DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Gestión de riesgos

Profesor
Juan Ignacio Iturbe A.

Fundamentos de ciberseguridad

Objetivos de aprendizaje

- OA: Evaluar y planear la ciberseguridad en las organizaciones
  - OA1: Reconocer las razones de porque la de gestión del riesgo es un elemento clave en la evaluación y planeación de la ciberseguridad.
  - OA2: Establecer los requisitos que debe tener una gestión del riesgo efectiva.
  - OA3: Identificar las características de la gestión del riesgo.

Gestión del riesgo

Riesgo es la posibilidad de que ocurra el daño y las consecuencias de los daños en caso de producirse.

La gestión del riesgo de la información (IRM) es el proceso de:

- Identificar
- Reducir a un nivel aceptable
- Implementar los debidos mecanismos para mantener ese nivel.

Gestión de riesgo

No existe el ambiente 100% seguro.

Cada ambiente tiene vulnerabilidades y amenazas.

Se requiere la habilidad de:

Identificar estas amenazas

Evaluar la probabilidad de que ellas ocurran

Evaluar el daño que puedan causar

Identificar el nivel de riesgo aceptable para la organización

Seleccionar los pasos necesarios para reducir y llegar al nivel de riesgo aceptable

Gestión de riesgos

Si se tiene un presupuesto para seguridad de $60 Millones (CLP) y una larga lista de vulnerabilidades

¿Cuál enfrentar primero?

¿Cómo priorizo las vulnerabilidad más críticas?

¿Cómo asegurar que la compañía esta manejando los riesgos más críticos y como obtengo un mayor retorno de la inversión (ROI)?

Esto trata la gestión de riesgos

$$ROI = \frac{(Retorno\ de\ la\ inversión - Invers\ ón\ inicial)}{Inversión\ inicial} * 100\%$$

Política de gestión del riesgo de la información

La gestión del riesgo requiere:

Un fuerte compromiso de la alta dirección.	Un proceso documentado que soporte la misión de la organización	La política de la gestión del riesgo de la información (IRM)	Y un equipo delegado a IRM

La política IRM debe ser un subconjunto de la política general de gestión del riesgo.

Equipo de gestión del riesgo

Cada organización es diferente en tamaño, postura de seguridad, perfil de amenazas y presupuesto de seguridad.

La composición del equipo podría ir desde uno a mas integrantes.

El objetivo del equipo es asegurar que la compañía es protegida con la mejor relación costo-efectividad

Análisis y evaluación de riesgo

Una vez que se tiene el equipo y la política, es hora del análisis.

Un análisis de riesgo tiene los siguientes objetivos:

Identificar activos y su valor para la organización	Identificar vulnerabilidades y amenazas	Cuantificar la probabilidad e impacto para el negocio de estas potenciales amenazas	Proveer un balance económico entre el impacto de las amenazas y el costo de la contramedida.

Análisis y evaluación de riesgo

Un análisis de riesgo provee una comparación de costo/beneficio.

Compara el costo anualizado de los controles frente al costo potencial de la perdida.

En la mayoría de los casos, un control no debe ser implementado si:

El costo anualizado de la perdida, excede el costo anualizado del control. Por ejm:

- Si las instalaciones cuestan $50 Millones, no tiene sentido implementar un control de $75 Millones.

Análisis y evaluación de riesgo

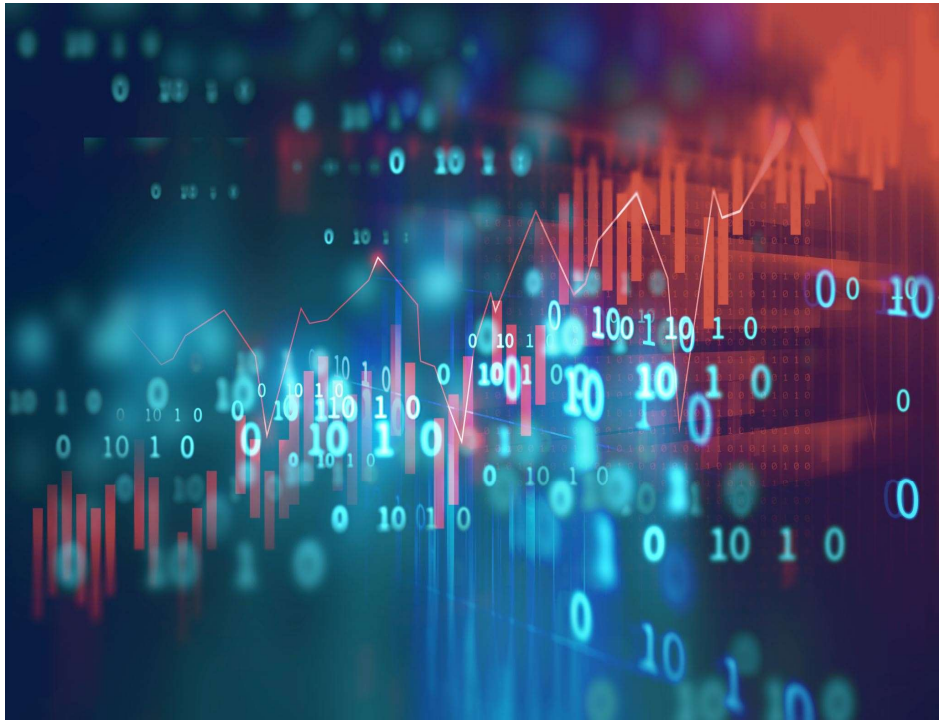
Antes de analizar y estimar los riesgos, se debe **definir el alcance**, para entender donde deben ser evaluados los activos y amenazas.

