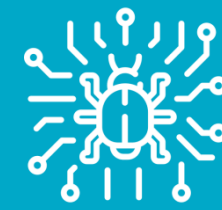
MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

RESPONDIENDO ANTE CIBERINCIDENTES

Marsh College Perú

15 de agosto de 2019



Edson Villar
Líder de Consultoría en Ciber-Riesgo
Latinoamérica y El Caribe
Marsh Risk Consulting

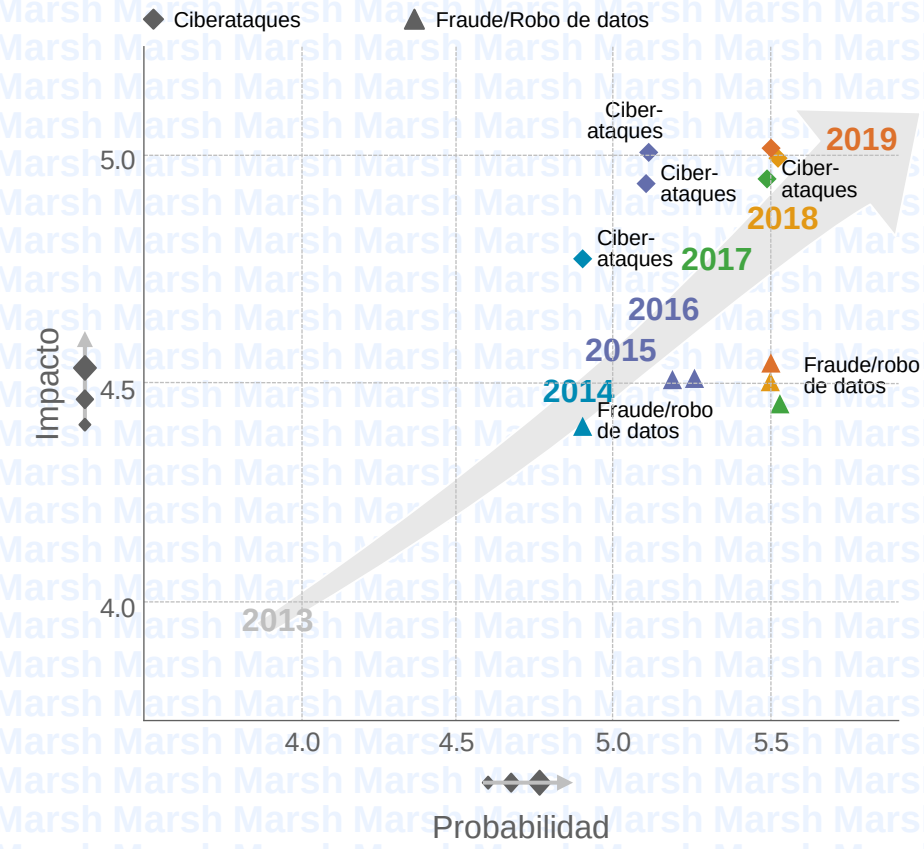
MARSH

Evolución del Ciber-Riesgo

Los ciberataques, al igual que el fraude y la pérdida de datos son percibidos como riesgos severos a nivel global

Mapa de Percepción de Riesgos del World Economic Forum

(Evolución de ciberataques y fraude/robo de datos 2013–2019)



Fuente: World Economic Forum Global Risk Report, Marsh & McLennan Companies
Nota: Data de 2017-2019 ha sido ajustada para ser comparada, debido a un cambio en la escala.

El Ciber-Riesgo es considerado un riesgo catastrófico

Los ciberataques y brechas de datos están en el top 5 de los riesgos globales a nivel de probabilidad e impacto

La ciber-dependencia está calificada como el evento número 2 que con mayor probabilidad afectará el desarrollo del mundo en los próximos 10 años, resaltando la fuerte interconexión de las infraestructuras críticas con cyber.

El Ciber-Riesgo es el 5to mayor riesgo para las operaciones del negocio, debido a que potencialmente puede parar el negocio de las compañías dependientes de la tecnología.

Los ciberataques tendrán un impacto mayor que los desastres del medio ambiente provocados por el hombre y las enfermedades infecciosas, causando un daño tan grande como el colapso de un ecosistema y solo un poco menos que los desastres naturales y la crisis por el agua en los próximos años.

¿Cuál es el impacto real de una brecha de seguridad?

