Cuestionario Zurich sobre Riesgos Cibernéticos

Este cuestionario está dirigido a las organizaciones del sector de las grandes empresas. Favor de responder todas las preguntas.

El cuestionario y los anexos deben ser cumplimentados, firmados y fechados por un representante debidamente autorizado del solicitante/titular del seguro que tenga los conocimientos y la información necesaria.

Este documento sólo constituye una solicitud de seguro y, por tanto, no representa garantía alguna de que la misma será aceptada por la Compañía de Seguros, ni de que, en caso de aceptarse, la aceptación concuerde totalmente con los términos de la solicitud.

Usted entiende que debe comunicarnos todos los hechos y circunstancias que puedan ser importantes para los riesgos cubiertos por la póliza de forma clara y accesible y no debe tergiversar ningún hecho importante. Un hecho material es aquel que podría influir en nuestra aceptación o evaluación del riesgo. Si tiene alguna duda sobre hechos considerados materiales, es conveniente revelarlos. Si no hace una presentación justa del riesgo, la póliza puede evitarse, suscribirse en condiciones diferentes o cobrarse una prima más alta, dependiendo de las siguientes circunstancias de la falta de presentación equitativa del riesgo.

De acuerdo a los Artículos 8 y 47 de la Ley Sobre el Contrato de Seguro, el solicitante debe declarar todos los hechos importantes para la apreciación del riesgo que tengan referencia a esta solicitud, como los conozca, o deba conocer al momento de firmar la misma, en la inteligencia de que la no declaración, la inexacta o falsa declaración de los hechos importantes podría originar la pérdida de los derechos del asegurado o beneficiario en su caso.

1. Información general

Nombre completo de la empresa

Dirección

Código postal, lugar

País

Año de creación

Ingresos del ejercicio anterior	01.01. - 31.12.		(aaaa)	USD[1]
Año de vencimiento previsto (actual)	01.01. - 31.12.		(aaaa)	USD[1]
Ingresos previstos (próximo año)	01.01. - 31.12.		(aaaa)	USD[1]

[1] USD: Dólares de los Estados Unidos de América.

Territorio	Reparto porcentual de los ingresos
País de origen	
Reino Unido	
Europa	
EE.UU.	
Australia/Nueva Zelanda	
Resto del mundo	

Número de empleados

Número de empleados en TI[2]

Número de empleados en ciberseguridad

Presupuesto de TI de la Compañía (anual) USD

Presupuesto de ciberseguridad (anual) USD

¿Se ha adquirido, fusionado o consolidado alguna otra empresa con el solicitante en los dos últimos años?
☐ Sí ☐ No
(en caso afirmativo, facilitar detalles a continuación)

Nombre de la Compañía

Fecha de adquisición (dd/mm/aaaa)

Volumen de negocio (últimos 12 meses) USD

Actividad empresarial distinta de la de la compañía adquirente

¿Se ha completado toda la integración informática? ☐ Sí ☐ No
(si no es así, facilite detalles a continuación)

2. Interrupción de la actividad

2.1 Sistemas informáticos internos:

¿Cuánto tiempo pueden sobrevivir sus procesos empresariales sin sistemas de TI críticos?

- ☐ Todos los procesos empresariales pueden sobrevivir una semana sin sistemas de TI críticos.
- ☐ La mayoría de los procesos empresariales pueden sobrevivir al menos una semana sin sistemas de TI críticos.
- ☐ La mayoría de los procesos empresariales pueden sobrevivir al menos un día, pero menos de una semana sin de TI internos críticos.
- ☐ La mayoría de los procesos empresariales pueden sobrevivir un día sin sistemas de TI críticos.

[2] TI: Tecnologías de la Información.

¿Cuál es el efecto esperado en los ingresos si un sistema de IT interno crítico sufre una interrupción de 24 horas?

☐ Impacto mínimo previsto si un sistema de TI interno se interrumpe durante 24 horas.
☐ Impacto moderado si un sistema de TI interno se interrumpe durante 24 horas.
☐ Se espera un impacto mayor si un sistema de TI interno se interrumpe durante 24 horas.

Favor de indicar el importe estimado USD

7 días:
☐ Impacto mínimo previsto si un sistema de TI interno se interrumpe durante 7 días.
☐ Impacto moderado si un sistema de TI interno se interrumpe durante 7 días.
☐ Se espera un impacto mayor si un sistema de TI interno se interrumpe durante 7 días.

Favor de indicar el importe estimado USD

2.2 Sistemas de Tecnología de la Información (TI) de terceros Proveedores de Servicios de TI:

¿Cuánto tiempo pueden sobrevivir sus procesos empresariales sin sistemas de TI crítico subcontratado?