Tratar de evaluar todos los activos puede llevar mucho tiempo.

El equipo de **análisis de riesgos** debe crear un reporte que detalle los activos y entregárselo a la alta gerencia, quien debe revisar y aceptar la lista.

El valor de la información y de los activos

- El valor puesto en la información es relativo a las partes relacionadas:
  - El trabajo requerido para desarrollarla
  - Cuanto cuesta mantenerla
  - Cual es el daño que puede causar su destrucción o perdida
  - Cuanto pagaría por ella una compañía enemiga
  - Y penalidades legales pueden ser aplicadas



Identificando vulnerabilidades y amenazas

Riesgo es la probabilidad de que un agente de amenaza explote una vulnerabilidad que causa daño a un activo, resultando en un impacto en el negocio.

A continuación algunos ejemplos.

Agente de amenaza	Puede explotar esta vulnerabilidad	Resultando en esta amenaza
Malware	Debilidad software antivirus	Infección de virus
Hacker	Servicios potentes corriendo en un servidor	Acceso no autorizado a información confidencial
Usuario	Parámetros no configurados en el sistema operativo	Malfuncionamiento del sistema
Fuego	Debilidad en los extintores	Daño en las instalaciones y computadores y posible perdida de vidas.
Empleado	Pobre Entrenamiento o aplicación de los estándares	Compartición de información crítica Alteración de entrada/salida de datos por aplicaciones de procesamiento de datos
Contratista	Mecanismos de control de acceso relajados	Robo de secretos comerciales
Atacante	Aplicaciones escritas pobremente. Falta de ajustes en el firewall	Conducente a un buffer overflow Conducente a un ataque DoS
Intruso	Falta de guardia de seguridad	Quebradura de vidrios y robo de computadores y dispositivos

Identificando vulnerabilidades y amenazas

- Una vez que las vulnerabilidades y sus amenazas asociadas son identificadas, sus ramificaciones deben ser investigadas.
- El riesgo tiene una pérdida potencial y una pérdida tardía

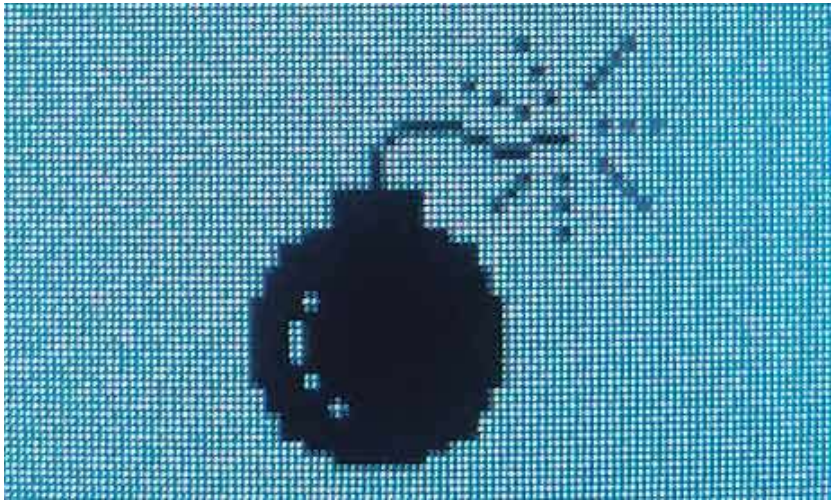
- El riesgo tiene una pérdida potencial
  - Es lo que una compañía puede perder si un agente de amenaza actualmente explota una vulnerabilidad.
  - Por ejem: Corrupción de datos, destrucción de sistemas y/o instalaciones, divulgación de información confidencial, reducción en productividad de los empleados, etc.

- El riesgo también tiene una pérdida tardía:
  - Toma lugar después de que la vulnerabilidad fue explotada.
  - Por ejem: Daño a la reputación de la compañía, perdida de mercado, penalizaciones por retrasos, demandas, etc.

Ejercicio

- El sitio web de comercio electrónico es atacado y puesto en offline.
  - ¿Cuál es la perdida potencial y tardía?

•Corrupción de datos
•HH necesarias para subir los servidores (online)
•Reemplazo de componentes o código
•Si se demora un día completo en arreglar el servidor y colocarlo online, la compañía puede perder un montón de ventas y beneficios.
•Si toma una semana, puede perder ventas y beneficios y no tener los recursos para pagar otras cuentas y gastos.
•Si la compañía pierde confianza en lo que es su actividad, esta puede perder negocios, por meses y años.



FIN

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Gestión del riesgo: Metodologías

Profesor
Juan Ignacio Iturbe A.

Fundamentos de ciberseguridad

Hasta el momento…

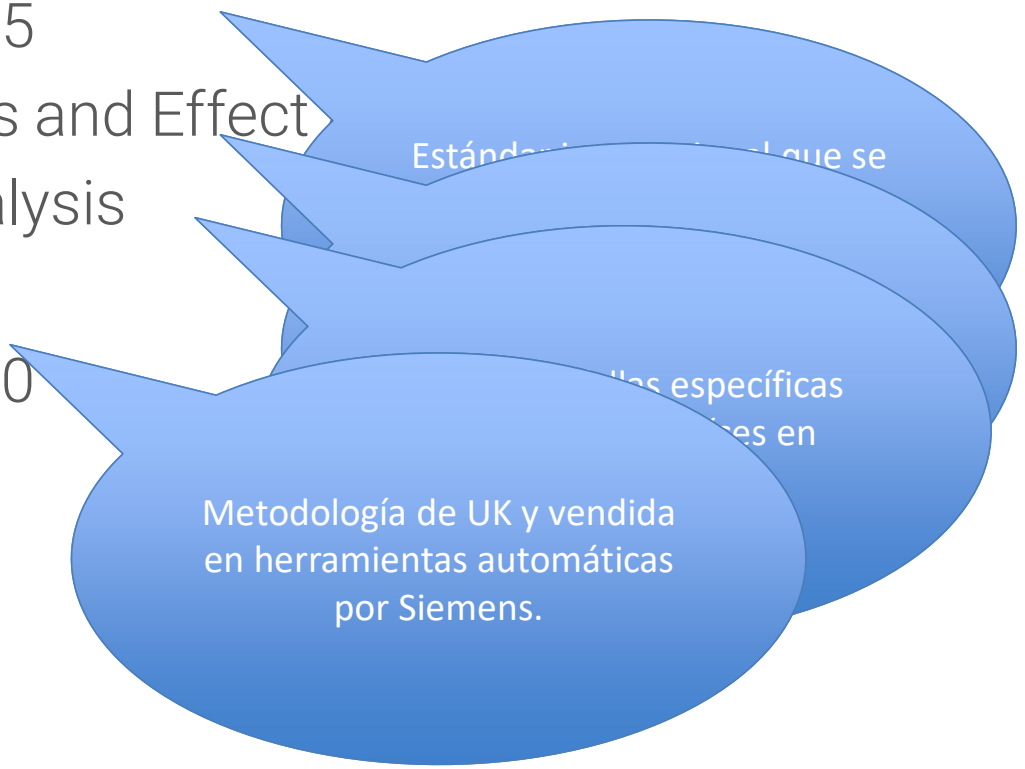
- Se ha:
  - Identificado los activos que serán evaluados
  - Asociado un valor a cada activo
  - Identificado las vulnerabilidades y amenazas que pueden afectar a cada activo

Metodologías de evaluación de riesgos

- La industria tiene diferentes metodologías estandarizadas para llevar a cabo el evaluación de riesgos. Cada una con un foco diferente.
  - NIST 800-30 Risk Management [illegible]n Technology
  - Facilitated Risk Analysis Process [illegible]
  - Operationally Critical Threat [illegible]uation (OCTAVE)
  - AS/NZS 4360

Metodologías de evaluación de riesgos

- ISO/IEC 27005
- Failure Modes and Effect
- Fault tree analysis
- CRAMM
- ISO/IEC 31000



Proceso de gestión del riesgo según la ISO 31.000

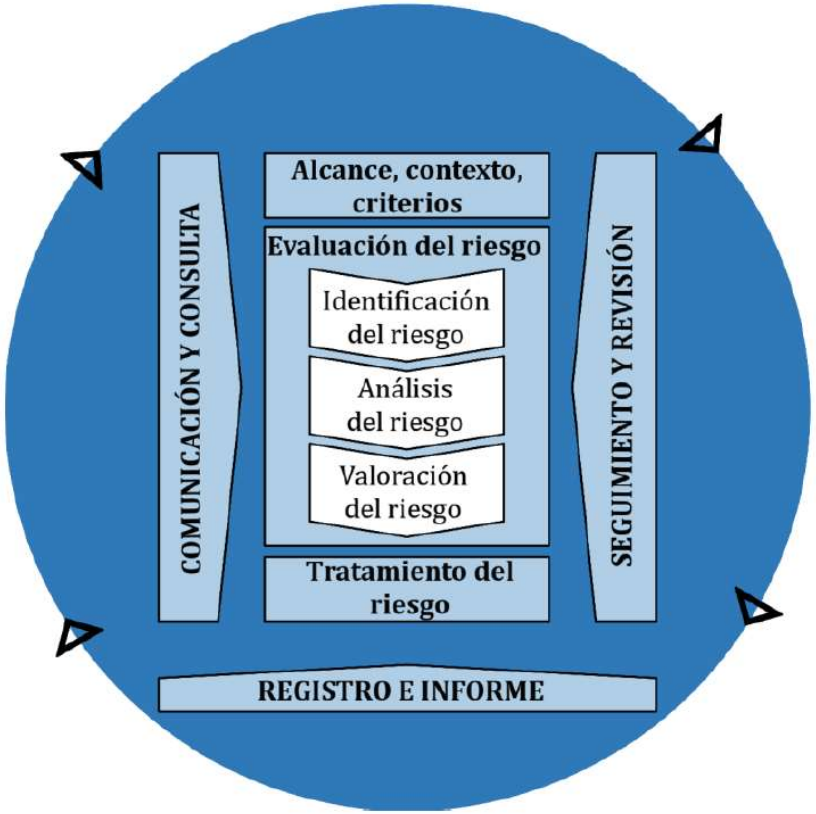


Figura 4 – Proceso

Tabla A.1 – Aplicabilidad de las herramientas utilizadas para la apreciación del riesgo

Herramientas y técnicas	Proceso de apreciación del riesgo					Véase el capítulo
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas	MA[1)]	NA[2)]	NA	NA	NA	B 01
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA	B 02
Delphi	MA	NA	NA	NA	NA	B 03
Listas de verificación	MA	NA	NA	NA	NA	B 04
Análisis preliminar de peligros	MA	NA	NA	NA	NA	B 05
Estudios de peligros y de operatividad (HAZOP)	MA	MA	A[3)]	A	A	B 06
Análisis de peligros y puntos de control críticos (HACCP)	MA	MA	NA	NA	MA	B 07
Apreciación de riesgos ambientales	MA	MA	MA	MA	MA	B 08
Estructura «y si….» (SWIFT)	MA	MA	MA	MA	MA	B 09
Análisis de escenario	MA	MA	A	A	A	B 10
Análisis del impacto económico	A	MA	A	A	A	B 11
Análisis de la causa primordial	NA	MA	MA	MA	MA	B 12
Análisis de los modos de fallo y de los efectos	MA	MA	MA	MA	MA	B 13
Análisis del árbol de fallos	A	NA	MA	A	A	B 14
Análisis del árbol de sucesos	A	MA	A	A	NA	B 15
Análisis de causa-consecuencia	A	MA	MA	A	A	B 16
Análisis de causa-y-efecto	MA	MA	NA	NA	NA	B 17
Análisis de capas de protección (LOPA)	A	MA	A	A	NA	B 18
Diagrama de decisiones	NA	MA	MA	A	A	B 19
Análisis de fiabilidad humana	MA	MA	MA	MA	A	B 20
Análisis de pajarita	NA	A	MA	MA	A	B 21
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA	B 22
Análisis del circuito de fuga	A	NA	NA	NA	NA	B 23
Análisis Markov	A	MA	NA	NA	NA	B 24
Simulación Monte-Carlo	NA	NA	NA	NA	MA	B 25
Estadísticas Bayesian y redes Bayes	NA	MA	NA	NA	MA	B 26
Curvas FN	A	MA	MA	A	MA	B 27
Índices de riesgo	A	MA	MA	A	MA	B 28
Matriz de consecuencia/probabilidad	MA	MA	MA	MA	A	B 29
Análisis de costes/beneficios	A	MA	A	A	A	B 30
Análisis de decisión multi-criterios (MCDA)	A	MA	A	MA	A	B 31

1) Muy aplicable.
2) No aplicable.
3) Aplicable.

ISO 31010

Etapas del análisis de riesgos según NIST SP 800-30

Enfoques de análisis de riesgos

- Existen dos enfoques para el análisis de riesgos:
  - Cuantitativo: Usado para asignar valores numéricos y monetarios todos los elementos del análisis de riesgo. Ej:
    - El riesgo de perder $50.000.000 si un buffer overflow es explotado en un webserver, $10.000.000 si una BD o $5.000.000 si un servidor de archivos.
  - Cualitativo: Enfoque mas “blando”, no asigna valores numéricos, asigna clasificación a los riesgos. Ej:
    - A través de una encuesta se definen niveles de riesgos (rojo es el mas alto y verde es el mas bajo).

Cuantitativo vs Cualitativo

Atributo	Cuantitativo	Cualitativo
No requiere cálculos		X
Requiere cálculo complejos	X	
Requiere un alto grado de supuestos		X
Proporciona áreas generales e indicaciones de riesgos		X
Es fácil para automatizar y evaluar	X	
Usado para el seguimiento de la performance del manejo de riesgo	X	
Permite un análisis costo/beneficio	X	
Usa métricas verificables y objetivas	X	
Provee opiniones de los individuos que mejor conocen los procesos		X
Muestra las perdidas que pueden ser producidas en un año	X	

Riesgo total vs Riesgo residual

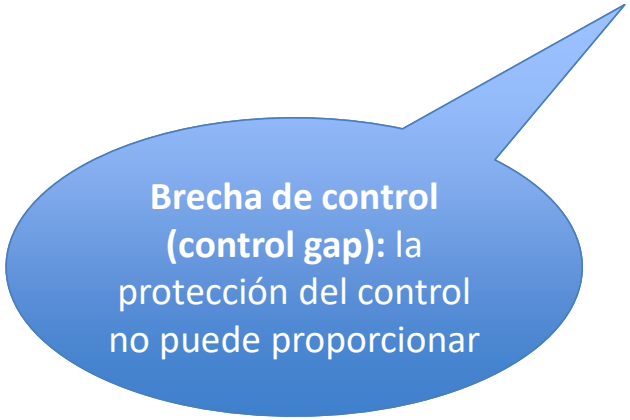
- La razón de una compañía para que implemente control es reducir el **riesgo total** a un nivel aceptable.
- Ningún sistema es 100% seguro
- Lo que significa que siempre algún riesgo queda y hay que lidiar con el. Este se llama **riesgo residual**.

