Marsh

¿Cómo actuar en caso de un ataque de ransomware a un tercero?

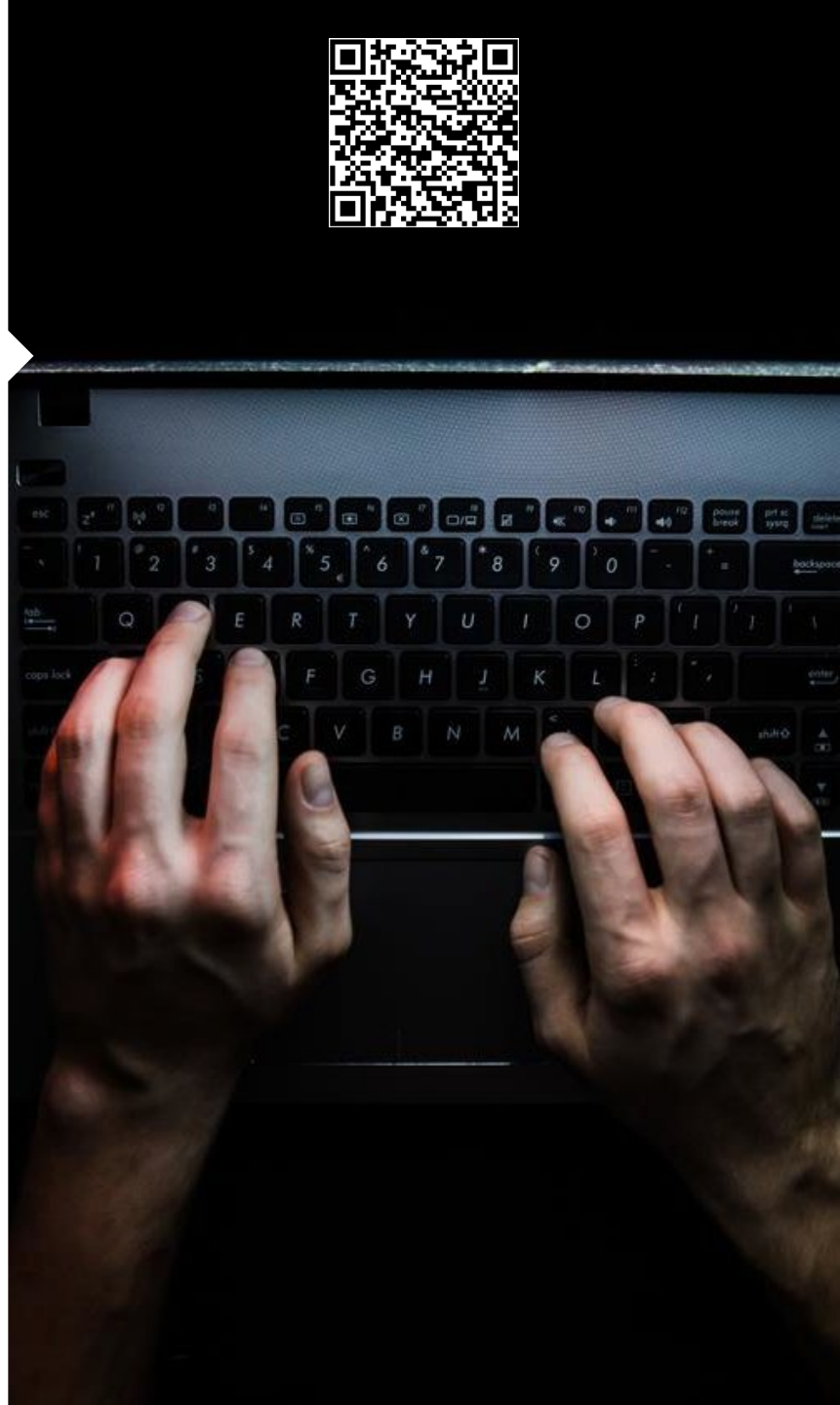
Recomendaciones generales

Latinoamérica
2023

