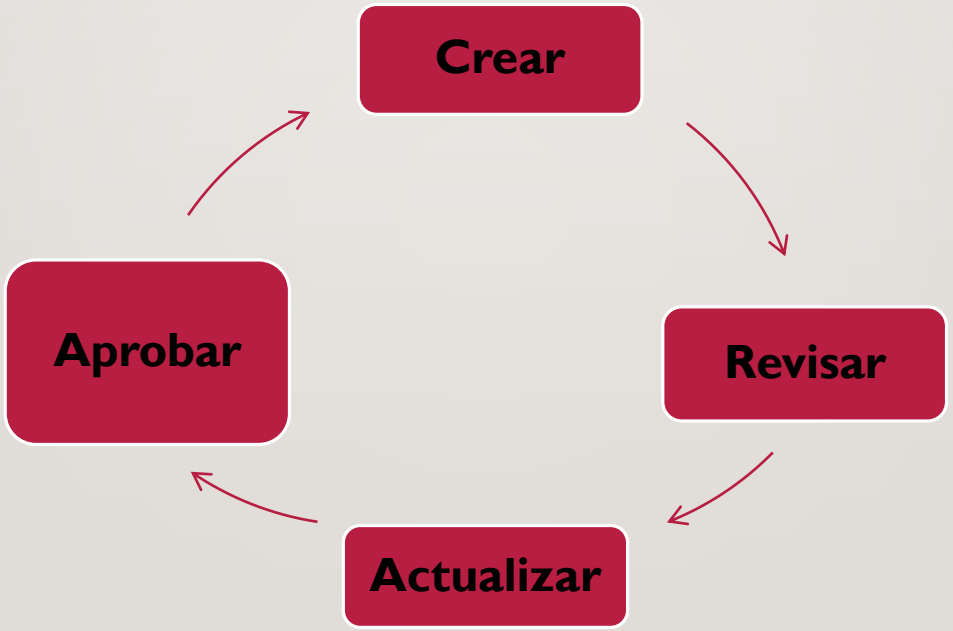
INGENIERO JOSE ROBERTO RIVAS MAGAÑA. MBA. M.SC.

DOCENTE MINED NIVEL I, GERENTE DE PROYECTOS Y AUDITOR LIDER INTEGRADO.

2.3 Políticas

Ciclo de vida de la política.

Cada política de seguridad de la información debe ser parte de un proceso formal de ciclo de vida.



Tipos de documentos de conformidad

21/2/2021 23:43:14

Tipo	Descripción
Políticas	Comunicar las actividades y comportamientos requeridos y prohibidos.
Estándares	Interpretar políticas en situaciones especificas.
Procedimientos	Proporcionar detalles sobre cómo cumplir con las políticas y estándares.
Pautas, línea guía.	Proporcionar información general sobre asuntos tales como ¨Qué hacer en circunstancias particulares¨.

COBIT5 Conjunto de políticas de seguridad de la información

Tipos de políticas de seguridad

Política de control de acceso

Política de seguridad de la información del personal

Política de respuesta a incidentes de seguridad

La política de control de acceso

Proporciona un acceso adecuado a las partes interesadas internas y externas para lograr los objetivos comerciales.

Debe garantizar que el acceso de emergencia apropiadamente permitido y denegado de manera oportuna.

La política está destinada a todas las unidades de negocios, proveedores y terceras partes, y debe cubrir al menos los siguientes temas:

- Ciclo de vida de aprovisionamiento de acceso físico y lógico
- Menos privilegio / necesidad de saber
- Separación de deberes y Accesos de emergencia.

El objetivo de la política de seguridad de la información del personal, incluye, pero no se limita a las siguientes acciones:

- Verificación periódica de antecedentes de todos los empleados y personas en puestos clave.
- Adquisición de información sobre personal clave en puestos de seguridad de la información.
- Desarrollo de un plan de sucesión para todos los puestos clave de seguridad de la información.
- Definición e implementación de procedimientos apropiados para la terminación, incluidos los procedimientos para denegar los privilegios y el acceso a la cuenta.

La Política de Respuesta a incidentes de ciberseguridad

Debe responder de manera oportuna para recuperar las actividades comerciales, la cual debe incluir:

- Definiciones de incidentes de seguridad de la información.
- Declaración de cómo se manejarán los incidentes.
- Requisitos para el establecimiento del equipo de respuesta a incidentes, con roles y responsabilidades organizacionales.
- Requisitos para la creación de un plan de respuesta a incidentes probado y actualizado.

Evaluación de conocimientos adquiridos.

2.4 Controles de ciberseguridad

Controles de Ciberseguridad

- Gestión de identidad
- Autorización y restricciones de acceso
- Listas de control de acceso, Listas de acceso
- Gestión de cambio
- Gestión de usuarios privilegiados
- Gestión de la configuración
- Manejo de parches

La gestión de identidad: incluye muchos componentes, tales como:

- Directorio de Servicios
- Servicios de autenticación
- Servicios de autorización
- Capacidades de gestión de usuarios

Aprovisionamiento y des aprovisionamiento

La gestión de usuarios requiere el aprovisionamiento y des aprovisionamiento de contraseñas y derechos de control de acceso. sucede cuando un nuevo usuario es creado a través de la contratación o en función de los requisitos de trabajo cambiantes. El des aprovisionamiento ocurre cuando un usuario abandona la organización.

El proceso de autorización utilizado para **el control de acceso** requiere que el sistema sea capaz de identificar y diferenciar entre los usuarios. El acceso debe ser otorgado con el **mínimo privilegio** y puede establecerse en varios niveles, que incluyen:

- Leer, consultar o copiar solamente
- Escribir, crear, actualizar o eliminar solo o ejecutar solo
- Una combinación de lo anterior

Los mecanismos de control de acceso lógico utilizan tablas de autorización de acceso, denominadas **listas de control de acceso (LCA). Se refieren a:**

- Usuarios (incluidos grupos, máquinas, procesos) que tienen permiso para usar un recurso del sistema en particular.
- Tipos de acceso permitidos, LCA varían en su capacidad, flexibilidad, y se requiere cuidado para garantizar que el acceso del usuario sea apropiado para su función actual.

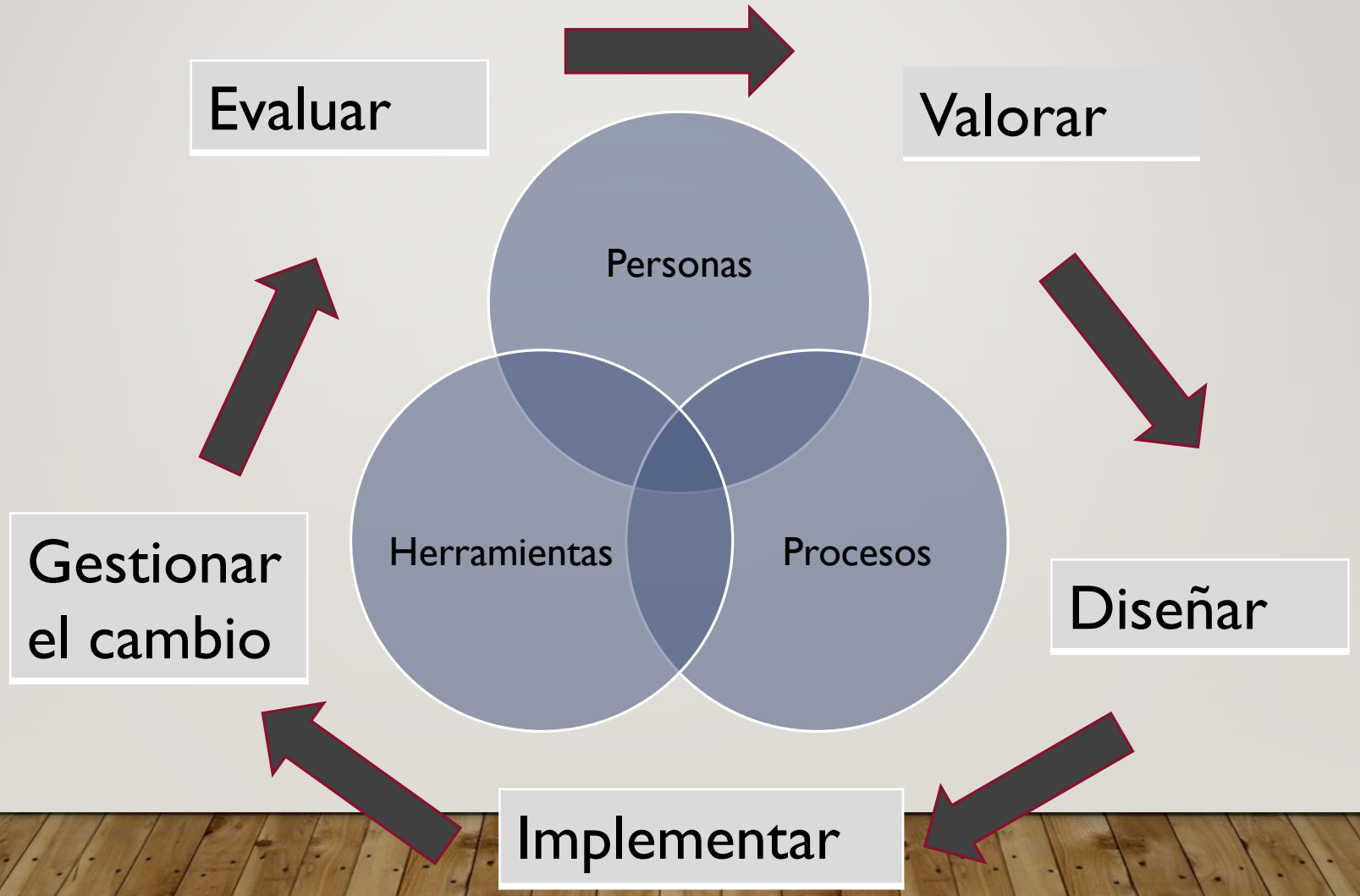
Las listas de acceso filtran el tráfico en las interfaces de red en función de criterios específicos, lo que proporciona seguridad de red básica.

Cuando las listas de acceso no están presentes, los dispositivos de red pasan todos los paquetes.

Después de crear una lista de acceso y aplicarla a una interfaz, solo pasa el tráfico permitido por las reglas.

Comprender la ubicación y el impacto de una lista de acceso es esencial para el profesional de la ciberseguridad, ya que los errores pueden detener el tráfico de la red.

Agente de cambio



Los controles comunes para la **administración de usuarios privilegiados** incluyen:

- Verificación de antecedentes para acceso elevado
- Registro de actividad adicional
- Uso de contraseñas más seguras
- Revisión regular y/o eliminación de privilegios

La gestión de la configuración, tiene como beneficios: 21/2/2021 23:43:14

- Verificación del impacto de cambios relacionados.
- Evaluación del riesgo relacionado con un cambio propuesto.
- Capacidad para inspeccionar diferentes líneas de defensa.
- Seguimiento de elementos de configuración contra líneas de base seguras aprobadas. (En busca de debilidades).
- Información sobre investigaciones después de una violación de seguridad o interrupción de operaciones
- Control de versiones y autorización de producción de componentes de hardware y software.

Los parches de software: son soluciones a errores de programación, algunos de los cuales pueden introducir vulnerabilidades de seguridad. Los proveedores de software lanzan actualizaciones y parches de software regulares a medida que se identifican y reparan vulnerabilidades.

Gestión de vulnerabilidades: es la identificación de parches necesarios para nuestra infraestructura de TI, debe probarse para asegurarse de que no afecte negativamente las operaciones.

Después de esta verificación, se pueden programar parches e instalar la actualización cuando se estime conveniente.

Evaluación de conocimientos adquiridos.