Riesgo total vs Riesgo residual

- El riesgo residual es diferente al riesgo total.
- El riesgo total es el riesgo que una compañía enfrenta cuando elige no implementar ningún tipo de control
- Una compañía puede elegir esto último si el análisis costo beneficio, indica que es la mejor opción.

Riesgo total vs Riesgo residual

- A continuación las formulas conceptuales:
  - Amenazas x Vulnerabilidad x Valor activo = Riesgo total
  - Riesgo total x brecha de control = riesgo residual
  - Riesgo total – controles = riesgo residual

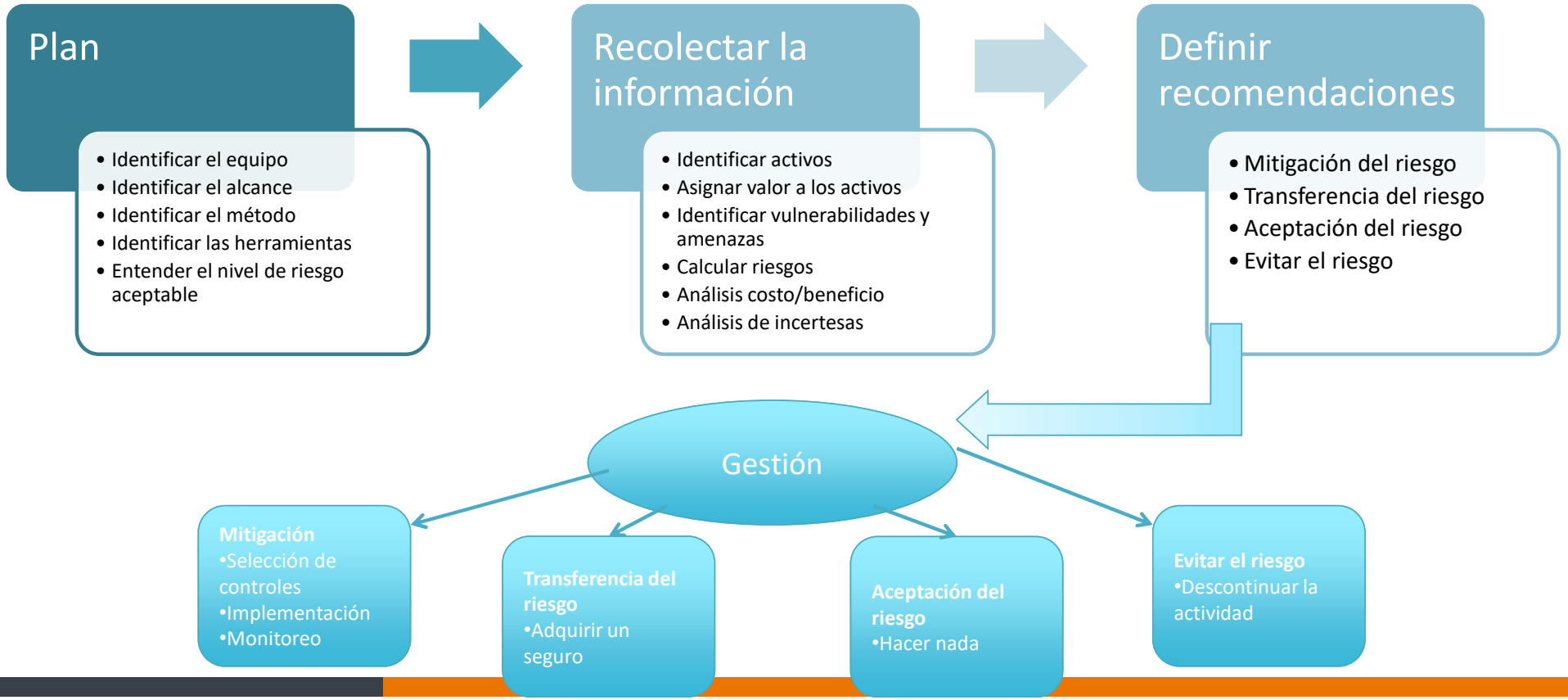


Nota: estas formulas son solamente para ilustrar las relaciones entre los conceptos. No son para incluir números en ellas.

Manejo de riesgo

- Una vez que se conoce el riesgo total y residual, se debe decidir que hacer con este:
  - Transferirlo (ej. A una compañía de seguros)
  - Evitarlo (ej. Bloquear la IM)
  - Reducirlo ó Mitigarlo (ej. Se implementan controles)
  - Aceptarlo (ej. La compañía entiende el nivel de riesgo y vive con el)

Esquema general del manejo del riesgo



FIN

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Gestión del riesgo: análisis cuantitativo

Profesor
Juan Ignacio Iturbe A.

Fundamentos de ciberseguridad

Pasos del enfoque cuantitativo

- Ahora es necesario llevar a cabo el análisis de riesgo, donde se requiere interpretar todos los datos obtenidos en las etapas anteriores.
- En este enfoque se utilizan los siguientes valores:
  - Expectativa de perdida única (Single Loss Expectancy, SLE)
  - Expectativa de perdida anual (Annual loss expentancy, ALE)

Pasos del enfoque cuantitativo

- SLE:
  - es un valor monetario que es asignado a un solo evento
  - representa la perdida potencial de la compañía si una amenaza específica tiene lugar. Su ecuación es:
  - SLE = Valor del activo * Factor de exposición (EF)
- EF: representa el porcentaje de la perdida una vez realizada la amenaza en un activo específico.

