Canal de Primera Respuesta a ataques cibernéticos

¿Cómo reaccionar a un ataque cibernético?

La póliza de Seguro de Protección de Datos de AIG CyberEdge®, resguarda su patrimonio ante reclamaciones de terceros por violación de seguridad de datos personales y corporativos, entre otras coberturas exclusivas.

Siempre que el asegurado tenga conocimiento de una reclamación de terceros o algún incidente interno dentro de las coberturas incluidas en su póliza, debe avisar de inmediato y activar el **Canal de Primera Respuesta** para tomar acción y notificar a AIG de los eventos.

Canal de Primera Respuesta

Considerando la urgencia de los eventos cibernéticos y la importancia de atenderlos con rapidez, siendo asegurado AIG CyberEdge®, ponemos a su disposición un **Canal de Atención de Primera Respuesta** ante incidentes de seguridad de la información que puede ser accionado en las siguientes situaciones:

Emergencia cibernética

- Extorsión cibernética.
- Ataque en curso.
- Supuesta violación de seguridad que esté causando daños a la operación del asegurado.
- Emergencia cibernética donde exista la posibilidad de contener un ataque o mitigar impactos causados por la violación.

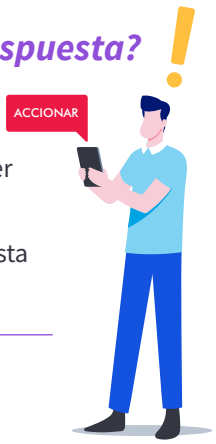
Aviso de siniestro o expectativa de siniestro

- Incidente ocurrido que ya ha generado impactos en consecuencia de una emergencia cibernética.
- Circunstancias previas de un incidente donde el asegurado esté sin posibilidades ni capacidades de accionar planes para contener los impactos.

El **Canal de Primera Respuesta** a incidentes estará disponible 24/7 los 365 días del año y ofrece a los asegurados atención de **nivel 1** del **CYBER INTELIGENCE CENTER de DELOITTE.**

¿Cómo accionar el Canal de Primera Respuesta?

800 999 2038



Durante la activación, la comunicación y documentación deberá ser compartida por email a **cyber_aig@deloittemx.com**

Este canal está operado por Deloitte México, líder global en respuesta a incidentes de ciberseguridad.

Validación

El equipo de Deloitte validará algunas informaciones para iniciar la activación del nivel 1:

- Nombre o razón social del asegurado/contratante de la póliza
- Número de póliza
- Vigencia de la póliza
- Nombre completo y cargo del solicitante
- Correo electrónico y teléfono de contacto del solicitante

Es importante que la persona que active el Canal de Primera Respuesta sea un representante legítimo de la empresa. Se requiere que el solicitante tenga conocimiento de la infraestructura tecnológica de información y telecomunicaciones, arquitectura de seguridad y procesos del negocio del asegurado de modo de ofrecer información certera a Deloitte para una atención más efectiva del incidente de acuerdo con la definición de nivel 1.

Atención del nivel 1

a. Durante la atención del nivel 1 el agente de Deloitte identificará el tipo de incidente y brindará asesoría remota con el fin de que el asegurado minimice los impactos de posibles violaciones de seguridad de la información o ataques en curso. El agente de Deloitte resolverá incidentes que tengan solución dentro del nivel 1 limitado a un periodo de 8 horas. En caso de identificarse dentro de las 8 horas límite que el incidente requiere una investigación más detallada para ser solucionado, este podrá ser escalado al nivel 2.

b. **La atención de nivel 1 es realizada con scripts técnicos enfocados a los principales riesgos que afectan al mercado como:**

- *Ransomware*, intrusión en sistemas operativos *(red hat/windows)*, denegación de servicio, escalación de privilegios, fuga de información, *phishing*, *business email compromise*, entre otros.

c. **Como resultado del nivel 1 será proporcionado por Deloitte un reporte sobre lo ocurrido que contendrá:**

- Fechas en la que se reportó y ocurrió el incidente
- Descripción de lo ocurrido
- Tipo de incidente
- Partes involucradas durante el incidente (empleados, proveedores, socios, etc.)
- Acciones de mitigación y corrección aplicadas
- Dispositivos y segmentos de red afectados
- Necesidades de involucramiento de otras áreas
- Acciones iniciales recomendadas al asegurado

Sí ← ¿Fue resuelto? → No

Cierre de la atención del Canal de Primera Respuesta

Atención de nivel 2

a. Cuando quede constatada la necesidad de atención a nivel 2 debido a una violación de seguridad verificada, el asegurado cuenta con libertad de escoger a los proveedores de servicio de atención y no está obligado a utilizar cualquier empresa sugerida por AIG.

b. En caso de que el asegurado haya utilizado el Canal de Primera Respuesta de AIG y opte por continuar los servicios de nivel 2 con otro proveedor que no sea Deloitte, toda la información recabada durante el nivel 1 quedará disponible al proveedor de elección del asegurado con la aprobación previa correspondiente.

Los siguientes pasos pueden ser determinantes para las necesidades de accionar el nivel 2:

- Complejidad del incidente reportado
- Imposibilidad de accionar o ejecutar las recomendaciones del agente de Deloitte
- Falta de información del ambiente afectado
- Falta de *logs* relacionados con el segmento afectado por el ataque, por ejemplo:

- Dimensión de los daños causados
- Paralización de unidades de negocio del asegurado
- Exposición al incidente
- Daños de privacidad de terceros
- En general, situaciones donde claramente exista la necesidad de involucrar más áreas o proveedores de diferentes servicios dentro de las coberturas del seguro

Accionando el **nivel 2**, AIG formará un **Comité de Crisis** con representantes de las siguientes partes involucradas:

- Asegurado y corredor
- AIG (equipo de siniestro y sucripción)
- Deloitte (en caso de que el asegurado escoja al proveedor)
- Otros proveedores de servicio de acuerdo a la naturaleza del incidente (relaciones públicas, abogados, etc.)

El Canal de Primera Respuesta a ataques cibernéticos indicado en el presente documento es aplicable para el producto denominado CyberEdge® registrado ante la Comisión Nacional de Seguros y Fianzas bajo el número CNSF-S0012-0315-2012 de fecha 31 de julio de 2012.