Análisis financiero del posible impacto de una brecha

24,615 es la cantidad promedio de registros que son afectados en una brecha de datos a nivel global
(Ponemon Institute - 2018 Cost of a Data Breach Study)

$148 es el costo promedio por registro afectado en una brecha de datos. Las empresas con equipo de respuesta tienen un ahorro promedio de $14 por registro.
(Ponemon Institute - 2018 Cost of a Data Breach Study)

$3.86M es el costo promedio total de una brecha de datos a nivel global.
(Ponemon Institute - 2018 Cost of a Data Breach Study)

$6B es el costo estimado de los daños causados por el ciber-crimen para el 2021, lo que convierte a los ciberataques en algo más beneficioso que el tráfico de drogas
(Cybersecurity Ventures - 2019 Official Annual Cybercrime Report)

$408 costo promedio por registro de salud*

$206 costo promedio por registro en sector financiero*

$181 costo promedio por registro en compañías de servicios*

*Fuiente: Ponemon Institute - 2018 Cost of a Data Breach Study

Aclarando conceptos
DRP ≠ IRP

Disaster Recovery Plan

1. Su objetivo es la continuidad del negocio.
2. Normalmente no requiere la recolección de evidencia y no siempre requiere un análisis detallado para la detección.
3. Suelen ser casos muy públicos con muchos involucrados para restaurar las operaciones.
4. Se enfoca en la calidad de los datos y la ejecución de los procesos.
5. Se enfoca en la recuperación de operaciones de TI.
6. Normalmente las causas suelen ser conocidas y el plan puede actualizarse con una frecuencia menor.
7. Requiere la participación del equipo de facilities.

[Cyber] Incident Response Plan

1. Su objetivo es la protección de activos.
2. Requiere un análisis de la causa raíz, recolección y preservación de evidencia, y una respuesta coordinada.
3. Suelen ser manejados de manera confidencial, por un equipo limitado de personas.
4. Se enfoca en la protección para evitar que el incidente vuelva a ocurrir, no en la restauración total de los datos.
5. Se enfoca en prevenir o limitar las interrupciones de TI y en mantener las operaciones de TI.
6. Aparecen nuevos tipos de ataque con más frecuencia y es más complicado de mantener actualizado.
7. Normalmente no se requiere la participación del equipo de facilities, a menos que haya un robo físico.

Similitudes

- Ambos cuentan con procedimientos para minimizar el impacto de un incidente, con posteriores planes de recuperación, planes de retorno a producción y lecciones aprendidas. Normalmente, necesitan la presencia del CISO, CIO y administradores de TI.
- Son complementos perfectos e incluso deberían ser probadas en conjunto.
- Ambos trabajan para lograr la ciber-resiliencia organizacional.

Fuente: https://www.csoonline.com/article/3218083/disaster-recovery-vs-security-recovery-plans-why-you-need-separate-strategies.html

Aclarando conceptos
Componentes clave

- Implementación de herramientas:
  - Detección
  - Análisis forense
  - SOAR
  - Notificación alterna
- **Concientización al personal.**
- Gestión de parches y vulnerabilidades.
- Definición del equipo de respuesta ante ciberincidentes.
- Definición de la ubicación (war room).
- Definir puntos de contacto con terceros críticos.
- Plan de respuesta ante ciberincidentes.
- Planes operativos para los escenarios principales (p.e. ransomware, fuga de información, etc.).
- Comunicación y capacitación.
- Ejercicios de respuesta a nivel táctico y estratégico.
- Incorporación de lecciones aprendidas de casos públicos e incidentes pasados.

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

- Desarrollo de las capacidades de detección de los principales incidentes que podrían ocurrir en la organización.
- El objetivo es ser capaces de detectar un incidente antes que escale.
- Es importante diferenciar: Precursores de indicadores.
- Algunos de los vectores de ataque a tratar, incluyen los siguientes:
  - Medio removible
  - Degradación de servicios
  - Ataque web
  - Correo electrónico
  - Suplantación de identidad
  - Uso inadecuado
  - Robo o pérdida de dispositivos
- Monitoreo de eventos para detectar anomalías o intrusiones: IDS, SIEM, Antivirus, logs del S.O., logs de aplicaciones, flujos de red, información de vulnerabilidades, personas, etc.

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

- Identificación de actividad sospechosa.
- Eliminación de falsos positivos.
- Algunas buenas prácticas incluyen:
  - Perfilamiento de redes y sistemas.
  - Entendimiento de patrones normales de comportamiento.
  - Definición de políticas de retención de logs.
  - Correlación de eventos.
  - Sincronización de relojes.
  - Preparar una base de datos de conocimiento.
  - Filtrado de información relevante.
  - Intercambio de información con terceros.
- Evaluación del impacto de la brecha: Cantidad de equipos impactados.
- Clasificación del incidente y priorización.
- Notificación del incidente.
- **La discreción es clave.**

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

Preparación | Detección y análisis | **Investigación, contención y erradicación** | Recuperación y notificación | Lecciones aprendidas

Investigación:

- Se busca determinar la causa raíz, antes de tomar cualquier otra acción.
- Convocar al equipo de respuesta ante ciberincidentes.
- Reconocimiento de lo(s) atacante(s):
  - Validación de IPs.
  - Investigación en la web.
  - Base de datos de incidentes.
  - Información de inteligencia.
- Adquisición de evidencia. ← Cadena de custodia
- e-Discovery (Análisis forense o no)
- Análisis de malware.
- Se debe ir activando la comunicación con los equipos de recuperación.

¿Qué?
¿Quién?
¿Cómo?
¿Cuándo?
¿Dónde?

- Sistema Operativo
- (últimos archivos abiertos, horas de acceso, programas utilizados, archivos borrados, etc.)
- Navegación web
- Correo electrónico
- Memoria volátil

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

Contención:

- Se busca controlar el incidente para minimizar el impacto en la organización.
- El objetivo es ganar tiempo para ejecutar una estrategia de remediación adecuada.
- Definición de la estrategia de contención según el tipo de incidente.
- Una contención sin reconocer qué ocurrió puede causar una mayor exposición.
- Ejecución de la estrategia de contención:
  - Apagado de equipos.
  - Desconexión de segmentos de red.
  - Desconexión de terceros.
  - Deshabilitación de servicios.
  - Cambios en el firewall, web filter, etc.

Erradicación;

- Se busca eliminar cualquier rastro del incidente en la organización.
- Definición del plan de erradicación para el incidente.
- Se busca eliminar cualquier rastro del incidente en la red. Por ejemplo:
  - Eliminación de malware.
  - Deshabilitación de cuentas de usuario maliciosas.
  - Cambiar contraseñas de usuarios comprometidos.

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

- Restauración de los sistemas para regresar a la operación normal y que la situación no vuelva a ocurrir.
- Una recuperación adecuada no se puede realizar hasta que no se haya contenido y erradicado un incidente.
- La recuperación puede incurrir en cambios a nivel de diseño del entorno y controles de seguridad.
- **Hay que tener en cuenta que si un ataque ocurre, hay una gran posibilidad de que el atacante vuelva a intentarlo.**
- Se debe priorizar el proceso de remediación.
- Puede incluir actividades como:
  - Restaurar sistemas desde un backup limpio.
  - Reinstalación desde cero.
  - Reemplazo de archivos infectados por los archivos originales.
  - Instalación de parches.
  - Cambio de contraseñas.
  - Refuerzo de las configuraciones de seguridad.
- Es clave contar con un plan de comunicación definido y probado, según cada fase de la respuesta.
- La comunicación involucra a clientes, colaboradores, reguladores, medios y otras entidades de gobierno.

Fuente: NIST SP 800-61r2

Aclarando conceptos
Componentes clave

- ¿Quién es el culpable?
- ¿Qué ocurrió y cuándo?
- ¿Cómo reaccionamos frente al incidente? ¿Seguimos los procedimientos documentados? ¿Eran correctos?
- ¿Qué información nos podría haber sido útil más pronto?
- ¿Qué podríamos haber hecho diferente?
- ¿Qué funcionó y qué no funcionó en la comunicación con terceros/reguladores/medios?
- ¿Qué acciones correctivas debemos implementar para evitar que esto vuelva a ocurrir?
- ¿Qué indicadores deberíamos revisar para detectarlo de manera más oportuna una próxima vez?
- ¿Qué recursos o herramientas adicionales se necesitan para detectar, analizar y mitigar futuros incidentes?

Fuente: NIST SP 800-61r2

Aclarando conceptos
SOAR - Automatizando la respuesta

Beneficios:
- Acelera la respuesta ante ciberincidentes
- Estandariza procesos
- Integra diferentes herramientas
- Mejora la productividad de los analistas

Gestión de alertas:
- Phishing y respuesta
- Enriquecimiento de información de malware
- Análisis de logins fallidos
- Análisis de logins desde ubicaciones inusuales

Soporte de operaciones de seguridad:
- Gestión de certificados digitales
- Monitoreo de políticas en endpoints
- Gestión de vulnerabilidades

Respuesta ante ciberincidentes y Threat Hunting:
- Búsqueda de IOC's
- Análisis de malware (detonación)
- Integración de plataformas de seguridad Cloud y On Premise
- Asignación de severidad de incidentes

Fuente: Demisto Security Orchestration Use Cases WP

Respondiendo ante ciberincidentes

Algunos de los principales retos que enfrentan las organizaciones

Entre los principales retos que enfrentan las organizaciones para poder definir un Plan de Respuesta ante Ciberincidentes, se encuentran los siguientes:

- Desconocimiento del nivel de exposición.
- Confusión entre DRP y CIRP.
- Ausencia de mecanismos de detección de ciberincidentes.
- Ausencia de la identificación de escenarios de riesgo que podrían generar impacto.
- Ausencia de formalización de los procesos de respuesta.
- Ausencia de liderazgo en el equipo de respuesta.
- Inadecuados procesos de comunicación externa e interna.
- Planes de respuesta ante ciberincidentes por cumplimiento o no probados.
- Herramientas en formato bala de plata.

Contáctanos

Si deseas saber cómo podemos apoyarte para preparar a tu organización para hacer frente a las ciberamenazas de hoy en día, contáctanos:

Mónica Acosta
Director
Marsh Risk Consulting
monica.acosta@marsh.com

Edson Villar
Líder Regional de Ciber-Riesgo
Marsh Risk Consulting
edson.villar@marsh.com

Gerardo Herrera
Director Regional
Marsh Risk Consulting
gerardo.herrera@marsh.com

MARSH RISK CONSULTING