Pasos del enfoque cuantitativo

- Por ejemplo, si un data warehouse tiene por valor $80.000.000, y se estima que si ocurre un incendio, el 25% del warehouse puede ser dañado, esto quiere decir que el SLE es:
  - SLE =Valor activo x Factor de exposición
  - SLE= $80.000.000 * 25% = $20.000.000
- Esto quiere decir que la perdida potencial es de $20.000.000 si el incendio se produce.
- Pero necesitamos la perdida potencial anual (ALE).

Pasos del enfoque cuantitativo

- ALE = SLE * Ratio anualizado de ocurrencia (ARO)
- ARO: es el valor que representa la estimación de frecuencia de una amenaza específica tomando como ventana de tiempo, 12 meses.
- El rango puede ser de 0,0 (nunca) a 1,0 (una vez al año) a mas de 1 (muchas veces en el año)
- Por ej: si la probabilidad de incendio y que dañe el data warehouse es de una cada diez años, el valor de ARO es 0,1
- Entonces si el SLE=20.000.000, ARO=0,1 entonces el ALE=2.000.000

Pasos del enfoque cuantitativo

- El ALE, le dice a la compañía que si busca implementar un control para proteger el activo (warehouse) de su amenaza (el incendio)
  - se puede gastar razonablemente anualmente $2.000.000 o menos para proveer el necesario nivel de protección.
  - No es un buen negocio gastar mas que eso.

Ejemplo de listado de activo y sus amenazas

Activo	Amenaza	Expectativa de perdida única (SLE)	Ratio anualizado de ocurrencia (ARO)	Expectativa anualizada de perdida (ALE)
Instalaciones físicas	Fuego	$12.000.000	0.1	$1.200.000
Secreto comercial	Robo	$20.000.000	0.01	$200.000
Servidor de archivos	Fallo	$5.000.000	0.1	$500.000
Datos	Virus	$3.500.000	1.0	$3.500.000
Información de tarjeta de crédito de clientes	Robo	$150.000.000	3.0	$450.000.000

Decisiones inteligentes

- En tabla anterior se tiene un ejemplo de valores de un análisis de riesgos cuantitativo
- Con esta información, la compañía, puede tomar decisiones inteligentes. Por ej:
  - En que amenazas focalizarse primero.
  - Cuanto dinero gastar en protegerse de la amenaza

Resultados de un análisis cuantitativo

- Se debe entregar a la gerencia un reporte detallado (con resumen ejecutivo), los siguientes tópicos:
  - Valores monetarios asignados a los activos.
  - Lista completa de todos los posibles y amenazas significativas.
  - Probabilidad del ratio de ocurrencia de cada amenaza.
  - Perdida potencial que la compañía puede soportar por amenaza en una ventana de tiempo de 12 meses.
  - Controles recomendados.
- Todo esto, haciendo énfasis en las posibles perdidas monetarias y los costos necesarios para mitigarlos.

Selección de controles

- Un control de seguridad debe hacer un buen negocio.
- Este requiere de un análisis costo/beneficio. Este se hace comúnmente con:
  - (ALE antes de implementar el control) –(ALE después de implementar el control) - (valor del control para la compañía)

Ejemplo

- Si el ALE (Expectativa de perdida anual) de la amenaza de un hacker derribando un webserver es $6.000.000 antes de implementar el control
- El ALE es $1.500.000 después de implementado el control.
- Mientras que el costo de mantención y operación del control es de $325.000
  - $6.000.000 - $1.500.000 - $325.000
- Entonces el beneficio de este control para la compañía es de $4.175.000 anualmente.

Selección de controles

- El costo de una contramedida es más que la cantidad anotada en la orden de compra.
- Los siguientes items deben considerarse y evaluarse cuando se este revisando el costo total del control.
  - Costo del producto
  - Costo Diseño, planificación e implementación
  - Modificaciones del entorno
  - Compatibilidad con otros controles
  - Requerimientos de mantenimiento
  - Requerimientos de prueba
  - Costos de reparación, reemplazo o actualización
  - Costos de operación y soporte
  - Efectos en la productividad
  - Costos de subscripción
  - HH extras para monitoreo y respuesta a alertas

Ejemplo

- Si una compañía decide comprar un IDS para proteger muchos de sus recursos por el cual pagan $5.500. ¿Este es el costo total?
  - Este software debe probarse en un ambiente diferente al de producción para evitar cualquier mal comportamiento o actividad inesperada
  - El grupo de seguridad debe instalar los sensores, el software de administración, el software de monitoreo, configurar los sensores con la consola de administración, etc.
  - También se deben configurar algunos *routers* para redirigir el tráfico y definitivamente para que los usuarios no tengan acceso a la consola de administración
  - Se deben actualizar las firmas de ataque en la base de datos y también correr simulaciones.
  - También se deben considerar los costos de una alerta del IDS.
  - Equipamiento para los administradores de seguridad (como *smartphones* para que estén atentos a las alertas)
  - etc

Ejemplo

- Por lo tanto:
  - El costo del control es $5.500
  - Entrenamiento $2.500
  - Tiempo de laboratorio y testing $3.400
  - Perdida de productividad de usuarios cuando el producto entra en producción $2.600
  - Reconfiguraciones de router, instalación del productos, resolución de problemas, e instalación de dos parches post instalación $4.000
  - Entonces, el costo real del control de $18.000
- Si nuestra perdida potencial total es de $9.000 entonces estamos 100% sobre el presupuesto cuando aplicamos este control para el riesgo identificado.