Cyber Risk Consulting
Marsh Advisory

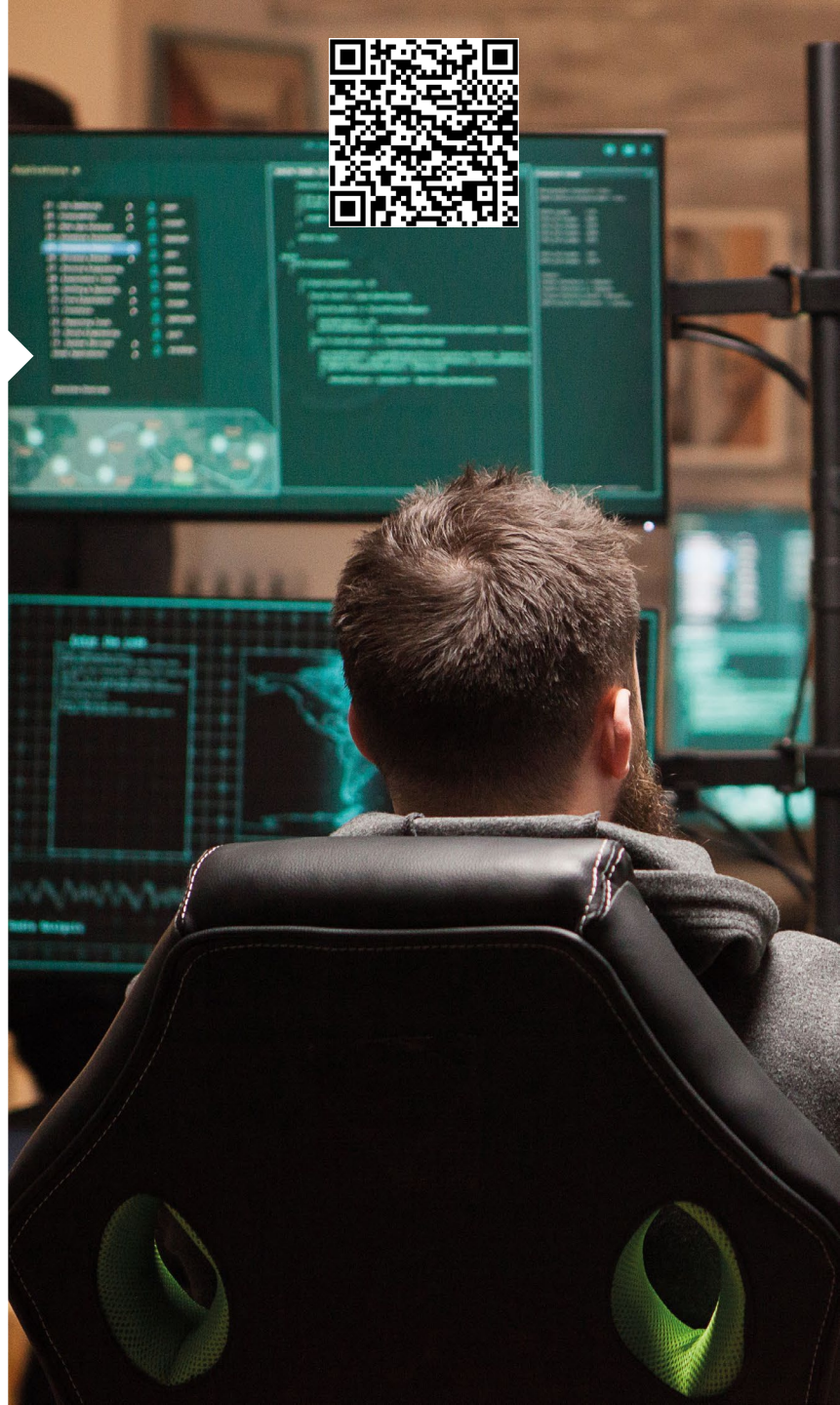
¿El tercero tiene conexión directa a través de la red o empleados on-site?

- Evaluar la posibilidad de bloquear cualquier punto de contacto entre las redes y sistemas del tercero afectado y la compañía (incluyendo administración de red).
- Solicitar o forzar el apagado y la desconexión de los equipos del tercero conectados a la red de la compañía.
- Analizar cualquier patrón sospechoso en la red que pueda sugerir una posible infección:
  - Usuarios no reconocidos.
  - Usuarios recientemente creados (principalmente con altos privilegios).
  - Tráfico de red anómalo (múltiples conexiones desde algunos equipos de red, principalmente en el puerto 139 y 445).
  - Gran volumen de datos saliendo de la red.
  - Accesos desde ubicaciones (países) inusuales a la red.
  - Conexiones de red hacia IPs alojadas en ubicaciones (países) inusuales.
  - Intentos de conexión hacia direcciones IP de mala reputación.
  - Revisar los registros de auditoría en equipos o sistemas que no estén integrados a las plataformas de monitoreo de seguridad.
  - Entre otros.
- Solicitar los indicadores de compromiso de compromiso al tercero para validar que no hayan indicios de afectación en la organización.
- En caso el tercero tenga acceso a credenciales de la organización o tenga acceso a los sistemas de la compañía, evaluar la posibilidad de forzar el cambio de contraseñas para evitar suplantación de identidad.
- Evaluar la posibilidad de enviar un comunicado a los empleados, con un detalle a alto nivel de lo ocurrido y que reporten cualquier situación anómala en la red. Además, solicitar la discreción y evitar la desinformación.
- Analizar los contratos con clientes y terceros que puedan generar incumplimientos y posibles sanciones.
- Evalúe la posibilidad de exigir un reporte de la situación, así como las medidas implementadas por el tercero para evitar que esta situación vuelva a repetirse.
- En caso de contar con un seguro de riesgo cibernético, analizar las coberturas que podrían ser de utilidad en una situación como la expuesta.
- Solo reanude las conexiones con el tercero una vez que asegure a través de un reporte formal que la amenaza haya sido erradicada y su organización está fuera de peligro. Del mismo modo, implemente las medidas necesarias para prevenir, detectar y responder ante un nuevo ataque similar.
- Al finalizar el incidente, realizar una sesión de lecciones aprendidas para entender lo que funcionó y lo que podría mejorarse en próximas situaciones.