☐ Todos los procesos empresariales pueden sobrevivir una semana sin sistemas de TI externos críticos.
☐ La mayoría de los procesos empresariales pueden sobrevivir al menos una semana sin sistemas informáticos externos críticos.
☐ La mayoría de los procesos empresariales pueden sobrevivir al menos un día pero menos de una semana sin sistemas de TI externos críticos.
☐ La mayoría de los procesos empresariales pueden sobrevivir un día o ninguno sin sistemas de TI externos críticos.

¿Cuál es el efecto esperado sobre los ingresos si un proveedor de TI crítico sufre una interrupción de: 24 horas:

☐ Impacto mínimo previsto si un proveedor de TI crítico se interrumpe durante 24 horas.
☐ Se espera un impacto moderado si un proveedor de TI crítico se interrumpe durante 24 horas.
☐ Se espera un impacto mayor si un proveedor de TI crítico se interrumpe durante 24 horas.

Favor de indicar el importe estimado USD

7 días:
☐ Impacto mínimo previsto si un proveedor de TI crítico se interrumpe durante 7 días.
☐ Se espera un impacto moderado si un proveedor de TI crítico se interrumpe durante 7 días.
☐ Se espera un impacto mayor si un proveedor de TI crítico se interrumpe durante 7 días.

Favor de indicar el importe estimado USD

2.3 Sistemas de Tecnología de la Información (TI) de terceros No Proveedores de Servicios Informáticos:

¿Cuánto tiempo pueden sobrevivir sus procesos empresariales sin acceso a un Sistema Informático de un Proveedor de Servicios que no sea de TI (por ejemplo, su proveedor principal)?

- ☐ Todos los procesos empresariales pueden sobrevivir una semana sin acceso a los Sistemas de TI de un Proveedor de Servicios que no sea del área.
- ☐ La mayoría de los procesos empresariales pueden sobrevivir una semana sin acceso a los Sistemas de TI de un Proveedor de Servicios que no sea de TI.
- ☐ La mayoría de los procesos empresariales no pueden sobrevivir días sin acceso a los los Sistemas de TI de un Proveedor de Servicios que no sea de TI.
- ☐ La mayoría de los procesos empresariales no pueden sobrevivir horas sin acceso a los los Sistemas de TI de un Proveedor de Servicios que no sea de TI.

¿Cuál es el efecto esperado sobre los ingresos si un proveedor que no es de TI se enfrenta a una interrupción de 24 horas?

- ☐ Se prevé una pérdida mínima de beneficios si un proveedor que no sea de TI sufre una interrupción de hasta 24 horas.
- ☐ Se prevé una pérdida de beneficios moderada si un proveedor que no sea de TI es interrumpido de hasta 24 horas.
- ☐ Se espera una pérdida de beneficios mayores si un proveedor no informático es interrumpido de hasta 24 horas.

Favor de indicar el importe estimado USD _____

7 días:

- ☐ Impacto mínimo previsto si un proveedor que no es de TI es interrumpido durante 7 días.
- ☐ Impacto moderado si un proveedor no es de TI es interrumpido durante 7 días.
- ☐ Se espera un impacto mayor si un proveedor no es de TI es interrumpido durante 7 días.

Favor de indicar el importe estimado USD _____

3. Sector industrial (Marque la casilla correspondiente)

- ☐ Servicios de Alojamiento y Alimentación
- ☐ Servicios Administrativos y de Apoyo y Gestión de Residuos y Servicios de Saneamiento
- ☐ Agricultura, Silvicultura, Pesca y Caza
- ☐ Artes, Entretenimiento y Ocio
- ☐ Construcción
- ☐ Servicios educativos
- ☐ Energía
- ☐ Finanzas y Seguros
- ☐ Asistencia sanitaria y social
- ☐ Información
- ☐ Gestión de Sociedades y Empresas
- ☐ Fabricación
- ☐ Minas, Canteras y Extracción de Petróleo y Gas
- ☐ Servicios Profesionales, Científicos Técnicos
- ☐ Administración Pública
- ☐ Bienes Inmuebles y Arrendamiento Comercio Minorista
- ☐ Transporte y Almacenamiento
- ☐ Servicios Públicos
- ☐ Comercio Mayorista
- ☐ Otros: _____

Describir brevemente su actividad empresarial

4. Exposición de Datos

4.1 Cuántos registros de datos personales u otros datos protegidos recopila, procesa o almacena?

	Ninguno	<10'000	<100'000	<1 millón	<10 millones	>10 millones
Información Personal Identificable (IPI)	☐	☐	☐	☐	☐	☐
Información Sanitaria Personal (PHI)	☐	☐	☐	☐	☐	☐
Información Personal sobre Tarjetas de Crédito (PCI)	☐	☐	☐	☐	☐	☐
Otros	☐	☐	☐	☐	☐	☐

4.2 ¿La organización almacena, procesa o transmite datos clasificados gubernamentales? ☐ Sí ☐ No

4.3 ¿La organización almacena, procesa o transmite datos de tarjetas de pago? ☐ Sí ☐ No

4.4 ¿Utiliza o proporciona la organización tecnología que escanea identificadores biométricos (huellas dactilares, faciales, voz, iris, etc.)? ☐ Sí ☐ No

4.5 ¿Se considera la organización una Entidad Cubierta por la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) y la Ley de Tecnología de la Información Sanitaria para la Salud Económica y Clínica (HITECH)? ☐ Sí ☐ No

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

5. Proveedor de Servicios Externo

¿Qué proveedor de servicios en la nube utiliza la organización? Seleccione todos los que correspondan:

☐ Microsoft ☐ Amazon

☐ Google ☐ Otros: _____

¿Qué procesos/sistemas empresariales clave se subcontratan a terceros? Seleccione todos los que corresponda.

- ☐ Microsoft 365 (Office + AD) Aplicaciones de productividad
- ☐ Procesamiento/Almacenamiento de Datos
- ☐ Planeación de Recursos Empresariales (ERP)
- ☐ Servicios de Recuperación de Desastres
- ☐ Sistema de Recursos Humanos

- ☐ Procesamiento de Pagos y Transacciones Gestión de Relaciones con los Clientes (CRM)
- ☐ Gestión de Riesgos de Terceros (TPRM)
- ☐ Servicio de Seguridad Gestionada (MSSP) / Centro de Operaciones de Seguridad (SOC)
- ☐ Operaciones de TI
- ☐ Compartición de archivos
- ☐ Otros: _____

Enumerar sus proveedores de TI, Proveedores de Servicios en la Nube y Subcontratistas de Procesos Empresariales más importantes junto con los servicios que prestan (por ejemplo, Servicios Gestionados de Seguridad, Alojamiento en la Nube/Respaldos de Seguridad/Alojamiento Sitios de la Web, Proveedores de Servicios de Internet, Proveedores de Software Crítico para las Empresas, Procesadores de Datos, Proveedores de Hardware para Puntos de Venta (PoS), Servicios de Colocación, Procesamiento de Pagos/Transacciones):

Proveedor	Servicio

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicar a continuación:

6. Exposición a la Tecnología

6.1	¿La organización utiliza y gestiona sistemas de usuario final (computadora, portátiles, de escritorio, dispositivos móviles, tabletas, etc.)?	☐ Sí	☐ No
6.2	¿La organización utiliza o gestiona terminales (cajeros automáticos, quioscos, terminales de pago, etc.)?	☐ Sí	☐ No
6.3	¿La organización utiliza o gestiona medios extraíbles (dispositivos de almacenamiento tipo USB, discos duros externos, etc.)?	☐ Sí	☐ No
6.4	¿La organización utiliza o gestiona Dispositivos Sanitarios (incluyendo sistemas de soporte vital, goteros de insulina, sistemas de monitorización de la salud, etc.)?	☐ Sí	☐ No
6.5	¿La organización utiliza o gestiona dispositivos críticos de Internet de las Cosas (IoT) (cerraduras / accionadores de puertas, detectores de humo, etc.)?	☐ Sí	☐ No

6.6 ¿La organización utiliza o gestiona Tecnología Operativa (por ejemplo, máquinas industriales, sistemas de control, etc.)? ☐ Sí ☐ No

(en caso afirmativo, completar el cuestionario complementario sobre tecnología operativa, 8.1)

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7. Cuestionario de Seguridad de la Información

7.1 Dirección de la Organización

7.1.1 La organización mantiene una política formal de Seguridad Informática/Cibernética con procedimientos definidos para todas las operaciones (idealmente gestionados de forma centralizada). ☐ Sí ☐ No ☐ Parcial

7.1.2 Se establece un puesto de liderazgo dedicado a la ciberseguridad (por ejemplo, un Director Parcial de Seguridad de la Información, CISO). Esta persona se compromete activamente con los principales responsables de la toma de decisiones dentro de la organización para priorizar y obtener la aprobación de las iniciativas de seguridad. ☐ Sí ☐ No ☐ Parcial

7.1.3 Se establece en la compañía una función específica para la protección de datos (Responsable de Protección de Datos, DPO/Director de Producto, CPO). ☐ Sí ☐ No ☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.2 Estrategia y Procesos de Gestión de Riesgos Cibernéticos

7.2.1 Las evaluaciones de los riesgos de seguridad se realizan al menos una vez al año, ya sea internamente o por un tercero independiente ☐ Sí ☐ No ☐ Parcial.

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación:

7.3 Conformidad y Certificaciones

7.3.1	La organización cuenta con una certificación activa del Sistema de Gestión de Seguridad de la Información (SMS) (por ejemplo, ISO27001).	☐ Sí	☐ No	☐ Parcial
7.3.2	Se requiere que la organización cumpla los Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard, PCI-DSS).	☐ Sí	☐ No	☐ Parcial
7.3.3	La empresa cumple la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) y está certificada.	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.4 Gestión de activos

7.4.1	Se mantiene un inventario centralizado de hardware. (Si el inventario está automatizado mediante la exploración de descubrimientos en tiempo real, responda "sí, avanzado")	☐ Sí	☐ No	☐	☐ Sí, Parcial avanzado
7.4.2	Se mantiene un inventario centralizado de software. (Si el inventario está automatizado mediante la exploración de descubrimientos en tiempo real, responda "sí, avanzado")	☐ Sí	☐ No	☐	☐ Sí, Parcial avanzado
7.4.3	Se mantiene un inventario de datos centralizado y los activos de datos se etiquetan de acuerdo con las normas de clasificación de datos. (Si el inventario está automatizado mediante el escaneo de descubrimiento en tiempo real, responder "sí, avanzado").	☐ Sí	☐ No		☐ Sí, Parcial avanzado
7.4.4	En los últimos dos años se ha llevado a cabo un Análisis de Impacto en el Negocio (BIA) formal para comprender la criticidad y las dependencias de todos los sistemas.	☐ Sí	☐	☐ No	☐ Parcial
7.4.5	Se definen Objetivos de Tiempo de Recuperación (RTO) y Objetivos de Punto de Recuperación (RPO) para los sistemas críticos y sus sistemas dependientes. **Especificar los plazos establecidos:**	☐ Sí	☐	☐ No	☐ Parcial

7.4.6 La organización tiene una lista de activos de toda la Tecnología Operativa (OT) / Sistemas de Control Industrial (ICS) que se conectan a la red y se mantienen.
(si procede, completar el cuestionario complementario sobre tecnología operativa, 8.1)

☐ N/A ☐ Sí ☐ No

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.5 Gestión de Proveedores

7.5.1	Los terceros con acceso a la red de la organización y/o a datos sensibles se someten a una evaluación de riesgos antes de su incorporación y están sujetos a requisitos contractuales de ciberseguridad y responsabilidad.	☐ Sí	☐ No	☐ Parcial
7.5.2	Los terceros esenciales son controlados y auditados periódicamente.	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.6 Gestión de Identidades y Accesos

7.6.1	Los administradores disponen de cuentas separadas y privilegiadas para tareas administrativas que no se utilizan para acceder a Internet y al correo electrónico.	☐ Sí	☐ No	☐ Parcial
7.6.2	Las cuentas privilegiadas son escalonadas/únicas para diferentes tipos de sistemas (por ejemplo, controladores de dominio, endpoints, servidores y aplicaciones).	☐ Sí	☐ No	☐ Parcial
7.6.3	Una solución de Administración de Acceso Privilegiado (PAM) es desplegada y/o el acceso requiere el uso de una Estación de Trabajo de Acceso Privilegiado (PAW).	☐ Sí	☐ No	☐ Parcial
7.6.4	La Autenticación Multifactor (MFA) se aplica a todas las cuentas privilegiadas.	☐ Sí	☐ No	☐ Parcial
7.6.5	El acceso remoto a la red corporativa se obtiene a través de un canal cifrado (por ejemplo, una red privada virtual, VPN) y requiere autenticación multifactor (MFA).	☐ Sí	☐ No	☐ Parcial
7.6.6	La autenticación multifactor (AMF) es necesaria para acceder a las aplicaciones críticas de Internet.	☐ Sí	☐ No	☐ Parcial
7.6.7	Los derechos de acceso administrativo se revisan y recertifican al menos una vez al año. (Si las revisiones son más frecuentes y/o se implementa una herramienta de gestión de acceso privilegiado, PAM, responda “sí, avanzado”)	☐ Sí	☐ No	☐ Parcial
7.6.8	Los derechos de acceso se establecen utilizando el «principio del menor privilegio».	☐ Sí	☐ No	☐ Parcial
7.6.9	Las Cuentas de Administración local se gestionan de forma centralizada (por ejemplo, mediante Local Administrator Password Solution, LAPS) y se desactivan por omisión en los dispositivos de los usuarios finales.	☐ Sí	☐ No	☐ Parcial
7.6.10	El inicio de sesión interactivo está denegado para las cuentas de servicio.	☐ Sí	☐ No	☐ Parcial
7.6.11	El acceso al entorno de copia de seguridad requiere credenciales que no sean de Active Directory (AD) y autenticación por factores (MFA), o el uso de credenciales almacenadas en una solución de Gestión de Acceso Privilegiado (PAM).	☐ Sí	☐ No	☐ Parcial
7.612	Las credenciales de las cuentas de servicio privilegiadas se rotan al menos una vez al año. (Si se despliega una herramienta de Gestión de Acceso Privilegiado, PAM, y se incorporan cuentas de servicio, responda ”sí, avanzado”)	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.7 Seguridad de los datos

7.7.1	Todas las copias de seguridad están encriptadas.	☐ Sí	☐ No	☐ Parcial
7.7.2	Se han implementado controles de Prevención de Pérdida de Datos (DLP) en Endpoint. (Si está en modo de bloqueo, responda "sí, avanzado")	☐ Sí	☐ No	☐ Parcial
7.7.3	La Autenticación Multifactor (MFA) es necesaria para acceder a información crítica/sensible.	☐ Sí	☐ No	☐ Parcial
7.7.4	Los entornos de desarrollo, pruebas y preproducción no utilizan datos vivos/sensibles.	☐ Sí	☐ No	☐ Parcial