FIN

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Gestión del riesgo: análisis cualitativo

Profesor
Juan Ignacio Iturbe A.

Fundamentos de ciberseguridad

Análisis de riesgos cualitativo

- No se asignan números y valores monetarios.
- Se orienta en diferentes escenarios de posibilidades de riesgos
- Rankea las seriedad de la amenaza y la validez de las diferentes posibles contramedidas basándose en opiniones
- Un barrido amplio de los escenarios, se puede llegar a tener cientos de estos.

Análisis de riesgos cualitativo

Un análisis de riesgo cualitativo puede incluir:

- Opiniones
- Mejores prácticas
- Intuición
- Experiencia

Delphi: es un método de decisión de grupo usada para asegurar que cada miembro da una opinión honesta de lo que piensa sobre los resultados de una amenaza particular.

Técnicas para obtener datos para el análisis cualitativo:

- Tormenta de ideas
- Storyboards
- Focus group
- Encuestas
- Cuestionarios
- Checklists
- Reuniones uno a uno
- Entrevistas
- Delphi

Análisis de riesgos cualitativo

- El equipo:
  - determina que técnica utilizar para la evaluación de las amenazas.
  - se reúne con personal que tiene experiencia y conocimiento sobre las amenazas que se están evaluando
  - Le presenta al personal escenarios que describen amenazas y perdidas potenciales.
  - Cada miembro del personal responde con su parecer y experiencia sobre la probabilidad de la amenaza y el consiguiente daño que puede resultar

Análisis de riesgos cualitativo

- Un escenario de cada vulnerabilidad es identificado y es explorado como puede ser explotado.
- El experto en el grupo (el mas familiar con la amenaza), debe revisar el escenario para asegurarse de que refleja cómo se llevaría a cabo una amenaza real.
- Controles que pueden disminuir el daño de esta amenaza son evaluados.
- El escenario se desarrolla con cada control

Análisis de riesgos cualitativo

- La posibilidad de exposición y la posibilidad de perdida pueden ser rankeados como Alto medio o bajos, en una escala de 1 al 5 o de 1 a 10.

Matriz de análisis cualitativo

Probabilidad vs consecuencias (impacto)

Probabilidad	Consecuencias				
	Insignificante	**Menor**	**Moderado**	**Mayor**	**Severo**
Casí seguro	M	A	A	E	E
Probable	M	M	A	A	E
Posible	B	M	M	A	E
Improbable	B	M	M	M	A
Raro	B	B	M	M	A

E	Extremadamente alta
A	Alta
M	Media
B	Baja

Análisis de riesgos cualitativo

- Una vez que el personal seleccionado rankea:
  - La posibilidad de que una amenaza suceda
  - La perdida potencial
  - Las ventajas de cada control
- Esta información es compilada dentro de un reporte y presentada a la gerencia para ayudar a tomar mejores decisiones sobre como implementar los mejores controles en el ambiente productivo.

Ejemplo

- El equipo de análisis de riesgo:
  - presenta un escenario explicando las amenazas de una hacker accediendo a información confidencial almacenada en cinco servidores de archivos en la compañía.
  - Distribuye este escenario en formato escrito a un equipo de cinco personas y se les da una tabla para que clasifiquen diferentes puntos.

Ejemplo de análisis cualitativo

Amenaza = Hacker accediendo a información confidencial	Severidad de la amenaza	Probabilidad de materialización de la amenaza	Perdida potencial para la compañía	Efectividad del firewall	Efectividad del IDS	Efectividad del Honeypot
Gerente TI	4	2	4	4	3	2
Administrador BD	4	4	4	3	4	1
Programador	2	3	3	4	2	1
Operador de sistema	3	4	3	4	2	1
Gerente de operaciones	5	4	4	4	4	2
Resultados	**3.6**	**3.4**	**3.6**	**3.8**	**3**	**1.4**

Ejemplo análisis cualitativo

- La tabla anterior, trata de solamente una amenaza.
- A la gerencia se le presentan una serie de escenario de amenazas
  - de acuerdo a la severidad, probabilidad y la perdida potencial para la empresa, elige cual enfrentar primero
  - Y se eligen que controles implementar.

FIN

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Actividades y preguntas propuestas

Actividad propuesta

- Realice la matriz de riesgos sobre el enunciado de la actividad anterior.
  - Identifique activos y valorícelos
  - Realice un análisis cualitativo sobre 4 riesgos.
  - Realice un análisis cuantitativo sobre 1 riesgo.
- Esto debe ser parte de la exposición del próximo día Jueves.
- Realice y especifique los supuestos necesarios.
- Utilice como base la planilla llamada “Seccion A13 ISO 17799 Matriz ISO_27001V3”

Sección de preguntas

- Preguntas con alternativas
- Las alternativas pueden ser todas validas pero, se debe elegir la mejor alternativa.

