DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Introducción – Vulnerabilidad, Amenaza, Riesgo y exposición

Fundamentos de ciberseguridad

Profesor
Juan Ignacio Iturbe A.

Objetivos de aprendizaje

- OA1: Explicar y definir los conceptos relacionados con ciberseguridad.
- OA2: Diferenciar aquellos conceptos que habitualmente se utilizan como sinónimos
- OA3: Relacionar los conceptos entre ellos.

Definiciones

¿Qué significa vulnerabilidad, amenaza, riesgo y exposición?

Definiciones de Seguridad

- Las palabras *vulnerabilidad, amenaza, riesgo y exposición* se utilizan generalmente como sinónimos, pero cada una tiene su propio significado y relación entre ellas.

Definiciones de Seguridad

- Vulnerabilidad:
  - Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
  - Esta puede ser un software, hardware, procedimiento o debilidad humana que puede ser explotada.

Ejemplos:

- Un servicio corriendo en un servidor
- Aplicaciones o sistemas operativos sin parches
- Un Access Point (AP) inalámbrico sin restricciones
- Un puerto abierto en un firewall
- Seguridad física relajada, que permite a cualquiera entrar en la sala de servidores

Definiciones de Seguridad

- Amenaza:
  - Según ISO 27032 (2015) es “Causa potencial de un incidente no deseado, que puede resultar en un perjuicio a un sistema, individuo u organización”

    - Por ejemplo:
      - Fuego, Daños por agua, Desastres naturales
      - Fuga de información, Alteración de la información, Destrucción de la información, Corrupción de la información, Interceptación de la información (escucha)
      - Corte de suministro eléctrico, condiciones inadecuadas de temperatura o humedad, fallo de servicio de comunicaciones, interrupción de otros servicios y suministros esenciales.
      - Degradación de los soportes de almacenamiento de la información, difusión de software dañino, errores de mantenimiento (software, hardware), pérdidas de equipos, indisponibilidad del personal, abuso de privilegios de acceso, acceso no autorizado.
      - Errores de usuarios, administrador o configuración
      - Denegación de servicio, robo, extorción, ingeniería social.

Definiciones de Seguridad

- La entidad que toma ventaja de una vulnerabilidad es referida como un **agente de amenaza**.

Ejemplos:

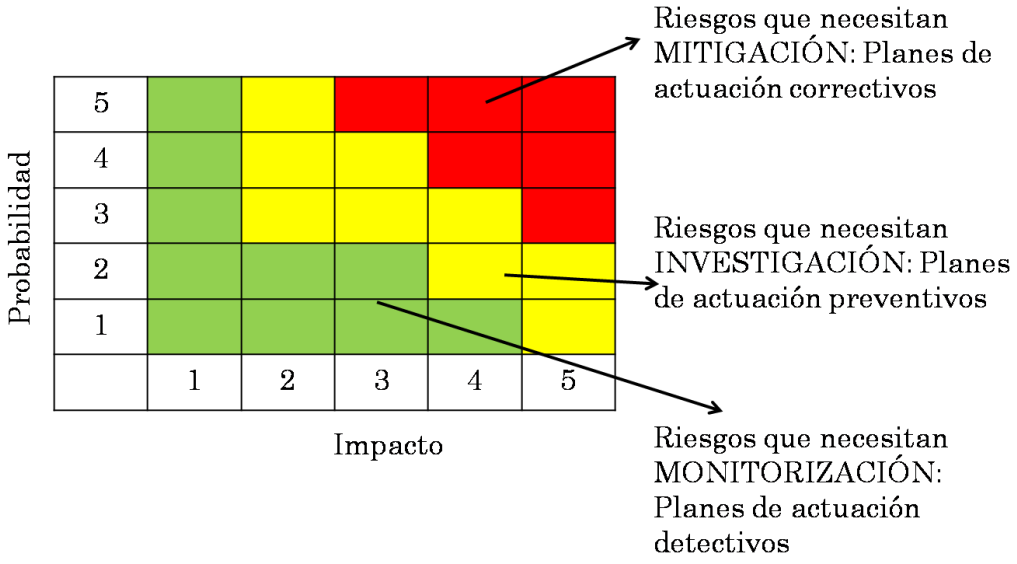
- Un intruso accediendo a la red a través de un puerto del firewall
- Un proceso accediendo a datos en una forma que viola la política de seguridad.
- Un maremoto arrasando con una instalación
- Un empleado cometiendo errores sin intención que puede exponer información confidencial.

Definiciones de Seguridad

- Riesgo:
  - Es la *probabilidad* de que un agente de *amenaza* explote una *vulnerabilidad* y tenga el correspondiente impacto en el negocio.

Por ejemplo:

- Si un firewall tiene muchos puertos abiertos se tiene una probabilidad muy alta de riesgo de intrusión.
- Si los usuarios no son educados en los procesos y procedimientos de la empresa, hay un riesgo muy alto de que cometa un error no intencional que pueda destruir datos.
- Si un IDS no es implementado en la red, hay una probabilidad muy alta que un ataque pase desapercibido hasta que sea demasiado tarde.



Definiciones de Seguridad

- Exposición:
  - Es una instancia de estar expuesto a perdidas
  - Una vulnerabilidad expone a una organización a posibles daños.

- Por ejemplo:
  - Si la administración de password es relajada y las reglas de creación de password no están reforzadas
    - la compañía esta expuesta a la posibilidad de tener password de usuarios capturadas.
    - estas pueden ser usadas de una manera no autorizada.
  - si una empresa no tiene su cableado eléctrico inspeccionado y no tiene medidas proactivas de prevención de incendios.
    - la compañía esta expuesta a incendios potencialmente devastadores.

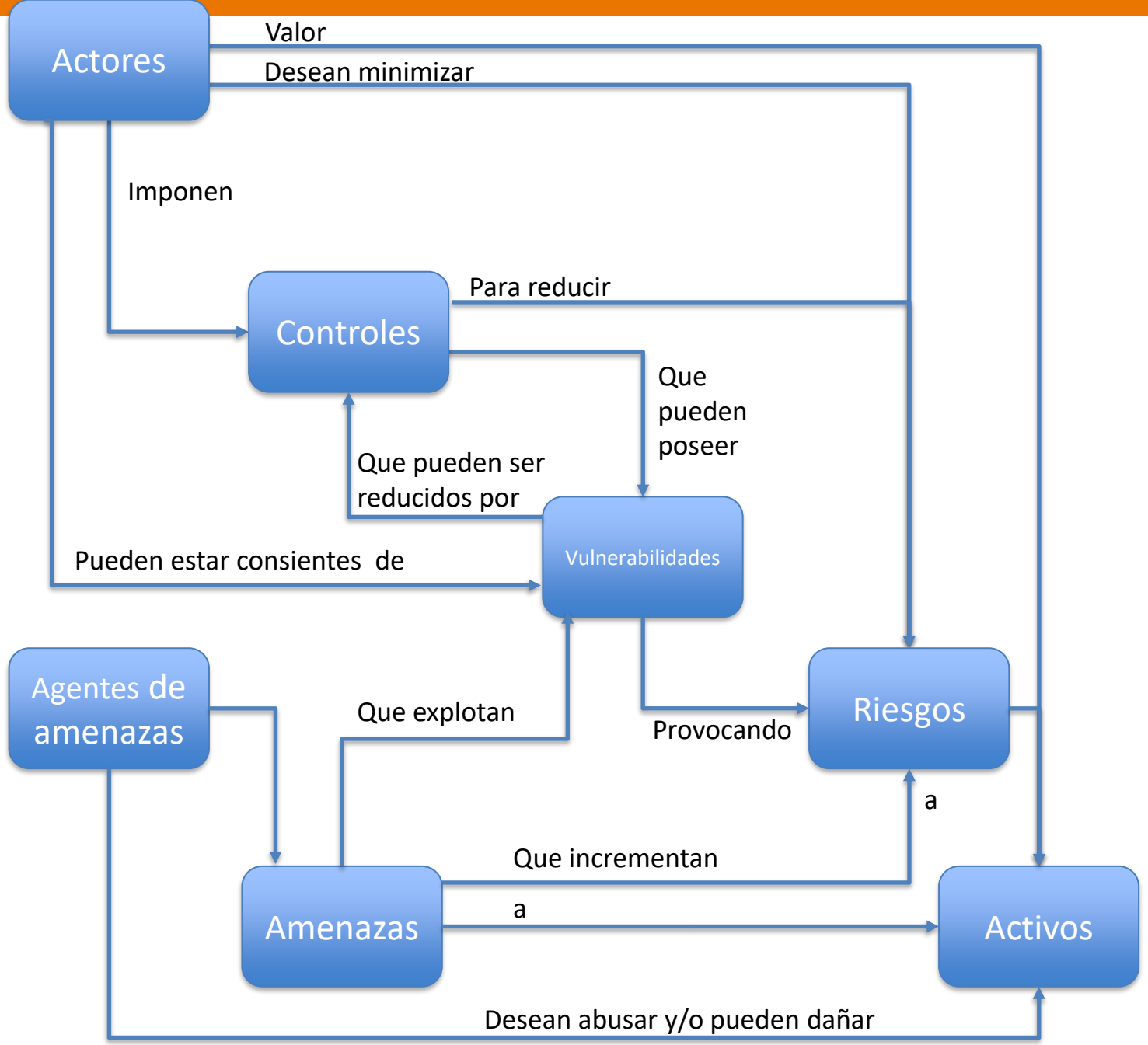
Definiciones de Seguridad

- Control:
  - O contramedida, se pone en marcha para mitigar (reducir) el riesgo potencial.
  - Esta puede ser:
    - Una configuración de software
    - Un dispositivo de hardware
    - O un procedimiento
  - Que elimina una vulnerabilidad o que reduce la probabilidad de que un agente de amenaza sea capaz de explotar la vulnerabilidad.

Relacionemos conceptos.

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Relación entre diferentes conceptos



ISO 27032 (2015) Tecnologías de la información – Técnicas de seguridad – Directrices para la Ciberprotección

Resumen

- Se explicaron y definieron algunos de los principales conceptos relacionados con ciberseguridad.
- Se diferencian aquellos conceptos que habitualmente se utilizan como sinónimos. Ej. Riesgo y amenaza
- Se relacionaron los conceptos en un mapa conceptual.

Recursos bibliográficos

- https://www.ciberseguridad.gob.cl/
- Biblioteca digital USACH – AENOR
- ISO/IEC 27K
- https://www.incibe.es/

Glosario

- **Política**: Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.
- **Objetivo de control:** Declaración que describe lo que quiere lograr como resultado de la implementación de controles.
- **Control de acceso:** Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

Glosario

- **Vector de ataque:** Camino o medios por los cuales un atacante puede obtener acceso a un servidor de computador o de red para entregar un resultado malicioso.
- **Bot:** Programa de software automatizado usado para llevar a cabo tareas específicas.
- **Botnet:** Software de control remoto, específicamente una colección de bots maliciosos, que corre de manera autónoma y automática en computadores comprometidos.

Glosario

- **Adware:** Aplicación que fuerza al usuario a ver publicidad y/o registra el comportamiento online del usuario.
- **Avatar**: Representación de una persona que participa en el Ciberespacio.
- **Ataque**: Intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada.

Glosario

- **Autenticación:** Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma.
- **Autenticidad:** Propiedad consistente en que una entidad es lo que dice ser.
- **No repudio:** Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.