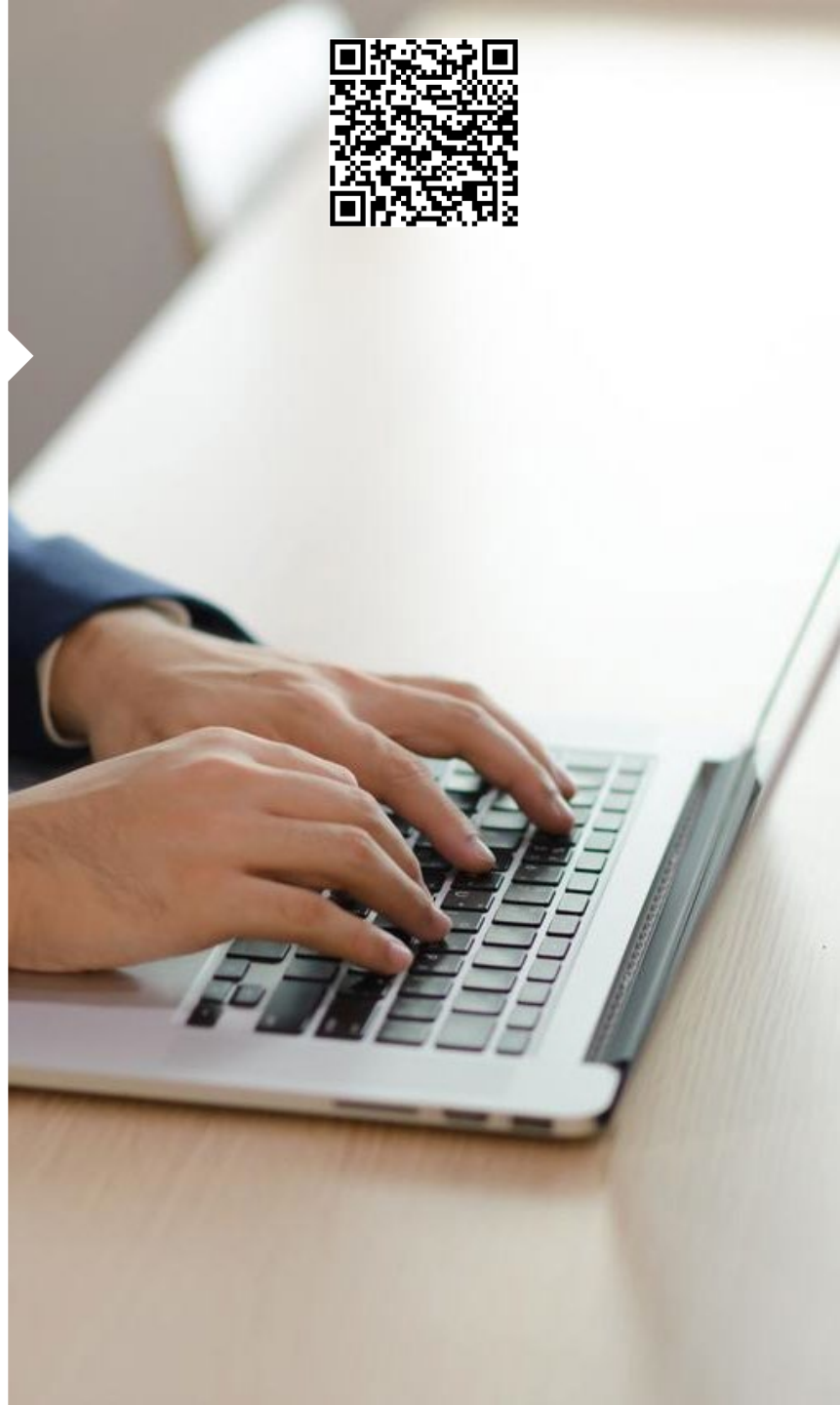
¿El tercero almacena o procesa datos sensibles de la organización?

- Evaluar la posibilidad de activar o al menos notificar al Comité de Crisis de la organización de manera temprana y mantenerlo informado de la evolución de la situación.
- En caso de conocer el foro o sitio web del grupo criminal que originó el ataque, monitorearlo a través de un equipo experto para identificar de manera oportuna cualquier información expuesta relacionada con la organización. El hacerlo por personal no especializado, podría poner en riesgo la seguridad de la red de la compañía.
- En caso se confirme la exposición o el acceso no autorizado por el grupo criminal a información sensible de la organización, realizar el reporte correspondiente a los reguladores y autoridades.
- Evaluar la posibilidad de construir mensajes base que serán enviados a las personas y empresas afectadas por la exposición de los datos del tercero, según diferentes escenarios relacionados con la evolución del caso.
- Evaluar la posibilidad de enviar un comunicado a los empleados, con un detalle a alto nivel de lo ocurrido y que reporten cualquier situación anómala en la red. Además, solicitar la discreción y evitar la desinformación.
- Si la organización es una entidad financiera y los datos de clientes han sido expuestos, evaluar la posibilidad de incrementar la sensibilidad del monitoreo de prevención del fraude para reducir los casos de suplantación de identidad.
- En caso el tercero tenga acceso a credenciales de la organización, evaluar la posibilidad de forzar el cambio de contraseñas para evitar suplantación de identidad.
- Desde el frente Legal, definir una estrategia preventiva para atender a las posibles denuncias que se generen por la afectación presentada.
- Analizar los contratos con clientes y terceros que puedan generar incumplimientos y posibles sanciones.
- Evalúe la posibilidad de exigir un reporte de la situación, así como las medidas implementadas por el tercero para evitar que esta situación vuelva a repetirse.
- En caso de contar con un seguro de riesgo cibernético, analizar las coberturas que podrían ser de utilidad en una situación como la expuesta.
- Al finalizar el incidente, realizar una sesión de lecciones aprendidas para entender lo que funcionó y lo que podría mejorarse en próximas situaciones.



¿La afectación del tercero genera una interrupción en las operaciones de la organización?

- Evaluar la posibilidad de activar o al menos notificar al Comité de Crisis de la organización de manera temprana y mantenerlo informado de la evolución de la situación.
- Evaluar la posibilidad de activar planes de contingencia que permitan mantener los procesos activos, mientras son recuperados desde el frente tecnológico. Es posible que la recuperación pueda demorar horas, días o incluso semanas.
- Evaluar la posibilidad de construir mensajes base que serán enviados a las personas y empresas afectadas por la exposición de los datos del tercero, según diferentes escenarios relacionados con la evolución del caso.
- Evaluar la posibilidad de enviar un comunicado a los empleados, con un detalle a alto nivel de lo ocurrido y que reporten cualquier situación anómala en la red. Además, solicitar la discreción y evitar la desinformación.
- En caso el tercero tenga acceso a credenciales de la organización, evaluar la posibilidad de forzar el cambio de contraseñas para evitar suplantación de identidad.
- Analizar los contratos con clientes y terceros que puedan generar incumplimientos y posibles sanciones en caso de interrupción prolongada.
- Evalúe la posibilidad de exigir un reporte de la situación, así como las medidas implementadas por el tercero para evitar que esta situación vuelva a repetirse.
- En caso de contar con un seguro de riesgo cibernético, analizar las coberturas que podrían ser de utilidad en una situación como la expuesta.
- Al finalizar el incidente, realizar una sesión de lecciones aprendidas para entender lo que funcionó y lo que podría mejorarse en próximas situaciones.



¿Cómo puede ayudar Marsh?

Consultoría de Ciberseguridad

Principales servicios

Herramientas Especializadas

Estrategia y gobierno

- Diagnóstico de seguridad y ciberseguridad
- Desarrollo de la estrategia de ciberseguridad
- Diagnóstico de ciberseguridad ICS/SCADA
- Diagnóstico de ciberseguridad Cloud
- Diagnóstico de prevención del fraude digital
- Definición de políticas y procedimientos de seguridad de la información y ciberseguridad
- Definición del dashboard ejecutivo de ciberseguridad
- Tercerización de la Oficina de Seguridad
- Diagnóstico frente a ransomware

Gestión y cuantificación de riesgos

- Identificación y clasificación de activos de información
- Definición de la metodología cualitativa y cuantitativa de gestión de riesgos de seguridad de la información y ciberseguridad
- Evaluación de riesgos de seguridad de la información y ciberseguridad
- Cuantificación de la exposición al riesgo cibernético (CyberXQ, Cyber RFO, Marsh Blue[i] Cyber)

Desarrollo seguro de software

- Desarrollo de la metodología de desarrollo seguro de software
- Capacitación de desarrollo seguro
- Revisión de seguridad en el código fuente
- Web & Mobile Application Hacking

Cyber Risk Analytics

Cumplimiento

- Auditoría de Controles Generales de TI
- Evaluación de cumplimiento regulatorio
- Implementación de requerimientos regulatorios
- Diagnóstico de PCI DSS
- Desarrollo del diagrama de flujo de datos del tarjetahabiente (PCI DSS)
- Diagnóstico de Protección de Datos Personales
- Implementación del programa de privacidad

Gestión de riesgos con terceros

- Definición del marco de gestión de ciber-riesgos con terceros (TPRM - Cyber)
- Evaluación de riesgos de seguridad de la información y ciberseguridad con terceros
- Due-diligence de ciberseguridad para fusiones y adquisiciones (M&A)

Seguridad defensiva y ofensiva

- Ciberinteligencia (búsqueda de información fugada en Internet)
- Gestión de vulnerabilidades
- Revisión de la configuración de ciberseguridad (hardening)
- Pruebas controladas de intrusión (ethical hacking)
- Web & Mobile Application Hacking
- Pruebas de ingeniería social
- Pruebas de red team

Cultura de ciberseguridad

- Cyber Chemistry – Evaluación de cultura de ciberseguridad
- Desarrollo del programa de concientización en ciberseguridad
- Capacitaciones especializadas en ciberseguridad
- Evaluación de las capacidades del equipo de Seguridad de la Información y Ciberseguridad*

Seguro de riesgo cibernético

- Autoevaluación de madurez de ciberseguridad para el seguro de riesgo cibernético*
- Cyber IDEAL - Estimación de pérdidas para el seguro (brecha de privacidad, ransomware y lucro cesante de un ciberataque)*
- Cybersecurity Rating (BitSight y SecurityScorecard)*
- Evaluación de riesgos para el seguro cyber
- Contratación del seguro de riesgo cibernético*
- Cyber Claims & Crisis Orchestration (soporte en el reclamo de siniestros cyber)

Gestión de incidentes

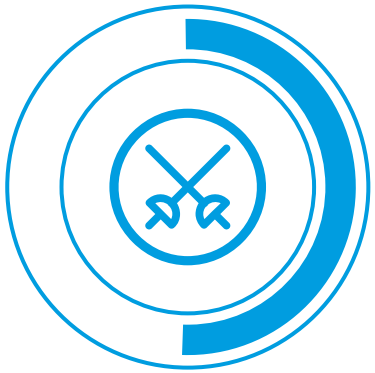
- Respuesta ante ciberincidentes
- Desarrollo del plan de respuesta ante ciberincidentes y playbooks
- Desarrollo del protocolo organizacional frente a casos de ransomware
- Ejercicios de escritorio de ciber-crisis y del plan de respuesta ante ciberincidentes
- Desarrollo del plan de mejoras post-incidente

Cyber Incident Management

Principales servicios

PREVENCIÓN

- Evaluación de las capacidades de respuesta ante ciberincidentes.
- Desarrollo del Plan de Respuesta ante Ciberincidentes y Playbooks.
- Desarrollo del protocolo de respuesta organizacional frente a ransomware.
- Desarrollo del plan de recuperación tecnológica en caso de ransomware.
- Entrenamiento en gestión de cibercrisis.
- Implementación de Cygnvs.
- Evaluación y remediación de riesgos en la superficie de ataque (ASM).
- Cyber Threat Hunting.



PRUEBA

- Simulación de cibercrisis a nivel del Comité de Crisis.
- Simulación de respuesta ante ciberincidentes a nivel táctico/operativo.
- Pruebas de Red Team.
- Simulación de adversarios y malware.

RESPUESTA

- Respuesta ante ciberincidentes, incluyendo:
  - Gestión de cibercrisis
  - Recomendación de terceros (p.e. firmas legales, empresas de relaciones públicas, centrales de monitoreo, etc.)
  - Análisis forense digital
  - Ciberinteligencia
  - Cyber Threat Hunting
  - Entre otros

POST

- Cyber Claims.
- Taller de lecciones aprendidas.
- Cyber Threat Hunting.
- Implementación de mejoras de seguridad.

Visita nuestro centro de recursos de respuesta ante incidentes cibernéticos

Contactos

Para conocer cómo podemos apoyar a su organización en la gestión del riesgo cibernético, póngase en contacto con nuestros profesionales.

Gerardo Herrera

Director de Marsh Advisory para Latinoamérica
Marsh Advisory
Gerardo.Herrera@Marsh.com

Ángela Cubillos

Líder de Consultoría en Riesgo Cibernético para Colombia
Marsh Advisory
Angela.Cubillos@Marsh.com

Edson Villar

Líder de Consultoría en Riesgo Cibernético para Latinoamérica
Marsh Advisory
Edson.Villar@Marsh.com

Alberto Martínez

Líder de Consultoría en Riesgo Cibernético para México
Marsh Advisory
Alberto.Martinez01@Marsh.com

Diego Godoy

Líder de Consultoría en Riesgo Cibernético para Perú
Marsh Advisory
Diego.Godoy@Marsh.com

André Gomes

Líder de Consultoría en Riesgo Cibernético para Brasil
Marsh Advisory
Andre.Gomes@Marsh.com

A business of Marsh McLennan