Preguntas

- ¿Quién es el primer responsable de determinar el nivel de clasificación para la información?
  a) El gerente de TI
  b) El usuario
  c) El dueño (owner)
  d) Gerente general
  e) N.A.

Preguntas

- ¿Quién es el último responsable de asegurarse que la data es clasificada y protegida?
  a) El dueño (owner)
  b) Usuario
  c) Administradores
  d) Gerencia
  e) T.A

Preguntas

- Cual es la mejor técnica para determinar si una control especifico de seguridad debe implementarse
  a) Análisis de riesgo
  b) Análisis costo-beneficio
  c) ALE
  d) Identificar vulnerabilidades y amenazas que causan el riesgo.
  e) N.A

Preguntas

- ¿Cómo se calcula el riesgo residual?
  a) Amenaza x riesgos x valor del activo
  b) (Amenaza x valor del activo x vulnerabilidad) x riesgos
  c) SLE x frecuencia
  d) (Amenaza x vulnerabilidad x valor del activo) x brecha de controles (controls gap)
  e) T.A

Preguntas

- ¿Que describe mejor un análisis de riesgo cuantitativo?
  a) Un análisis basado en escenarios para investigar diferentes amenazas de seguridad
  b) Un método usado para analizar niveles severos de perdidas potenciales, probabilidad de perdida y riesgos
  c) Un método que asigna valores monetarios a componentes en la evaluación del riesgo
  d) Un método que es basado en corazonadas y opiniones
  e) N.A

Preguntas escenario 1

- Las próximas preguntas se basan en el siguiente escenario.
  - En los últimos años, un servidor, que tiene datos sensibles, es almacenado en una habitación sin seguros en la compañía A.
  - La puerta de la habitación tiene un escrito en la puerta que dice “Oficina 1”. Este escrito fue puesto, para que la gente pensara que no hay servidores importantes en la habitación.
  - Convencidos que esta no es una buena práctica, la compañía ha decidido:
    - Instalar una cerradura reforzada a la oficina y una jaula al servidor.
    - Removieron el escrito de la puerta
    - Incrementaron la seguridad de la configuración del servidor y estricto control de acceso al sistema operativo.

Preguntas escenario 1

- El hecho que el servidor haya estado en un cuarto sin seguros marcado como “Oficina 1” por los últimos años significa que la compañía está practicando:
  a) Seguridad lógica
  b) Gestión del riesgo
  c) Transferencia del riesgo
  d) Seguridad a través de la oscuridad
  e) N.A

Preguntas escenario 1

- ¿La nueva cerradura reforzada y la jaula del servidor que tipos de controles son?
  a) Controles lógicos
  b) Controles físicos
  c) Controles administrativos
  d) Controles compensatorios
  e) T.A

Preguntas escenario 1

- ¿Los controles de acceso del sistema operativo que tipo de controles son?
  a) Controles lógicos
  b) Controles físicos
  c) Controles administrativos
  d) Controles compensatorios
  e) T.A

Preguntas escenario 2

- Una pequeña oficina remota para una compañía es avaluada en $800.000 USD.
- Basado en datos históricos, la probabilidad de ocurrencia de un incendio es de uno cada diez años en una instalación en el área.
- Se estima, que un incendio puede destruir el 60% de las instalaciones bajo las actuales circunstancias y con los actuales controles detectivos y preventivos instalados.

Preguntas escenario 2

- ¿Cual es el SLE?
  a) $80.000
  b) $480.000
  c) $320.000
  d) 60%
  e) N.A

Preguntas escenario 2

- ¿Cual es el ARO?
  a) 1
  b) 10
  c) 0.1
  d) 0.01
  e) N.A

Preguntas escenario 2

- ¿Cuál es el ALE?
  a) $480.000
  b) $32.000
  c) $48.000
  d) .6
  e) N.A

Preguntas propuestas

- ¿Cuáles son los cuatro dominios de COBIT?
  a) Planear y organizar, adquirir e implementar, entregar y dar soporte, monitorear y evaluar.
  b) Planear y organizar, entregar y dar soporte, adquirir e implementar, monitorear y evaluar.
  c) Planear y organizar, adquirir e implementar, soportar y comprar, monitorear y evaluar.
  d) Adquirir e implementar, entregar y dar soporte, y monitorear y evaluar.
  e) N.a.

Preguntas propuestas

- ¿Por qué el equipo que realiza el análisis de riesgos de la información debe entrevistar a gente de diferentes departamentos?
  a) Para estar seguros que el proceso es justo y estar seguros que nadie quede fuera.
  b) No lo debe hacer. Con un pequeño grupo de la compañía es suficiente.
  c) Por que la gente de diferentes departamentos entienden mejor sus riesgos. Esto asegura que los datos del análisis son lo mas cercanos a la realidad posible.
  d) Porque la gente en los diferentes departamentos son los que causan los riesgos.

Preguntas propuestas

- ¿Que tipo de control son las luces y los seguros de puertas?
  a) Preventivo
  b) Correctivo
  c) Detectivo
  d) Disuasivo
  e) Recuperativo

Preguntas propuestas

- ¿Cuál es el primer paso en un análisis de riesgo?
  a) Identificar el equipo y el alcance
  b) Identificar los activos y valorizarlos
  c) Realizar un análisis costo/beneficio
  d) Mitigar el riesgo
  e) N.a

FIN

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE