Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

Curso Ciberseguridad para Auditores Internos

Ciberseguridad

Santiago, 18 de octubre de 2018

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia

Conceptos utilizados en Ciberseguridad

Gobierno de la Seguridad

El gobierno de la seguridad de la información general, establece el marco y los límites para la gestión de la seguridad y soluciones relacionadas. Esto incluye necesariamente políticas formales, procedimientos y otros elementos de guía que la empresa y sus socios deben seguir. No obstante, cuando el gobierno en su mejor sentido significa “hacer lo correcto”, tiene que tener en cuenta que una gran parte de la ciberseguridad se ocupa de la gestión de eventos e incidentes inesperados.

El gobierno de ciberseguridad es tanto preventivo como correctivo. Abarca los preparativos y precauciones adoptados contra el cibercrimen, la ciberguerra y otras formas pertinentes de ataque. Al mismo tiempo, el gobierno de la ciberseguridad determina los procesos y procedimientos necesarios para hacer frente a incidentes reales causados por un ataque o violación de seguridad.

Objetivos de Gobierno de la Ciberseguridad

Objetivo	Gobierno de la Ciberseguridad
Orientado a la inteligencia sobre amenazas	Integrar e internalizar las nuevas vulnerabilidades, amenazas y riesgos—implantar elementos adaptativos y alinear el riesgo con las necesidades del negocio y la inteligencia de amenazas.
Funciones integradas de seguridad	Integrar plenamente las funciones de seguridad con funciones de negocio, implantar el intercambio obligatorio de información y canales de comunicación bien definidos.
Proactivo y basado en la anticipación	Anticipar los ataques y el comportamiento del atacante, evitar el minimalismo en la estrategia y el gasto de seguridad, implantar un ciclo de vida de seguridad sistémico.
Flexible, adaptable y resiliente	Dar cabida al cambio—implantar la adaptación y el aprendizaje y la mejora reflexivos tanto operacionales como organizacionales, incluir el pensamiento en la continuidad del negocio y de los servicios de TI.
Orientada a servicios hacia el negocio	Definir e implantar la seguridad como un servicio al negocio.

Transformando la Ciberseguridad

- La ciberseguridad a menudo se subdivide en cuatro fases de un ciclo de vida continua. Esto es útil para ilustrar la naturaleza continua de la seguridad como concepto. Mantener el nivel de seguridad deseado en y alrededor de la empresa y sus socios es un camino de mejora continua.

- Para defenderse con éxito frente a las APTs y otras amenazas y vulnerabilidades críticas, la ciberseguridad debe transformarse en un proceso de negocio que esté alineado con el gobierno, la gestión de riesgos y los acuerdos de cumplimiento de la empresa.

- Las cuatro fases son:
  - Preparar
  - Investigar
  - Remediar/responder
  - Transformar

- Si bien las tres primeras fases están estrechamente vinculadas a los ataques APT actuales u otros incidentes de seguridad, la fase de transformación tiene una perspectiva mucho más amplia. Esta perspectiva incluye el análisis posterior al incidente así como aprendizajes clave y oportunidades de mejora. Incluye, además, cambios en el régimen de gobierno, riesgo y cumplimiento (GRC) aplicados en la empresa, sus asociados y sus socios de negocios.

Ciclo de vida PIRT

- Una vez que una organización se enfrenta al impacto de este tipo de ataques, el ciclo de vida PIRT debería ser aplicado como en cualquier otro escenario.

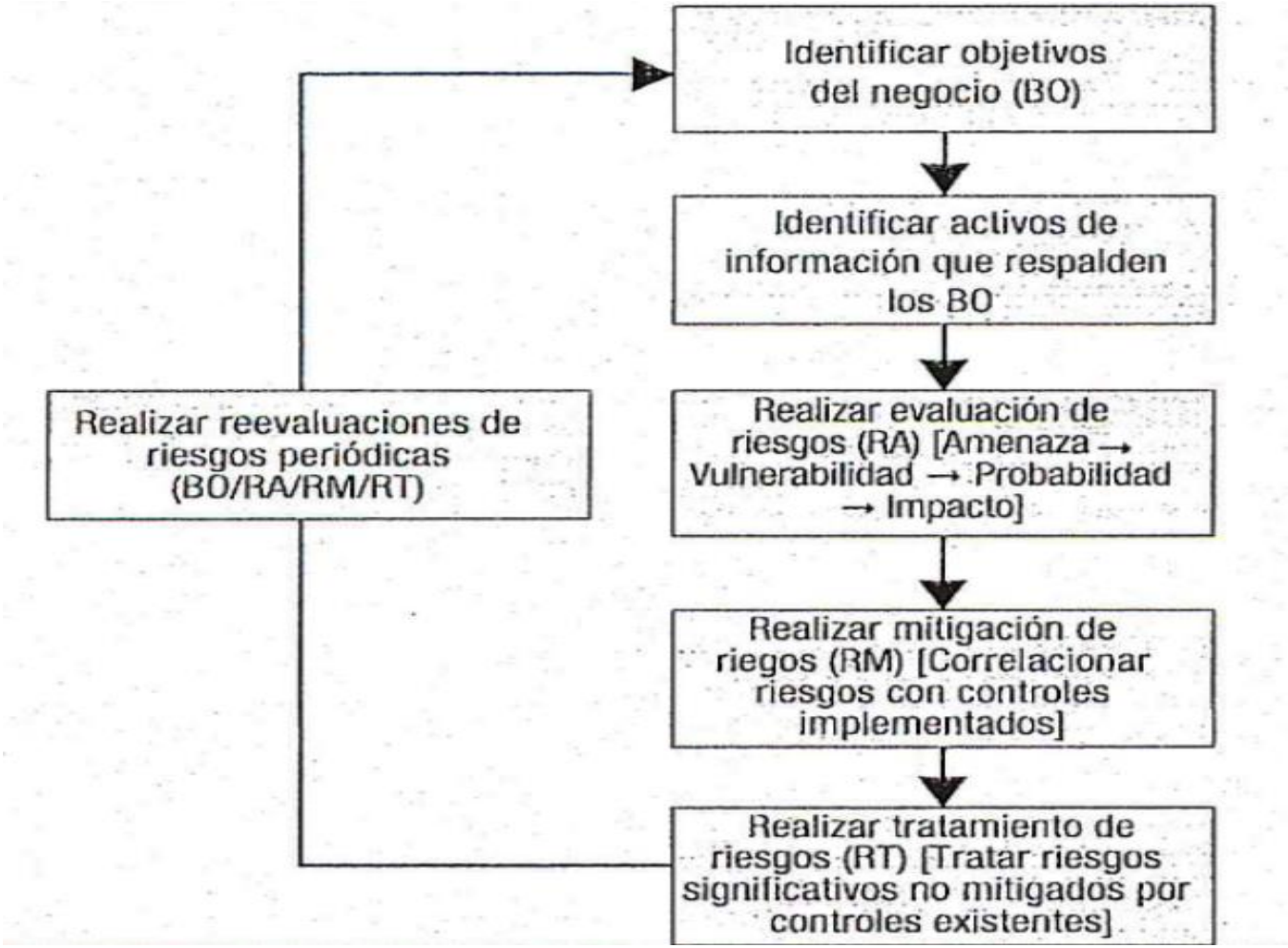
Amenazas, Vulnerabilidades y Riesgo

La transformación de la seguridad comienza con la identificación, categorización y mapeo de las vulnerabilidades, las amenazas y el riesgo

Categorización de Amenaza y Vulnerabilidad

Desde una perspectiva de la ciberseguridad, las amenazas y vulnerabilidades necesitan ser categorizadas, así como, el riesgo asociado. Al contrario que en la seguridad de la información en general, el foco se encuentra en las amenazas avanzadas y sobre las vulnerabilidades que no pueden ser, ni fácilmente detectables, ni solventadas

Proceso de evaluación de Riesgos



Riesgo

- El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por consiguiente, ocasione pérdida o daño a la organización.

Amenaza

Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que es capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado (ISO/IEC 13335)

Vulnerabilidad

Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

Contramedida

Cualquier proceso que reduce directamente una amenaza o vulnerabilidad.

Concepto de Control de TI

Controles son las políticas, procedimientos, prácticas y estructuras organizacionales creadas para proveer una razonable garantía de que los objetivos del negocio serán alcanzados y que eventos indeseables serán evitados o detectados y corregidos.

Son varios los objetivos de los controles, entre los cuales se pueden citar:

a. prevenir fraudes, errores o abusos;
b. proteger activos organizacionales;
c. asegurar obediencia de las directrices, planes, normas y procedimientos;
d. asegurar la validez y la integridad de los datos utilizados para la toma de decisión;
e. servir como instrumento auxiliar de gestión;
f. tener un carácter preventivo.

Controles de TI

Los controles generales de TI más comunes son:

a. procesos de planificación estratégico institucional y de TI;

b. organización y administración de TI;

c. políticas y estándares organizacionales, especialmente los relacionados con TI, tales como política de seguridad, política de control de acceso etc.;

d. definición de los roles y responsabilidades de cargos, funciones y ambientes de TI y de negocio, con respecto al principio de la segregación de funciones;

e. procesos de capacitación, elaboración de presupuesto y gestión de proyectos de TI;

f. controles del ciclo de vida de software, tal como el proceso de software;

g. controles de gestión de cambios;

h. controles de acceso lógico;

i. controles de seguridad física sobre los centros de procesamiento de datos (data centers);

j. controles de copias de seguridad y de recuperación de sistemas y datos;

k. controles de operaciones de TI;

l. plan de continuidad de negocios.

Gobierno de TI

Le incumben 2 aspectos:

- Que TI entregue valor al negocio y
- Que los riesgos sean gestionados

Lo primero se logra con la alineación estratégica de TI con el negocio

Lo segundo se logra con el establecimiento de la gestión y el gobierno de riesgos y también la responsabilidad dentro de la empresa.

Protección de los activos de Información

Hay 5 tareas:

1. Evaluar las políticas, los estándares y los procedimientos de seguridad de la información para determinar su integridad y alineación con las practicas generalmente aceptadas

2.Evaluar el diseño, la implementación y el monitoreo de los controles de seguridad lógicos y del sistema para verificar la confidencialidad, la integridad y la disponibilidad de la información.

3. Evaluar el diseño, la implementación y el monitoreo de los procesos y procedimientos de clasificación de datos para determinar si están alineados con las políticas, los estándares, los procedimientos de la organización, y requerimientos externos aplicables.

4. Evaluar el diseño, la implementación y el monitoreo de los controles de acceso físico y del entorno para determinar si los activos de información están adecuadamente protegidos.

5. evaluar los procesos y procedimientos utilizados para almacenar, recuperar, transportar y desechar activos de información (por ejemplo, soportes de respaldo, almacenamiento externo, copia impresa, soportes y copia electrónica) para determinar si los activos de información están adecuadamente protegidos.

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

¡Gracias por su Atención!

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia