

Guía de tu seguro Data Protect

Con esta guía, tendrás a la mano todo lo que necesitas saber para sacar el máximo provecho de tu seguro.



Coberturas principales de tu seguro



Respuesta a Incidentes

Cubre los gastos inmediatos para contener y gestionar un incidente cibernético.



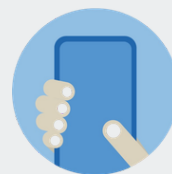
Pérdidas Propias

Protege a la empresa por daños directos a su operación.



Responsabilidad Civil por Privacidad y Seguridad

Cubre demandas de terceros por filtración de datos personales.



Responsabilidad por Publicación Electrónica

Cubre reclamos por contenido publicado en sitios web, redes sociales o plataformas digitales.

Atención a clientes

En el Centro de Atención Zurich estamos para atenderte.

Reporta tus siniestros, cotiza, recibe información ó paga tu póliza

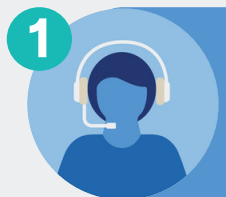
Horario de atención para seguimiento: lunes a viernes de 8:00 a 20:00 hrs., y sábado de 9:00 a 15:00 hrs.

Recibimos reportes de siniestro las 24 horas.

 ***9191**

 **800 288 6911**

¿Qué hacer en caso de siniestro?



1

Reporta tu incidente marcando al
***9191 o al 800 288 6911.**

Una vez que hagas tu reporte, uno de nuestros ajustadores te contactará para asistirte.



3

El ajustador brindará atención a tu siniestro y te solicitará documentación necesaria.



2

Tu ajustador te dará el número de siniestro y creará un grupo de WhatsApp contigo para agilizar el seguimiento.



4

Una vez confirmado que el reclamo procede, se firmará un convenio y se gestionará la solicitud del reembolso. El ajustador te confirmará una vez se realice tu pago.

En Zurich aseguramos tu vida, auto, hogar y mucho más

¿Qué documentos necesitas para dar seguimiento a un siniestro?

Data Protect



Estos son los documentos que necesitas para reportar un siniestro. Es importante mencionar que los documentos requeridos pueden cambiar dependiendo de las circunstancias específicas de tu caso.

1. **Reclamación formal dirigida a la aseguradora**, con monto total y desglose de conceptos.
2. **Reportes forenses IT**: descripción de hechos, tipo de ataque, punto de compromiso, cronología.
3. **Información de seguridad**: dispositivos y software del asegurado.
4. **Servidores/sistemas afectados** y explicación de cómo se vulneraron.
5. **Proveedores contratados**: contratos, reportes, entregables y bitácoras de actividades.
6. **Soporte de gastos**: facturas, comprobantes de pago y evidencia adicional.
7. **Acciones correctivas** aplicadas para restaurar la operación.
8. **Facturas y bitácoras** de proveedores de servicios.
9. **Evaluación de información afectada**: datos personales/confidenciales, tipo de información, tamaño de bases, nacionalidad, relación con asegurado, medidas de seguridad.
10. **Denuncia penal ante Ministerio Público**, con carpeta de investigación y anexos.
11. **Notificaciones legales/regulatorias**: titulares de datos, autoridades de protección, evidencia de notificaciones.
12. **Reclamaciones de terceros**: recibidas o potenciales relacionadas con el incidente.
13. **Cuantificación del daño (interrupción de negocios)**: soporte contable/financiero, facturas, cronología de impacto, reinicio de operaciones, declaraciones fiscales, constancias SAT.
14. **Estados de resultados mensuales**.



Esta es información general.
Si es necesario, podrían solicitarse más documentos.
Para más detalles, escanea el código QR.