7.7.5	La empresa sigue procedimientos de conservación y destrucción de datos para toda la información sensible.	☐ Sí	☐ No	☐ Parcial
7.7.6	Los datos sensibles en reposo se cifran utilizando protocolos de cifrado compatibles.	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.8 Seguridad del Sistema

7.8.1	Todos los respaldos están encriptados.	☐ Sí	☐ No	☐ Parcial
7.8.2	Los respaldos de seguridad se almacenan sin conexión y/o en una red segmentada.	☐ Sí	☐ No	☐ Parcial
7.8.3	Todos los sistemas operativos están reforzados siguiendo las configuraciones de sistemas recomendadas (por ejemplo, Microsoft Security Baselines).	☐ Sí	☐ No	☐ Parcial
7.8.4	Se documenta y sigue el Ciclo de Vida de Desarrollo Seguro (SDLC) (incluyendo pruebas de penetración antes de la liberación en producción y desarrollo, las pruebas y los entornos de pre-producción no utilizan datos en vivo/sensibles).	☐ Sí	☐ No	☐ Parcial
7.8.5	Los entornos de desarrollo, pruebas y preproducción están separados de la red corporativa.	☐ Sí	☐ No	☐ Parcial
7.8.6	La evaluación de la configuración basada en los puntos de referencia del Centro para la Seguridad en Internet (CIS) se realiza regularmente.	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.9 Seguridad de Redes y Comunicaciones

7.9.1	Una solución de seguridad del correo electrónico sirve para filtrar el spam, los intentos de phishing y los contenidos maliciosos.		☐ Sí	☐ No	☐ Parcial
7.9.2	Se ha implementado la funcionalidad Sandboxing para inspeccionar objetos adjuntos y enlaces de correo electrónico sospechosos en un entorno de pruebas aislado.		☐ Sí	☐ No	☐ Parcial
7.9.3	Los sitios web maliciosos son bloqueados por una solución proxy/filtro que se actualiza regularmente.		☐ Sí	☐ No	☐ Parcial
7.9.4	Se implementan cortafuegos y/o Sistemas de Detección y prevención de intrusiones (IDS/IPS) para gestionar las conexiones de red entrantes/salientes.		☐ Sí	☐ No	☐ Parcial
7.9.5	El sitio web de la organización y los sistemas orientados a Internet están protegidos por un cortafuegos de aplicaciones web (WAF). (Si el sitio web no se utiliza para generar ingresos, responda "N/A").	☐ N/A	☐ Sí	☐ No	☐ Parcial
7.9.6	Existen Sistemas Adecuados[3] de Prevención de Denegación de Servicio Distribuido (DDoS). (por ejemplo, AWS Shield, Cloudflare, NETSCOUT Arbor DDoS Protection, etc.)		☐ Sí	☐ No	☐ Parcial
7.9.7	El acceso a recursos corporativos desde dispositivos personales (Bring Your Own Device, BYOD) es restringido o administrado usando una solución de Administración de Dispositivos Móviles (MDM).		☐ Sí	☐ No	☐ Parcial
7.9.8	Los activos legados o al Final de su Vida Útil (EOL) están convenientemente segmentados de la red corporativa.	☐ N/A	☐ Sí	☐ No	☐ Parcial
7.9.9	La red está segmentada/micro-segmentada utilizando un enfoque basado en riesgos (es decir, sistemas críticos, datos sensibles y copias de seguridad críticas/sensibles).		☐ Sí	☐ No	☐ Parcial
7.9.10	Los sistemas de control industrial y la tecnología operativa están segmentados entre plantas, red corporativa e Internet.	☐ N/A	☐ Sí	☐ No	☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.10 Seguridad Operativa

7.10.1	Se realizan análisis mensuales de vulnerabilidades en la red interna y los sistemas conectados.	☐ Sí	☐ No	☐ Parcial
7.10.2	Existe una gestión centralizada de parches y los parches se despliegan dentro de los 30 días de su lanzamiento. Idealmente, esto se realiza utilizando una solución de parcheo automatizada.	☐ Sí	☐ No	☐ Parcial
7.10.3	La política de parches de emergencia se sigue tanto para los parches de Microsoft como para los que no son de Microsoft y se despliegan en un plazo de tres (3) días.	☐ Sí	☐ No	☐ Parcial

[3] Las siguientes soluciones se consideran sistemas adecuados de prevención de denegación de servicio distribuido (DDoS) (no exhaustivo):
- Una solución de un proveedor de servicios de telecomunicaciones;
- Una solución de Microsoft o de un proveedor en la nube (si la empresa está alojada en la nube o en una nube híbrida);
- Una solución de Microsoft o de un proveedor en la nube (si la empresa está alojada en la nube o en una nube híbrida);
- Una solución dedicada de un proveedor de protección contra la denegación de servicio distribuida (DDoS).

7.10.4	Se instala una solución de protección avanzada de puntos finales de buena reputación y respaldada por el proveedor en todos los puntos finales y servidores (por ejemplo, CrowdStrike Falcon, SentinelOne EDR, Microsoft Defender o Endpoint o Cynet EDR).	☐ Sí ☐ No ☐ Parcial
7.10.5	Las pruebas de penetración se llevan a cabo anualmente en toda la infraestructura crítica de cara al exterior. (Si se realiza el "purple teaming", responda "sí, avanzado")	☐ Sí ☐ No ☐ Parcial ☐ Sí avanzado
7.10.6	Los activos al final de su vida útil (EOL) se segmentan de la red corporativa y se adquiere soporte cuando está disponible.	☐ N/A ☐ Sí ☐ No ☐ Parcial
7.10.7	Se implementa una herramienta de Gestión de la Postura de Seguridad en la Nube (CSPM).	☐ Sí ☐ No ☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.11 Concienciación y Capacitación de los Usuarios

7.11.1	La capacitación en materia de seguridad es obligatoria para todos los empleados y terceros con acceso a la red corporativa en el momento de su contratación y, posteriormente, al menos una vez al año.	☐ Sí ☐ No ☐ Parcial
7.11.2	Se realizan ejercicios de simulación de phishing periódicamente. **Especificar la frecuencia a continuación**	☐ Sí ☐ No ☐ Parcial

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.12 Registro de Eventos y Generación de Alertas

7.12.1	Existe una solución de gestión de eventos e información de seguridad (SIEM).	☐ Sí ☐ No ☐ Parcial
7.12.2	La herramienta de gestión de eventos e información de seguridad (SIEM) está instalada e ingiere registros de la mayoría de los activos y tecnologías de protección de la organización (por ejemplo, puntos finales, servidores, dispositivos de red, cortafuegos, Gestión de Acceso Privilegiado, PAM, y Detección y	☐ Sí ☐ No ☐ Parcial ☐ Sí avanzado

Respuesta de Puntos Finales, EDR).
(Si el sistema de Gestión de Eventos e información de Seguridad, SIEM, ingiere registros de más del 80% de los activos, responder "sí, avanzado")

7.12.3	Los Registros de Tecnología Operacional (OT) son ingeridos por el SIEM (Security Information and Event Management). (si procede, completar el cuestionario complementario sobre tecnología operativa, 8.1)	☐ N/A	☐ Sí	☐ No	☐ Parcial	
7.12.4	La información sobre amenazas es regularmente recolectada y considerada como parte del Control de Organización de Servicios (SOC) / Detección y Respuesta Gestionada (MDR) (por ejemplo, Indicadores de Compromiso, IOC / Equipo de Respuesta a Emergencias Informáticas, CERT).		☐ Sí	☐ No	☐ Parcial	
7.12.5	Un Centro de Operaciones de Seguridad (SOC) que opera 24×7 es establecido internamente o subcontratado a un tercero (SOCaas/MDR). Los analistas están capacitados y autorizados para contener y remediar posibles incidentes de seguridad después su detección.		☐ Sí	☐ No	☐ Parcial	
7.12.6	La Organización cuenta con herramientas de seguridad (por ejemplo, Endpoint Detection and Response, EDR o Security Information and Event Management, SIEM) que proporcionan análisis de comportamiento.		☐ Sí	☐ No	☐ Parcial	

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.13 Respuesta a Ciberataques

7.13.1	La organización tiene un Plan de Respuesta a Incidentes (IRP) documentado.	☐ Sí	☐ No	☐ Parcial	
7.13.2	El Plan de Respuesta a Incidentes (IRP) contiene un escenario de ransomware.	☐ Sí	☐ No	☐ Parcial	
7.13.3	La organización tiene especialistas forenses internos o talento forense contratado.	☐ Sí	☐ No	☐ Parcial	
7.13.4	Los ejercicios de mesa para probar el Plan de Respuesta a Incidentes (IRP) y los libros de jugadas se realizan al menos una vez al año e incluyen la participación de actores clave.	☐ Sí	☐ No	☐ Parcial	

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

7.14 Recuperación después de ciberataques

7.14.1	La organización tiene un Plan de Recuperación de Desastres (DRP) documentado para guiar los esfuerzos de recuperación después de un incidente o desastre.	☐ Sí	☐ No	☐ Parcial	
7.14.2	*La recuperación de todas las copias de seguridad de los sistemas críticos se comprueba anualmente y cumple los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO), Objetivos de Tiempo de Recuperación (RTO) / Objetivos de Punto de Recuperación (RPO).*	☐ Sí	☐ No	☐ Parcial	
7.14.3	La organización tiene un Plan de Continuidad del Negocio (BCP) documentado para asegurar la continuación de las funciones críticas del negocio en caso de un incidente o desastre.	☐ Sí	☐ No	☐ Parcial	
7.14.4	Los ejercicios de mesa para probar el Plan de Continuidad del Negocio (BCP) se realizan al menos una vez al año e incluyen la participación de las partes interesadas clave.	☐ Sí	☐ No	☐ Parcial	
7.14.5	Se realizan copias de seguridad de los datos críticos de la empresa al menos una vez al día. (si las copias de seguridad son semanales o menos frecuentes, responder "parcial")	☐ Sí	☐ No	☐ Parcial	
7.14.6	La Organización escanea las copias de seguridad en busca de malware antes de restaurarlas.	☐ Sí	☐ No	☐ Parcial	

Si desea hacer algún comentario adicional sobre alguna pregunta o respuesta concreta de esta sección, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

8. Cuestionarios Complementarios

8.1 Tecnología Operativa (OT)

8.1.1	La organización tiene un presupuesto separado dedicado a la ciberseguridad de la Tecnología Operativa (OT).	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.2	A Se establece un puesto de liderazgo específico para la ciberseguridad de la Tecnología Operativa (OT).	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.3	El acceso remoto a los activos de Tecnología Operativa (OT) se obtiene a través de un canal cifrado (por ejemplo, red privada virtual, VPN) y requiere autenticación multifactorial (MFA).	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.4	La segmentación se despliega entre plantas/instalaciones de tecnología Operativa (OT)	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.5	Se mantiene un inventario completo y actualizado de los activos de Tecnología Operativa (OT).	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.6	Se segmentan los entornos de las Tecnología de la Información (TI) y la Tecnología Operativa (TO).	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.7	El entorno de la Tecnología Operativa (OT) se segmenta a partir de Internet.	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.8	El escaneo de vulnerabilidad de las redes de Tecnología Operacional (OT) se realiza regularmente.	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.9	Los activos de Tecnología Operativa (OT) se parchan según su criticidad.	☐ N/A	☐ Sí	☐ No	☐ Parcial	
8.1.10	Los registros de Tecnología Operacional (OT) son ingeridos por el SIEM (Security Information and Event Management).	☐ N/A	☐ Sí	☐ No	☐ Parcial	

8.1.11	El entorno de Tecnología Operacional (OT) es monitoreado por el Control de Organización de Servicios (SOC).	☐ N/A ☐ Sí ☐ No ☐ Parcial
8.1.12	En los últimos dos (2) años se ha llevado a cabo un ejercicio teórico de respuesta a incidentes específico para ciber amenazas de Tecnología Operativa (OT).	☐ N/A ☐ Sí ☐ No ☐ Parcial
8.1.13	Se realizan copias de seguridad de los sistemas de Tecnología Operativa (OT) al menos una vez al mes y cuando se realizan cambios significativos en el entorno/proceso.	☐ N/A ☐ Sí ☐ No ☐ Parcial
8.1.14	Las pruebas de restauración de las copias de seguridad de los sistemas de Tecnología Operativa (OT) se realizan con regularidad.	☐ N/A ☐ Sí ☐ No ☐ Parcial
8.1.15	Existe un Plan de Contingencia de Negocio (BCP) específico para la Tecnología Operativa (OT) y ha sido actualizado en los últimos dos (2) años.	☐ ☐ Sí ☐ No ☐ Parcial
8.1.16	Se realizan escaneos trimestrales de vulnerabilidad en la red de Tecnología Operacional (OT).	☐ N/A ☐ Sí ☐ No ☐ Parcial

8.2 Desarrollo de software

8.2.1	Un Ciclo de Vida de Desarrollo de Software/Sistema (SDLC) seguro está documentado e incluye estándares para pruebas de penetración, análisis de código, Pruebas de Aceptación de Usuario (UAT), planes de reversión, etc. El SDLC también prohíbe el uso de datos vivos/sensibles en entornos de desarrollo, pruebas y preproducción.	☐ N/A ☐ Sí ☐ No ☐ Parcial
8.2.2	Los entornos de desarrollo, pruebas y preproducción están segmentados de la red corporativa.	☐ N/A ☐ Sí ☐ No ☐ Parcial

8.3 Seguridad de los Datos del Sector de las Tarjetas de Pago (PCI-DSS)

8.3.1	La organización cuenta con la certificación de la Industria de Tarjetas de Pago (PCI) en el nivel adecuado, en función de la cantidad de transacciones procesadas al año. Si se utiliza un procesador de pagos externo, se obtienen y revisan informes de auditoría anuales para validar el cumplimiento de la PCI.	☐ N/A ☐ Sí ☐ No ☐ Parcial

8.4 Portabilidad y Responsabilidad de los Seguros Sanitarios (HIPAA)

8.4.1	La Información Sanitaria Personal (PHI) se protege y maneja de acuerdo con las normas de seguridad y privacidad de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).	☐ N/A ☐ Sí ☐ No ☐ Parcial

8.5 Datos Biométricos

8.5.1	Los datos biométricos están adecuadamente protegidos y la recopilación, tratamiento, conservación, almacenamiento, uso compartido, transferencia, eliminación, venta u otro uso de los datos biométricos cumple la legislación, norma, directiva, ordenanza, reglamento, disposición o derecho común aplicable que regula la recopilación, confidencialidad, acceso, control, divulgación, conservación, tratamiento, modificación, manipulación o uso de la información biométrica.	☐ N/A ☐ Sí ☐ No ☐ Parcial

Si hay algún comentario adicional sobre alguna pregunta o respuesta específica de la sección 8, indicarlo a continuación: (indicar el número de la pregunta a la que se refiere)

9.Historial del Solicitante

9.1 En los últimos tres años, ¿se ha rechazado al solicitante algún seguro cibernético similar o la aseguradora del solicitante ha cancelado algún seguro cibernético anterior? ☐ Sí ☐ No

9.2 ¿Ha sufrido su empresa o alguna filial alguna intrusión en el sistema, interrupción de la actividad, robo de datos u otras pérdidas de datos en los últimos cinco (5) años? ☐ Sí ☐ No

9.3 ¿Tiene usted, o algún otro miembro del Comité Ejecutivo o de la dirección, conocimiento de alguna circunstancia (por ejemplo, violación de datos) que pudiera dar lugar a una reclamación en relación con la cobertura de seguro solicitada? ☐ Sí ☐ No

En caso afirmativo, facilitar detalles sobre la fecha del incidente, descripción del mismo, estimación de pérdidas y/o costes, medidas inmediatas adoptadas y medidas adoptadas para evitar un siniestro similar.

Aviso de Privacidad

Al informar sus datos personales en este documento otorga su consentimiento para que los mismos se utilicen para fines relacionados al servicio prospectado o contratado conforme al aviso de privacidad cuyo texto completo está en www.zurich.com.mx

Entrega de Documentación Contractual

En caso de que el riesgo propuesto en la presente solicitud se concrete en un contrato de seguro, otorgo mi consentimiento para que la documentación contractual y cualquier otra información relacionada con este seguro, me sea entregada a través de la vía digital.

( ) Sí consiento ( ) No consiento (entrega física)

Por lo anterior, autorizo que la documentación contractual y cualquier otra información relacionada con este seguro me sean entregadas a la cuenta de correo electrónico:_____.

Sugerimos consultar las coberturas, limitaciones y/o exclusiones del producto contenidas en las Condiciones Generales que forman parte de la Documentación Contractual que le será entregada al momento de la contratación, conforme al medio definido en la solicitud del seguro y con independencia de que dichas condiciones también pueden ser consultadas en la página de internet www.zurich.com.mx

Datos de la Unidad Especializada (UNE).
Consultas y reclamaciones, contactar a la Unidad Especializada (UNE) de Zurich, ubicada en Toreo Parque Central. Blvd. Manuel Avila Camacho No. 5, Torre B, Piso 20, Col. Lomas de Sotelo, Naucalpan de Juárez, Estado de México C.P. 53390 en donde estaremos atendiendo de lunes a jueves de 9:00 a 17:30 y viernes de 9:00 a 15:00 horas o comunicarse a los teléfonos 55 52 84 11 03 o lada sin costo 800 0800 009 en un horario de 9:00 a 14:00 horas, o bien al correo electrónico unidad.especializada@mx.zurich.com

Declaración final

El representante del solicitante/titular del seguro abajo firmante declara que las respuestas a las preguntas contenidas en este documento son veraces, correctas y completas, y que no existen hechos o circunstancias materiales adicionales que puedan influir en la evaluación del riesgo para el que se solicita el seguro. El representante se compromete a notificar a Zurich cualquier cambio en la información facilitada en este cuestionario que se produzca antes de que comience cualquier cobertura de seguro resultante.

El solicitante/titular del seguro confirma haber recibido, comprendido y aceptado el aviso de Zurich sobre protección de datos.

Firma/Declaración

Nombre de la empresa

Nombre de la persona firmante

Puesto de la persona firmante

Lugar, Fecha

Firma

En cumplimiento a lo dispuesto en el Artículo 202 de la Ley de Instituciones de Seguros y de Fianzas, la documentación contractual y la nota técnica que integran este producto de seguro, quedarán registradas ante la Comisión Nacional de Seguros y Fianzas, a partir del día 19 de diciembre de 2024, con el número CNSF-S0037-0449-2024/CONDUSEF-005334-03.

Zurich Aseguradora Mexicana, SA. de C.V.
Blvd. Manuel A. Camacho No. 5, Toreo Parque Central,
Torre B, Piso 20, Colonia Lomas de Sotelo,
Naucalpan de Juárez, C.P. 53390, Estado de México

ZH53402e-2401-EXTENSIVE