Seminario de Seguridad Informática con énfasis en hacking ético.

joseroberto.rivas@itservicesin.com

503-78876717

CLASE 003 21/Febrero/2021

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

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

2.0 CONCEPTOS DE CIBERSEGURIDAD

2.1 RIESGO

PORQUE UN ENFOQUE ORIENTADO AL RIESGO

- EVALUAR EL RIESGO ES UNA DE LAS FUNCIONES MÁS CRÍTICAS DE UNA ORGANIZACIÓN DE CIBERSEGURIDAD.
- EL USO DE UN ENFOQUE DE CIBERSEGURIDAD BASADO EN EL RIESGO PERMITE UNA TOMA DE DECISIONES INFORMADA, UNA MEJOR PROTECCIÓN Y UNA APLICACIÓN EFECTIVA DE PRESUPUESTOS Y RECURSOS.

Basado en cumplimientos

También conocido como seguridad basada en estándares, este enfoque depende del cumplimiento de reglamentos o normas para determinar las implementaciones de seguridad.

Basado en riesgos - La seguridad basada en riesgos depende de la identificación del riesgo único al que una organización en particular se enfrenta y del diseño e implementación de los controles de seguridad que son necesarios para hacer frente a ese riesgo por encima y más allá de la tolerancia al riesgo y de las necesidades de negocio de dicha organización.

Términos y definiciones claves del enfoque

Riesgo—La combinación de la probabilidad de un evento y sus consecuencias. El riesgo se mitiga a través del uso de controles.

Amenaza—Cualquier cosa que sea capaz de actuar contra un activo de una manera que pueda dañarlo. Es una posible causa de un incidente.

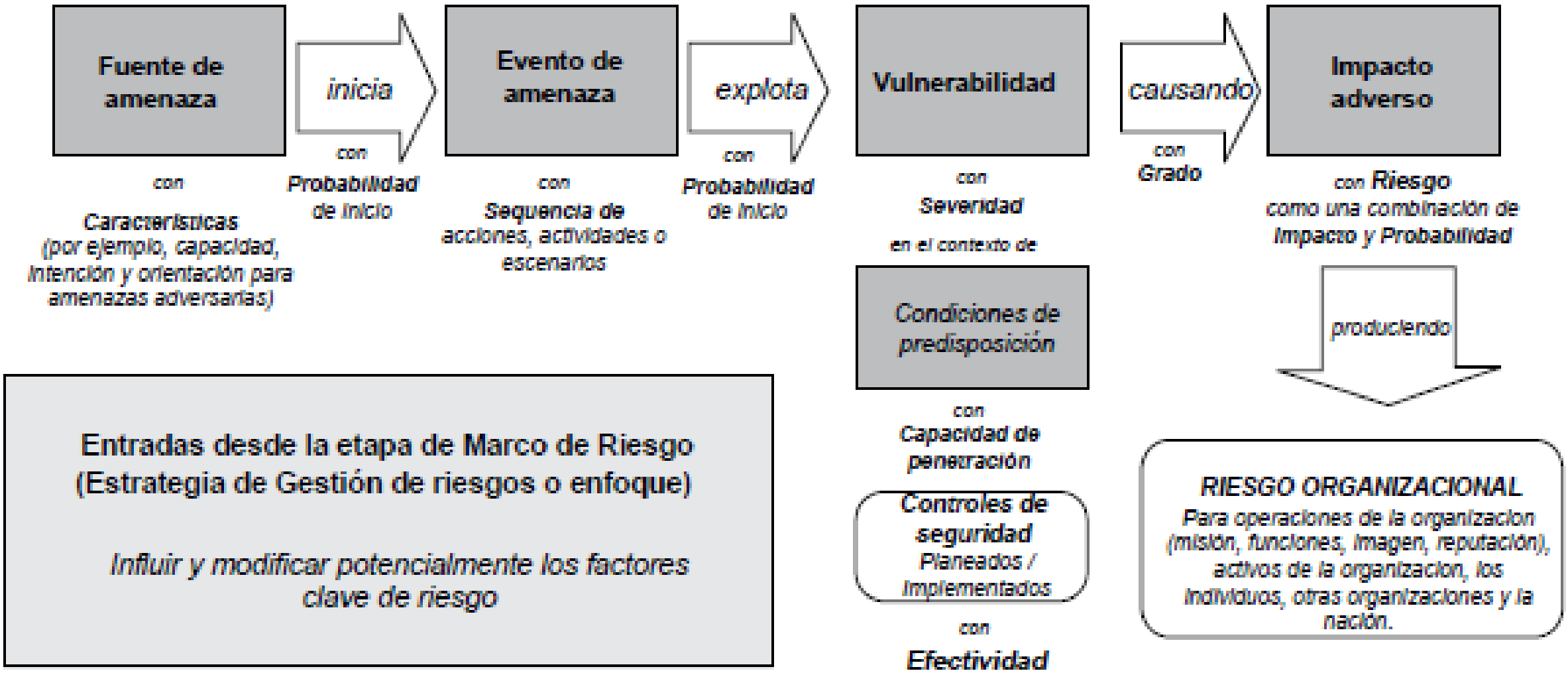
Activos—Bien de valor tangible o intangible que vale la pena proteger, incluyendo a las personas, la información, la infraestructura, las finanzas y la reputación.

Vulnerabilidad—Debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer el sistema a amenazas adversas.

Riesgo inherente—Nivel de riesgo o exposición sin tener en cuenta las acciones que la dirección ha tomado o puede tomar (por ejemplo, la implementación de los controles).

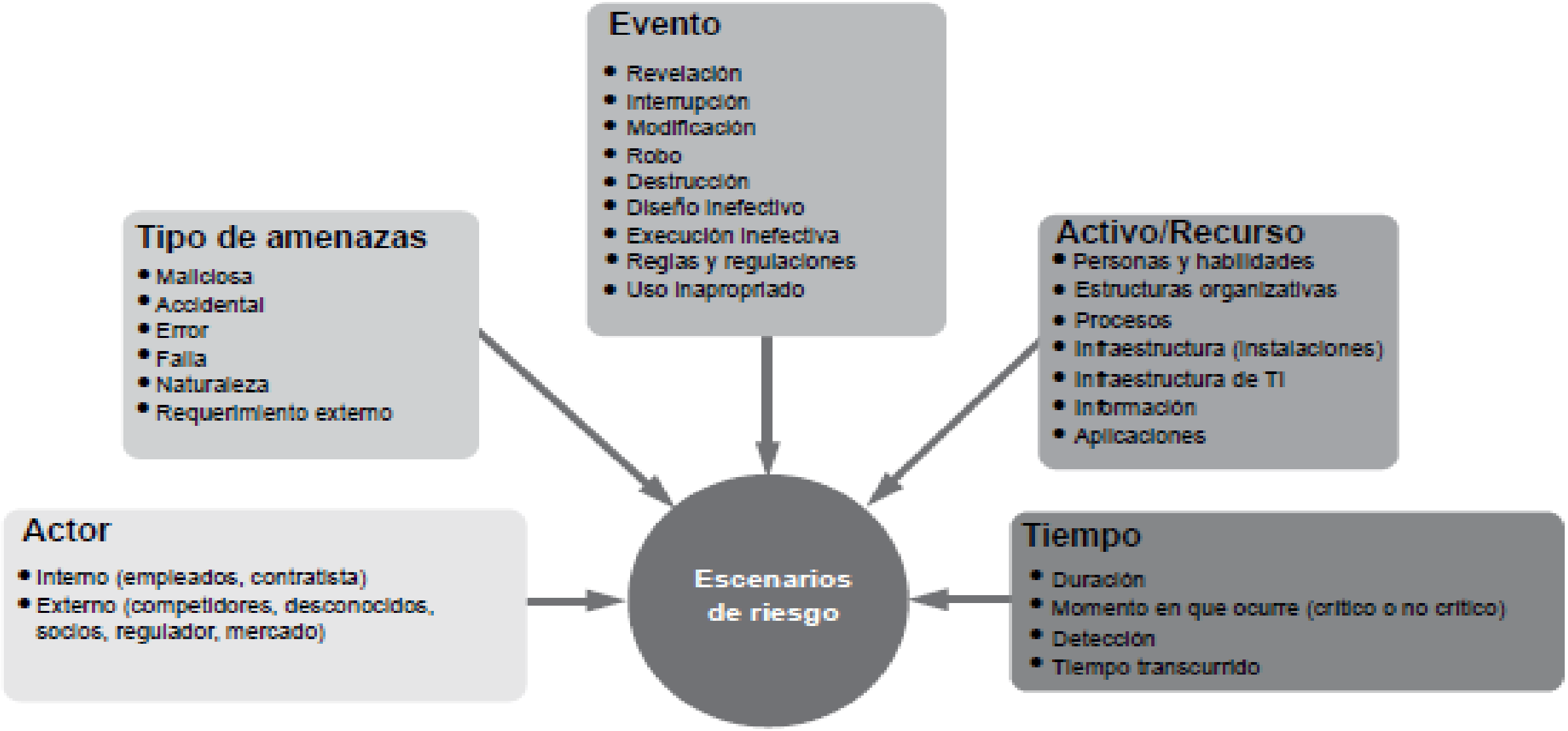
Riesgo residual—Incluso después de que los controles hayan sido adoptados, siempre habrá un riesgo residual, que se define como el riesgo que permanece después de que la dirección haya implementado una respuesta al riesgo.

Figura 2.2—Estructurando la Gestión de riesgos



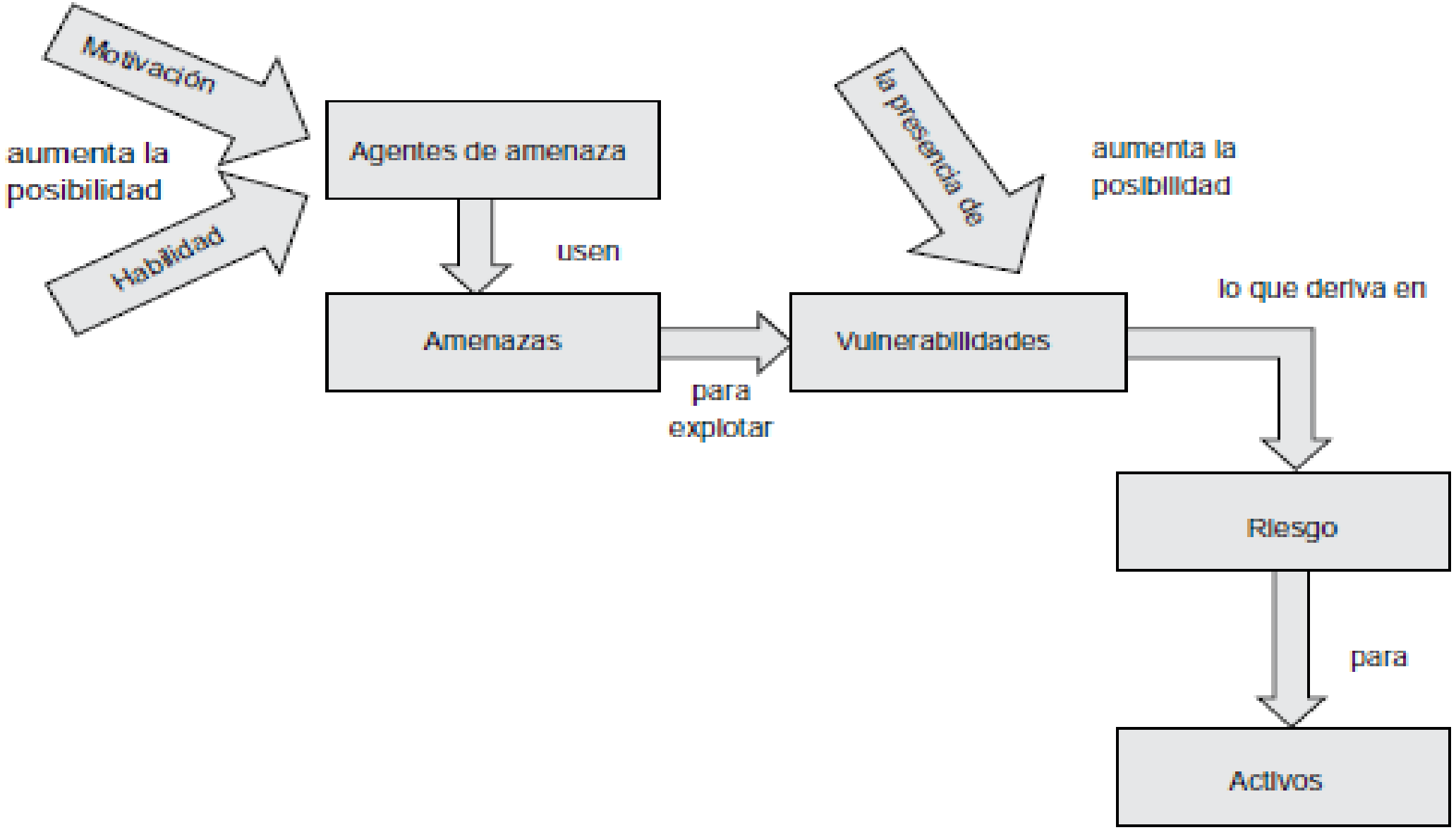
Fuente: Instituto Nacional de Normas y Tecnología, "Generic Risk Model with Key Risk Factors," NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, EE.UU., Sept 2012

Figura 2.3—Estructura de escenario del riesgo



Fuente: ISACA, *COBIT 5 para Riesgos*, EE.UU., 2013, figura 36

Figura 2.4—Factores de riesgo influyentes



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

Riesgos de Terceros (1) (Intercambio)

El control puede ser más difícil cuando hay terceros involucrados, especialmente cuando diferentes entidades tienen diferentes culturas de seguridad y diferentes tolerancias al riesgo. Existen riesgos de terceros, tales como el intercambio de información y el acceso a la red.

Riesgos de Terceros (2) (Outsourcing)

La externalización es común tanto a nivel nacional como internacional, ya que las compañías se concentran en sus competencias fundamentales y en formas de recortar gastos. Desde el punto de vista de seguridad de la información, estos acuerdos pueden presentar riesgos que pueden ser difíciles de cuantificar y potencialmente difíciles de mitigar. Porque no se encuentran dentro del control de la organización.

Riesgos de Terceros (3) (Fusiones)

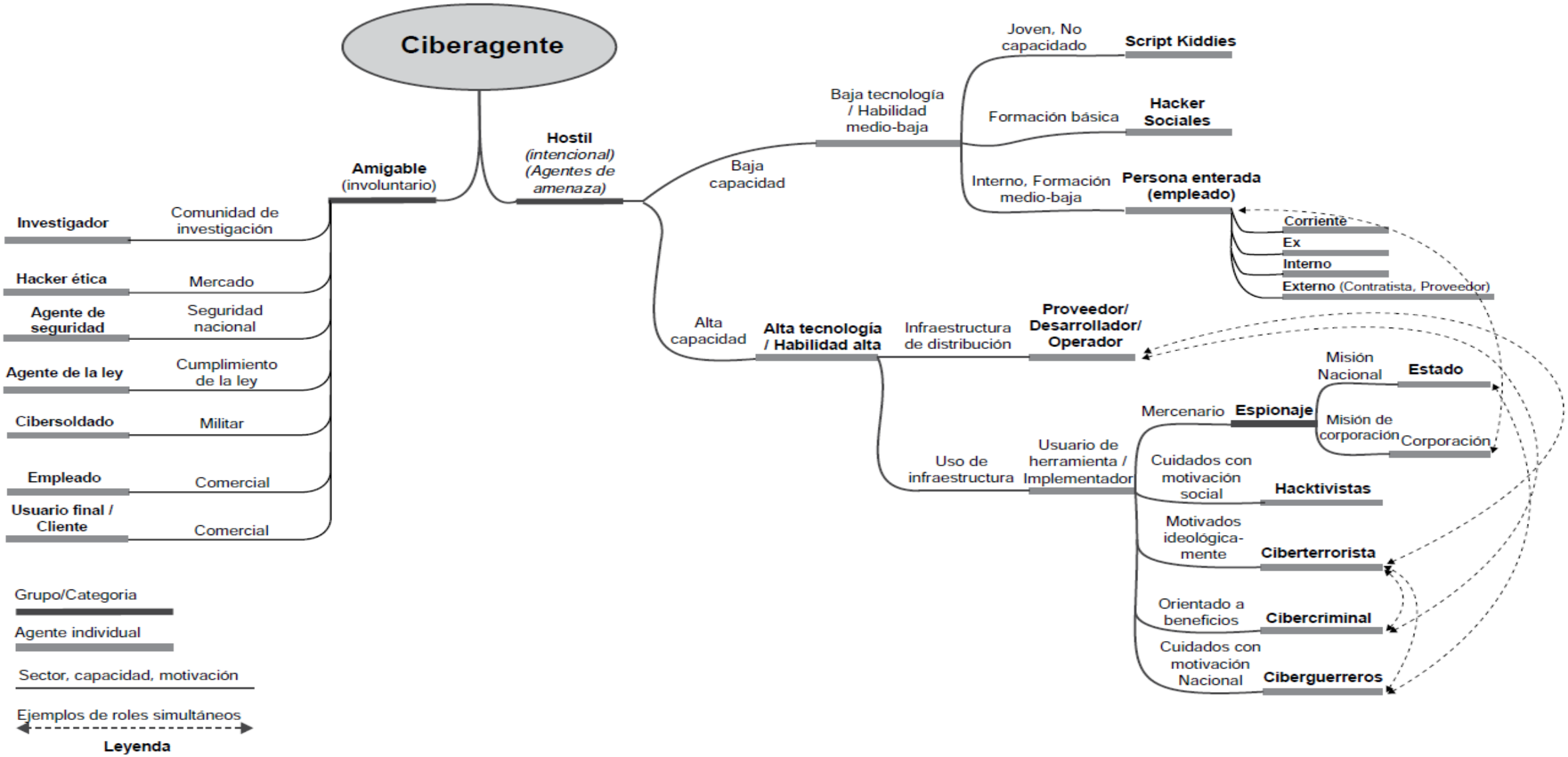
Fusiones y Adquisiciones - Normalmente, las diferencias significativas en la cultura, los sistemas, la tecnología y las operaciones entre las partes presentan numerosos retos de seguridad que deben identificarse y abordarse, se deben evaluar los riesgos para que sean tenidos en cuenta por la gerencia de seguridad.

Evaluación de conocimientos adquiridos.

2.2 TIPOS Y VECTORES DE ATAQUES COMUNES

Figura 2.5— Agentes de amenaza de ciberseguridad

14/2/2021 16:10:53



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

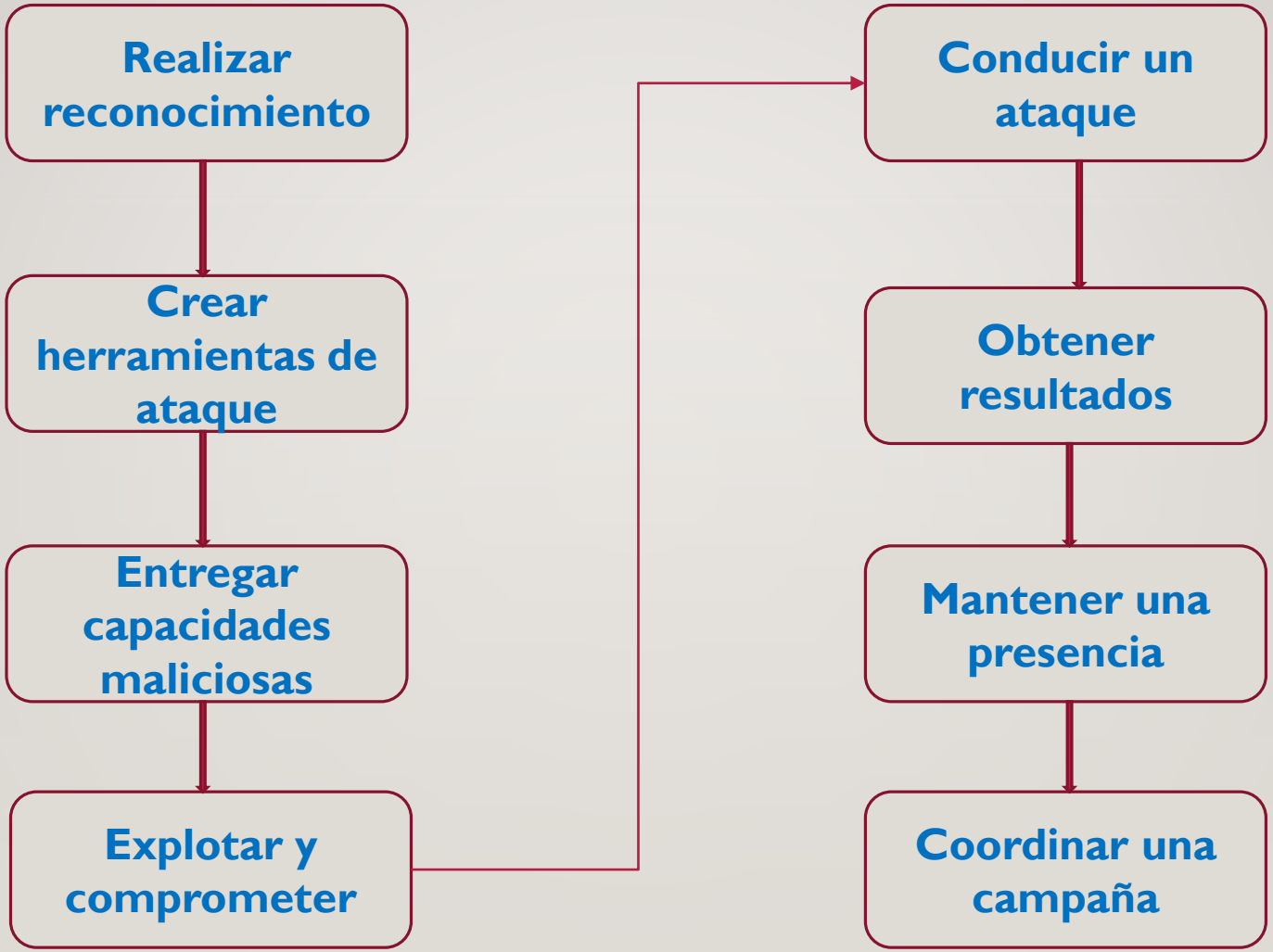
ATRIBUTOS DE ATAQUE

Un ataque es una actividad de un agente de amenaza, en contra de un activo.

Existen dos tipos de vectores de ataque: entrada y salida.

- Los ataques de entrada se centran en la intrusión y la piratería de sistemas.
- Los ataques de salida están diseñados para eliminar sistemas de datos y redes.

Proceso de Amenaza



Amenazas, que no son el resultado de actividad adversa.

- Mal uso de información critica o sensible de usuarios autorizados.
- Incorrecta configuración de privilegios.
- Incendio, inundación, huracán, tormenta de viento o terremoto en instalaciones primarias o de respaldo.
- Introducción de vulnerabilidades en productos de software.
- Errores de disco generalizados u otros problemas causados por el envejecimiento del equipo.

Tipos de Malware y ataques

14/2/2021 16:10:53

- Virus
- Gusano
- Caballo de troya
- Botnet
- Spyware
- Adware
- Secuestro de datos
- Keylogger
- Rootkit
- APT
- Puerta trasera
- Fuerza bruta
- Desbordamiento de búfer
- XSS
- DoS
- Hombre en el medio
- Ingeniería social
- Suplantación de identidad
- Spoofing
- Inyección SQL
- Explotación de día cero

KAPTOXA, es un tipo de malware de raspado de memoria, se usó en varias violaciones de seguridad de datos minoristas en 2013, incluido el ataque que comprometió los datos de pago de hasta 70 millones de clientes que compraron en Target, el segundo más grande minorista de descuento en los Estados Unidos. Kaptoxa, que es la jerga rusa para "papa", también ha sido apodado el "malware de papa".

Las políticas de seguridad de la información: son un elemento principal de ciberseguridad y en general del gobierno de la seguridad, las cuales deben:

- Especificar requerimientos.
- Definir los roles y responsabilidades dentro de la organización
- Establecer los comportamientos esperados en diversas situaciones.

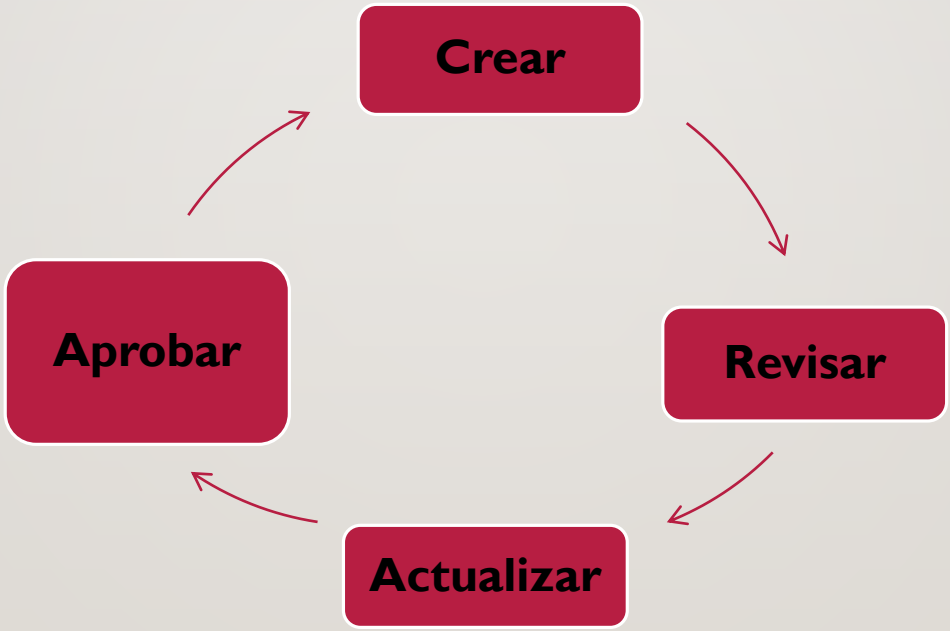
Debido a su importancia, estas políticas deben ser creadas, aceptadas y validadas por la alta gerencia antes de ser comunicadas en toda la organización.

Evaluación de conocimientos adquiridos.

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

14/2/2021 16:10:53

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

14/2/2021 16:10:53

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.

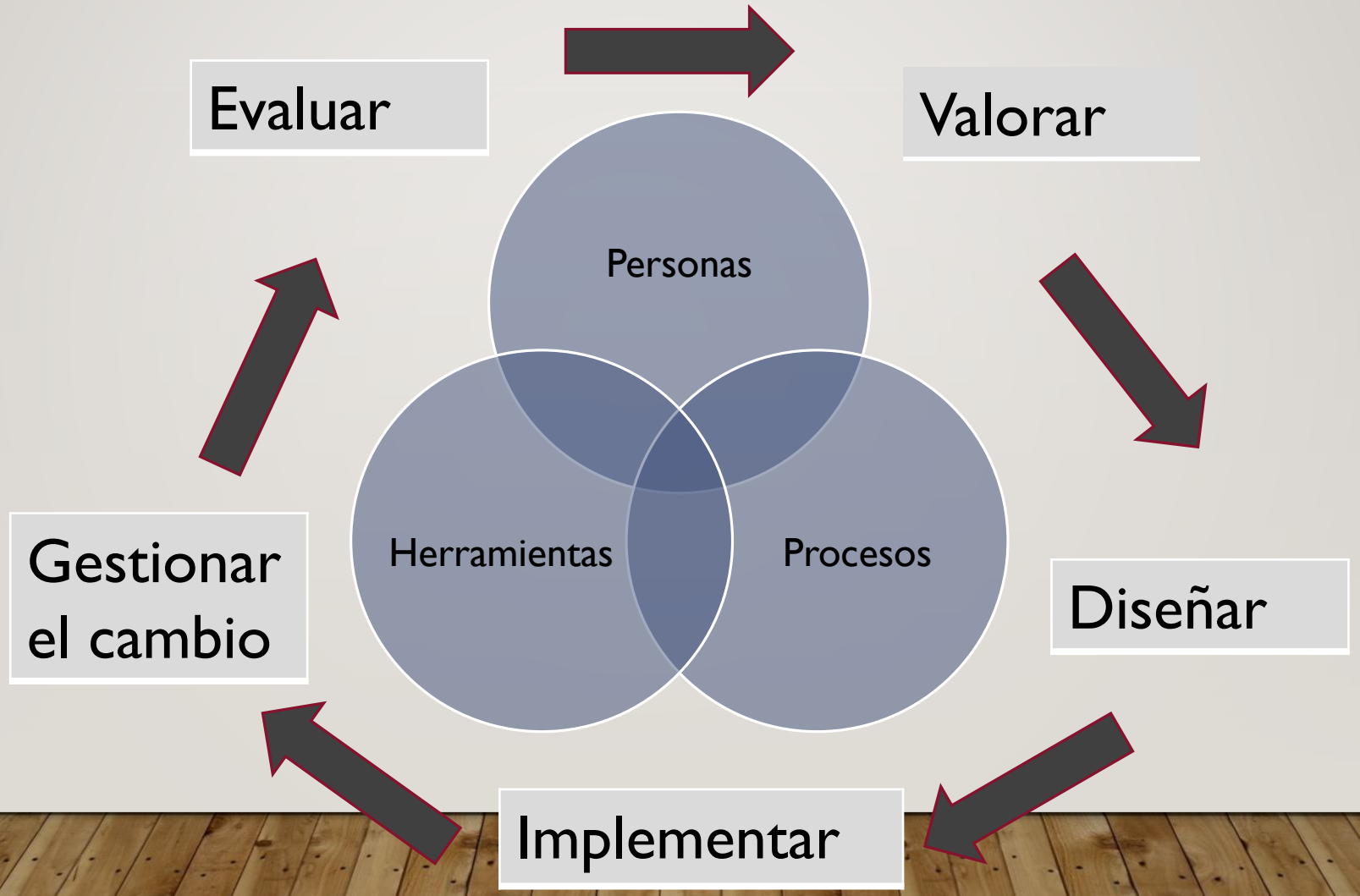
Las listas de acceso filtran el tráfico en las interfaces de red en función de criterios específicos, lo que proporciona seguridad de red básica.

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: 14/2/2021 16:10:53

- 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.