DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

1.4. Introducción – Clase 4

Fundamentos de ciberseguridad

Profesor

Juan Ignacio Iturbe A.

Objetivos de aprendizaje

- OA5: Reconocer el orden adecuado en que se aplican los conceptos estudiados.
- OA6: Diferenciar los tipos de controles.
- OA7: Proteger los activos digitales a través de la defensa en profundidad.
- OA8: Definir diferentes conceptos asociados a ciberseguridad.

Orden de los conceptos

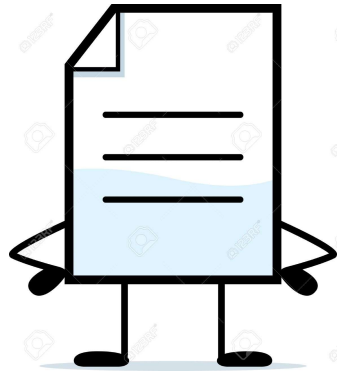
- El orden adecuado para ser aplicado a su, por ejemplo, propia red es: amenaza, exposición, vulnerabilidad, controles y al último el riesgo.
- Esto, porque:
  - puede haber una amenaza (ej. Nuevo ataque SQL)
  - pero a menos que la compañía tenga la correspondiente vulnerabilidad (Servidor SQL con la necesaria configuración)
  - La compañía no esta expuesta
  - y por lo tanto esto no es una vulnerabilidad.
  - Y si la vulnerabilidad estuviera en el ambiente, entonces un control es aplicado para reducir el riesgo.

Tipos de controles

- Los controles se ponen en marcha para reducir los riesgos de una organización.
- Estos son principalmente de tres tipos:
  - Administrativos
  - Técnicos
  - Físicos

Tipos de controles

- Controles administrativos
  - Llamados también “controles blandos”
  - Son orientados a la gestión
  - Por ejemplo:
    - Documentación de seguridad
    - Gestión del riesgo
    - Entrenamiento



Tipos de controles

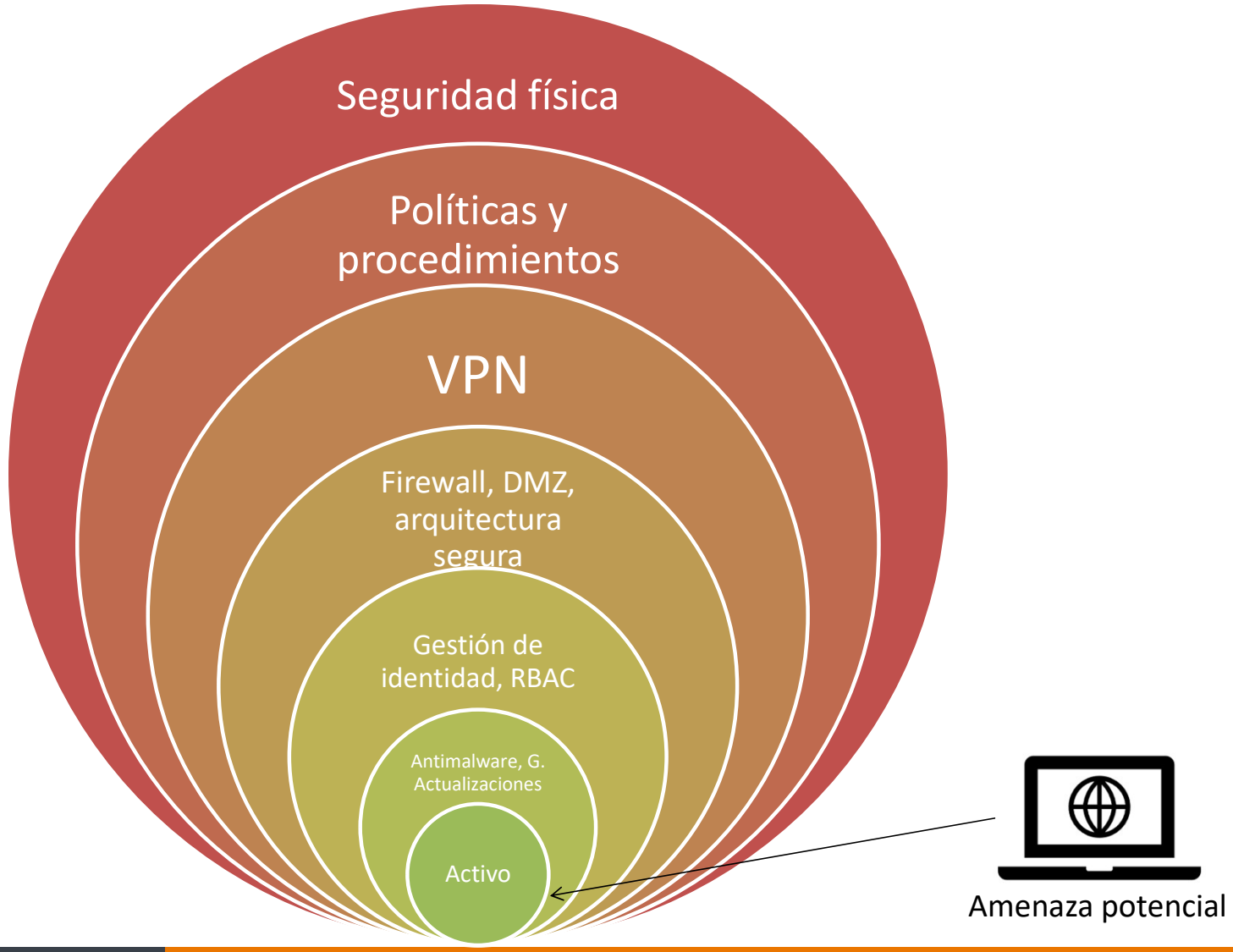
- Controles técnicos
  - También llamados “controles lógicos”
  - Son componentes de software o hardware
  - Por ejemplo:
    - Firewalls
    - IDS
    - Encriptación
    - Mecanismos de identificación y autentificación

Tipos de controles

- Controles físicos
  - Son elementos puestos en marcha para proteger las instalaciones, el personal y los recursos.
  - Ejemplos:
    - Guardia de seguridad
    - Seguros
    - Rejas
    - Iluminación

Tipos de controles

- Con estos controles se busca proveer una **defensa en profundidad.**
  - Lo cual se realiza coordinando y usando múltiples controles de seguridad.
  - Utilizando una *aproximación en capas*.
  - Este esquema minimiza la probabilidad de compromiso y penetraciones exitosas.
  - El atacante debe sortear varios tipos de diferentes mecanismos de protección antes de ganar acceso a los activos críticos de la organización.
  - El número de capas depende de la sensibilidad del activo.


Seguridad física
Políticas y procedimientos
VPN
Firewall, DMZ, arquitectura segura
Gestión de identidad, RBAC
Antimalware, G. Actualizaciones
Activo
Amenaza potencial

Tipos de control por funcionalidad

- Cada control nos ofrece diferentes funcionalidades y de acuerdo a ellas se pueden clasificar como:
  - Disuasivo
  - Preventivo
  - Correctivo
  - Recuperativo
  - Compensatorio

Tipos de control por funcionalidad

- Una vez que se entienden las diferencias entre los diferentes controles, estos serán usado para las locaciones apropiadas para riesgos específicos.
- El enfoque más productivo es un modelo preventivo y luego usar uno detectivo, luego de recuperación y finalmente correctivo.
  - Se busca parar el ataque ante que ocurra
  - Pero si no se logra prevenir, se debe ser rápido para detectar.

Mapeando funcionalidades de controles

- Ejemplo:
  - "Un Firewall es un control preventivo, pero si un hacker conoce que este está en su lugar, entonces este puede ser disuasivo".
- Cuando se trata de mapear una funcionalidad a un control, hay que pensar la principal razón por la que el control fue puesto en su lugar. Por ejm:
  - Un firewall trata de prevenir que algo malo pase. Entonces es preventivo.
  - Los logs de auditoría son utilizados después que un evento ocurra, entonces son detectivos.
  - Un sistema de respaldo de datos es desarrollado para que los datos puedan ser recuperados, entonces es recuperativo.
  - Las imágenes de disco son creadas por si el software se corrompe, entonces pueden ser cargadas nuevamente, entonces esto es un control correctivo.
- En resumen, hay que analizar el contexto para el cual se desarrolla el control.

Tipos de control

		Preventivo	Detectivo	Correctivo	Disuasivo	Recuperación
Categoría de control: Físico	Rejas				X	
	Seguro en puerta	X				
	Credenciales	X				
	Guardia	X				
	Sist. Biométrico	X				
	Luces				X	
	Detector de movimiento		X			
	CCTV		X			
	Instalación de respaldo fuera de la org.					X

Tipos de control

		Preventivo	Detectivo	Correctivo	Disuasivo	Recuperación
Categoría de control: Administrativo	Política de seguridad	X				
	Monitoreo y supervisión		X			
	Separación de funciones	X				
	Rotación de trabajo		X			
	Procedimientos de personal	X				
	Testing		X			
	Entrenamiento de concientización en seguridad	X				
	Investigaciones		X			

Tipos de control

		Preventivo	Detectivo	Correctivo	Disuasivo	Recuperación
Categoría de control: Técnico	ACLs	X				
	Encriptación	X				
	Logs de auditoria		X			
	IDS		X			
	Antivirus	X				
	Imagen de servidor			X		
	Smartcards	X				
	Respaldos de datos					X

Recordar y considerar:
- La defensa en profundidad.
- Primeramente los controles preventivo, detectivo, luego de recuperación y finalmente correctivo.

Ejercicios propuestos

- Si una empresa tiene en un servidor servicios web, ftp y ssh. Se aprecian otros puertos abiertos, sin que el administrador sepa de que se tratan.
- Son frecuentes los cambios en la página web de la empresa hechos directamente en el servidor, por lo que la clave de acceso es de conocimiento de varios empleados.
- La subred del servidor en producción se encuentra en el mismo segmento de red que la de los usuarios.
  - Identifique la vulnerabilidad, la amenaza y el riesgo.
  - ¿A que está expuesta la compañía?
  - ¿Qué contramedidas (o controles) y de qué tipo se podrían aplicar?

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.