SEGUROS

RIESGO DE PROTECCIÓN DIGITAL (Cyber)

Formulario de Propuesta

CUESTIONARIO DE EVALUACIÓN DE RIESGO DE PROTECCIÓN DIGITAL (Cyber)

INTRODUCCIÓN

Este cuestionario no es una oferta ni un contrato de seguro vinculante. Además, su diligenciamiento no obliga a la compañía de seguros a ofrecerle cobertura alguna. Las respuestas a este cuestionario son muy importantes para evaluar el riesgo con el fin de proporcionar un seguro de Protección Digital (Cyber) para su compañía en base a esta información. Por lo tanto, confiamos en sus declaraciones hechas en el cuestionario, que son la base del contrato de seguro. Si no tiene un recurso de seguridad de la información, entonces el cuestionario debe ser complementado por un representante principal (propietario o miembro de la junta).

¿Adjuntan alguna información o detalles adicionales con respecto a su seguridad informática como anexo? ☐ NO ☐ SI

Moneda de las cifras en este cuestionario: ☐ USD ☐ EUR ☐ GBP ☐ Otros

INFORMACIÓN SOLICITANTE

Nombre de la compañía	
Dirección	
País	
Correo electrónico	
Número telefónico	
Filiales	
Nombres de todos los sitios web (cubiertos por este seguro)	

1.1 ACTIVIDAD(ES) INDUSTRIAL(ES)

Por favor marcar todas las actividades industriales aplicables. Detalles y explicaciones se encuentran en el anexo en página 8.

- ☐ Alimentación & Agricultura
- ☐ Autoridad pública; ONG, sin fines de lucro
- ☐ Defensa / Contratista Militar
- ☐ Educación Entretenimiento &
- ☐ Medios Fabricación
- ☐ Minería & Industrias Primarias
- ☐ Productos farmacéuticos
- ☐ Propiedad Inmobiliaria & Construcción Salud
- ☐ Servicios Financieros - Bancos Otros
- ☐
- ☐ Servicios Financieros – Gestión de inversiones Servicios
- ☐ Financieros – Seguros
- ☐ Servicios profesionales
- ☐ Tecnología de la información – Hardware
- ☐ Tecnología de la información – Servicios
- ☐ Tecnología de la información – Software
- ☐ Telecomunicaciones
- ☐ Transporte / Aviación / Aerocpacial
- ☐ Turismo & Hospitalidad
- ☐ Utilidades
- ☐ Venta al por menor

En caso de "Otros", por favor especificar	
Por favor especificar detalles de sus actividades	

1.2 FACTURACIÓN/INGRESOS Y HUELLA REGIONAL

Por favor marcar todas las actividades industriales aplicables. Detalles y explicaciones se encuentran en el anexo en página 8.

	Local	EE.UU	Unión Europeo	Resto del Mundo
Su facturación / ingresos durante el último año fiscal				
Parte de su facturación / ingresos creados en línea durante el último año fiscal				
Último añoAño anterior Dos años anteriores				

	Último año	Año anterior	Dos años anteriores
Su beneficio bruto (o equivalente)			

Por favor indicar número de empleados	

1.3 TIPO Y CANTIDAD DE DATOS

¿Cuáles de las siguientes categorías de datos sensibles maneja/procesa su compañía?

☐ Información de Identificación Personal (PII)
☐ Información de salud personal (PHI)
☐ Información de Tarjetas de Pago (PCI)
☐ Propiedad Intelectual (IP)

Por favor estimar el número de registros únicos de datos sensibles manejado/procesado por usted:

☐ Menos de 1,000	☐ 1,000 a 10,000	☐ 10,000 a 100,000	☐ Más que 100,000

Informar: _____

1.4 COBERTURA DE SEGURO SOLICITADO

Por favor marcar todas las secciones de cobertura que solicite.

Daños Propios	Deducible para cada uno de los eventos asegurados	Sub-límite para cada uno de los eventos asegurados y en el agregado
☐ Recuperación de información digital		
☐ Interrupción de su actividad empresarial	Período de espera = [……] horas	
☐ Extorsión cibernética		
☐ Transacciones bancarias fraudulentas		Sub-límite max. del 30% del límite agregado
☐ Gastos por la protección a la reputación		

Responsabilidad Civil	Deducible para cada uno de los eventos asegurados	Sub-límite para cada uno de los eventos asegurados y en el agregado
☐ Responsabilidad por violación de información confidencialidad y datos personales		
☐ Responsabilidad por software malicioso o virus informático		
☐ Publicación en medios digitales		

Manejo de Crisis	Deducible para cada uno de los eventos asegurados	Sub-límite para cada uno de los eventos asegurados y en el agregado
☐ Gastos forenses		
☐ Gastos de Defensa – Autoridades Administrativas		

1.5 SEGURO ANTERIOR

• 1 Actualmente tiene o ha tenido un seguro de Protección Digital (Cyber) con la misma cobertura o cobertura similar a la solicitada actualmente? ☐ NO ☐ SI

• 2 Alguna aseguradora ha cancelado o no ha renovado una póliza que proporcione la misma cobertura o cobertura similar a la que solicita el seguro? ☐ NO ☐ SI

1.6 INCIDENTES DE SEGURIDAD E HISTORIAL DE PÉRDIDAS

Por favor responda a las siguientes preguntas considerando cualquier momento durante los últimos tres años.

• 1 Ha tenido algún incidente, interrupción no planificada del negocio, reclamos o demandas que involucren el acceso no autorizado o el uso indebido de su red, incluyendo malversación, fraude, robo de información de propiedad exclusiva, violación de información personal, robo o pérdida de computadoras portátiles, denegación de servicio, vandalismo electrónico o sabotaje, virus informático, intento o demanda de extorsión cibernética u otro incidente? ☐ NO ☐ SI

• 2 Ha recibido alguna reclamación o queja con respecto a denuncias de difamación, invasión o lesión de la privacidad, robo de información, violación de la seguridad de la información, transmisión de malware, participación en un ataque de denegación de servicio, solicitud para notificar a personas debido a un hecho real o sospecha de divulgación de información personal? ☐ NO ☐ SI

• 3 Está consiente de algún hecho, circunstancia, situación, error u omisión real o alegado, o un problema potencial que pueda dar lugar a una pérdida o reclamación en su contra en virtud de la presente póliza de seguro cibernético o cualquier otro seguro similar actual o anterior? ☐ NO ☐ SI

Si se responda "sí" a una o más preguntas de esta sección 1.6, por favour adjuntar una descripción incluyendo detalles completos (causa, costos, notificación, tiempo hasta descubrimiento, tiempo de recuperación y pasos tomados para mitigar futuras exposiciones) de cada evento (incidente, reclamación, etc.).

1.7 MARCOS Y ESTÁNDARES

Por favor marcar todos los marcos legales a los que tiene que cumplir.

☐ Reglamento General de Protección de Datos (GDPR) de la Unión Europea (EU)	☐ US Federal Privacy Act
☐ US Health Insurance Portability and Accountability Act (HIPAA) y US Health Information Technology for Economic and Clinical Health (HITECH) Ac	☐ Otros

Por favor marcar todos los estándares para los que haya sido auditado con éxito o tenga una certificación válida.

☐ Payment Card Industry Data Security Standard (PCI DSS)			
☐ Nivel mercantil 1	☐ Nivel mercantil 2	☐ Nivel mercantil 3	☐ Nivel mercantil 4

Si aplican otros estándares, por favor detallar	
Por favor detallar el ámbito de la certificación	

2 SEGURIDAD INFORMÁTICA

Las siguientes preguntas nos ayudan a evaluar la madurez de su seguridad informática. Por favor responda todas las preguntas y propor- cione evidencia donde esté disponible (p.ej. informes, presentaciones, documentos, etc.). Las preguntas están estructuradas de acuerdo con las cláusulas de la norma ISO 27000. Por lo tanto, las preguntas centradas en un mismo objetivo de seguridad pueden aparecer en diferentes secciones de este cuestionario. Con el fin de crear una mejor comprensión acerca de por qué hacemos las preguntas, cada sección comienza con el objetivo de las categorías de seguridad de ISO.

2.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

• 1 ¿Tiene su compañía una persona responsable para la seguridad informática (p.ej. Chief Information Security Officer "CISO")? ☐ NO ☐ SI

2.2 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo: Garantizar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las que se los considera. Garantizar que empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información.
Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

• 1 ¿Usted provee formación por lo menos anual para aumentar la conciencia de sus usuarios (empleados y contratistas) hacia la seguridad y para preparar a los usuarios a ser más resilientes y vigilantes contra el phishing? ☐ NO ☐ SI

2.3 CONTROL DE ACCESSO

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de información. Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Hacer responsables a los usuarios por salvaguardar su información de autenticación. Evitar el acceso no autorizado a sistemas y aplicaciones.

• 1 ¿Usted restringe los privilegios de empleados y usuarios externos en función de las necesidades comerciales (especialmente los permisos administrativos y el acceso a datos sensibles como datos personales)? ☐ NO ☐ SI

• 2 ¿Usted tiene un proceso formal de aprovisionamiento de acceso para asignar y revocar los derechos de acceso? ☐ NO ☐ SI

• 3 ¿Usted prohíbe los derechos de administrador local en las estaciones de trabajo para los usuarios? ☐ NO ☐ SI

• 4 ¿Usted revoca todo el acceso al sistema, las cuentas de usuarios y los derechos asociados después de la terminación de los usuarios (incl. a empleados, empleados temporales, contratistas y proveedores)? ☐ NO ☐ SI

• 5 ¿Usted ha implementado una política de contraseñas que impone el uso de contraseñas largas y complejas en su compañía? Contraseñas largas y complejas se definen como: 8 caracteres o más; no consiste en palabras incluidas en los diccionarios; libre de caracteres idénticos, numéricos o alfabéticos consecutivos. ☐ NO ☐ SI

2.4 CRIPTOGRAFÍA

Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

¿Está encriptada toda la información confidencial cuando se almacena en dispositivos móviles como laptops o móviles? ☐ No ☐ Sí

2.5 SEGURIDAD OPERACIONAL

Objetivo: Garantizar operaciones correctas y seguras de las instalaciones de procesamiento de información. Garantizar que la información y las instalaciones de procesamiento de información estén protegidos contra el malware. Proteger contra la pérdida de datos. Registrar eventos y generar evidencia. Garantizar la integridad de los sistemas operativos. Evitar la explotación de vulnerabilidades técnicas.
Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

• 1 ¿Usted utiliza protección contra malware en proxy web, puerta de enlace de correo electrónico (email-gateway), estaciones de trabajo y computadoras portátiles? ☐ NO ☐ SI

• 2 ¿Usted realiza copias de seguridad periódicas de datos críticos para el negocio al menos una vez a la semana? ☐ NO ☐ SI

• 3 ¿Usted aplica oportunamente - al menos dentro de un mes del lanzamiento – actualizaciones a sistemas aplicaciones de TI críticos ("parches de seguridad")? ☐ NO ☐ SI

2.6 SEGURIDAD DE LA COMUNICACIÓN

Objetivo: Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

• 1 ¿Están protegidos todos los puntos de acceso a Internet por firewalls apropiadamente configurados? ☐ NO ☐ SI

• 2 ¿Usted monitorea su red e identifica eventos de seguridad?

• 3 ¿Están todos sus sistemas accesibles por Internet (p.ej. servidores web/de correo electrónico) segregados de su red de confianza (p.ej. dentro de una zona desmilitarizada "DMZ" o en un proveedor externo)? ☐ NO ☐ SI ☐ NO APLICA

2.7 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que brindan servicios a través de redes públicas. Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información. Garantizar la protección de los datos utilizados para las pruebas.

• 1 ¿Su servidor web encripta los datos confidenciales (p.ej. HTTPS)? ☐ NO ☐ SI ☐ NO APLICA

• 2 ¿Usted está considerando aspectos de confidencialidad al utilizar datos operacionales para pruebas para garantizar que todos los detalles sensibles estén protegidos por eliminación o modificación? ☐ NO ☐ SI ☐ NO APLICA

2.8 RELACIONES CON PROVEEDORES

Objetivo: Garantizar la protección de los activos de la organización a la que pueden acceder los proveedores. Mantener un nivel acordado de seguridad de la información y entrega de servicios en línea con los acuerdos con los proveedores.

• 1 ¿Los acuerdos con proveedores externos de servicios requieren niveles de seguridad proporcionales al nivel de seguridad de su información? ☐ NO ☐ SI

2.9 GESTIÓN DE INCIDENTES DE LA SEGURIDAD INFORMÁTICA

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

• 1 ¿Usted tiene una persona asignada responsable para la respuesta a incidentes? ☐ NO ☐ SI

2.10 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Objetivo: La continuidad de la seguridad de la información debe integrarse en los sistemas de gestión de la continuidad del negocio de la organización.

• 1 ¿Usted ha realizado un análisis de impacto de negocio ("BIA")? ☐ NO ☐ SI

• 2 ¿Usted tiene implementado un plan de continuidad de negocio que se dirija específicamente a los incidentes cibernéticos? ☐ NO ☐ SI

• 3 ¿Usted prueba por lo menos anualmente sus planes de continuidad de la seguridad informática (p.ej. Continuidad de negocio, Recuperación de desastre? ☐ NO ☐ SI

• 4 ¿Sus instalaciones de procesamiento de información (i.e. cualquier sistema, servicio o infraestructura o ubicación física que lo albergue) están implementadas con redundancia? ☐ NO ☐ SI

2.11 COMPLIANCE

Objetivo: Evitar incumplimientos de obligaciones legales, reglamentarias o contractuales relacionadas a la seguridad de la información y con los requisitos de seguridad. Garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.

• 1 ¿Usted tiene implementado un procedimiento para cumplir de manera permanente con requisitos legales (o contractuales) y regulaciones de privacidad? ☐ NO ☐ SI

• 2 ¿Usted ha asignado a una persona responsable para brindar orientación y garantizar el conocimiento de los principios de privacidad (p.ej. Oficial de Privacidad (DPO))? ☐ NO ☐ SI

3 PUBLICACIÓN EN MEDIOS DIGITALES

En el caso de solicitar también la cobertura de Publicación en medios digitales, por favor responder también a las siguientes preguntas:

• 1 ¿Usted realiza actividades electrónicas / en línea? ☐ NO ☐ SI
En caso afirmativo, ¿qué tipo? (marque todo que aplica)

- ☐ Publicación de contenido electrónico propio
- ☐ Streaming de contenido de video o música bajo licencias
- ☐ /acuerdos con consentimiento Manejo
- ☐ de información sensible
- ☐ (PII/PCI/PHI, IP, otros)
- ☐ Dar consejos (p.ej. médicos, legales, etc.)
- ☐ Contenido para adultos, juegos, apuestas
- ☐ Contenido con licencia de terceros
- ☐ Presentación de productos/servicios de terceros
- ☐ (publicidad, compra o venta)
- ☐ Contenido sin licencia de terceros (p.ej. chats, blogs, foros,
- ☐ comentarios de clientes, etc.)
- ☐ Archivos para descargar
- ☐ Otros

En caso de "otros" tipos de actividades o contenido, por favor especificar	

•2 ¿Usted utiliza servicios basados en web para la distribución de dicho contenido? En caso afirmativo, ¿qué tipo? (marque todo que aplica) ☐ NO ☐ SI

- ☐ Página web (propio y/o alojado por un tercero)
- ☐ Servicios por correo (p.ej. newsletter)
- ☐ Medios Sociales (Twitter, Facebook, Snapchat etc.) Google
- ☐ AdsWords

• 3 ¿Su página web provee una política de privacidad (manejo de datos, uso de cookies, etc.) y una notificación legal sobre el uso de los derechos de terceros y enlaces a páginas web externas, incluyendo un descargo/liberación de responsabilidad? Confirmar, si dicho contenido está aprobado por un abogado competente? ☐ NO ☐ SI

4 MANEJO DE VULNERABILIDADES CONOCIDAS (como por ejemplo Log4Shell)

¿Usted revisa periódicamente con proveedores de tecnología internos y/o externos en búsqueda de vulnerabilidades conocidas del estilo Log4Shell o similares? Si ☐ No ☐

¿Usted realiza los parches necesarios en forma inmediata referentes a estas Vulnerabilidades Conocidas e implementa medidas correctivas en el corto plazo en caso de que los parches aún no estén disponibles? Si ☐ No ☐

¿Usted escanea si sus sistemas han sido vulnerables contra los Indicadores de Compromiso (IoC) y tomó las acciones necesario si usted encuentra cualquier IoC (por ejemplo volver a instalar desde la copia de seguridad y parche)? Si ☐ No ☐

5 COMENTARIOS ADICIONALES Y FIRMA(S)

¿Desea agregar más información o detalles sobre su seguridad de la información?

.....

.....

Al firmar este documento (debe ser firmado por el funcionario, el propietario o el gerente), confirmo que soy un representante debidamente autorizado de la empresa con las habilidades técnicas suficientes para proporcionar, según mi mejor conocimiento, respuestas ciertas y completas con respecto a las preguntas dentro de este cuestionario en nombre de la empresa. El cuestionario completado y los anexos opcionales son la base de la cobertura y, por lo tanto, serán parte del contrato de seguro.

Fecha.....

Firma.....

Nombre.....

Cargo.....

Correo electrónico.....

Fecha.....

Firma.....

Nombre.....

Cargo.....

Correo electrónico.....

ANEXO 1: RESUMEN – ACTIVIDADES INDUSTRIALES

Fuente: Cyber Insurance exposure data schema v1.0 by Cambridge Centre for Risk Studies

Alimentación & Agricultura	Compañías involucradas en la industria alimentaria, incluyendo la producción, transformación, distribución y suministro al por mayor.
Autoridad pública; ONG, sin fines de lucro	Agencias gubernamentales nacionales o locales, organizaciones no-gubernamentales y sin fines de lucro
Defensa / Contratista Militar	La industria de la defensa incluye el gobierno y la industria comercial, incluyendo la investigación, el desarrollo, la producción y el servicio del material, del equipo y de las instalaciones militares.
Educación	Colegios y universidades, distritos escolares independientes y unificados, préstamos a estudiantiles y colegiaturas
Energía	Empresas involucradas en la exploración, extracción y desarrollo de reservas de petróleo o gas, perforación de petróleo y gas o empresas de energía integrada.
Entretenimiento & Medios	Empresas que ofrecen noticias, información y entretenimiento: radio, televisión, cine, teatro.
Fabricación	Compañías fabricando o procesando bienes, sobre todo en grandes cantidades y a través de maquinaría industrial.
Minería & Industrias Primarias	Empresas involucradas en la minería, extracción y procesamiento de extracción de minerales, carbón, materias primarias y recursos naturales.
Productos farmacéuticos	La industria farmacéutica desarrolla, produce y comercializa fármacos para su uso como medicamentos. Las compañías farmacéuticas pueden tratar medicamentos genéricos o de marca y dispositivos médicos.
Propiedad Inmobiliaria & Construcción	Empresas que administran, desarrollan y realizan transacciones de propiedades que consisten en terrenos y edificios, junto con sus recursos naturales, como cultivos, minerales o agua.
Salud	Empresas proveedoras de bienes y servicios para el tratamiento de pacientes con atención curativa, preventiva, rehabilitadora y paliativa.
Servicios Financieros – Bancos	Empresas dedicadas a banca comercial, instituciones de ahorro, cooperativas de crédito, emisión de tarjetas de crédito, financiamiento, compañías y corredores de hipotecas y préstamos, procesamiento de transacciones financieras, actividades de reserva y cámara de compensación y banca central.
Servicios Financieros – Gestión de inversiones	Empresas dedicadas a la gestión de inversiones, negociación y corretaje de valores, negociación de contratos de productos básicos y corretaje, bolsas de valores e inversiones, fondos de inversión y capital de riesgo, adminis- tración de carteras, asesoramiento sobre inversiones y fondos y fideicomisos de entidades legales.
Servicios Financieros – Seguros	Aseguradoras directas, compañías de reaseguro y agencias de seguros y corredurías.
Servicios profesionales	Ocupaciones que ofrecen asesoramiento y servicios especializados de negocios. Algunos servicios profesionales requieren la tenencia de licencias o cualificaciones profesionales, tales como arquitectos, auditores, ingenieros, médicos y abogados.
Tecnología de la información – Hardware	Empresas dedicadas a la fabricación y/o montaje de ordenadores (mainframes, ordenadores personales, estaciones de trabajo, ordenadores portátiles y servidores) y equipos periféricos (p. ej. dispositivos de almacenam iento, impresoras, monitores, etc.)
Tecnología de la información – Servicios	Empresas proveedoras de servicios de almacenaje o de procesamiento de datos (incluyendo servicios cloud y streaming); Publicación en internet y contenido de radiodifusión (incluyendo medios sociales); Portales de búsqueda en Internet; Servicios relacionados con el diseño de sistemas informáticos, gestión de instalaciones informáticas, servicios de programación informática y consultoría en hardware o software informático.
Tecnología de la información – Software	Empresas que participan en el diseño, desarrollo, documentación y publicación de programas informáticos.
Telecomunicaciones	Empresas que facilitan el intercambio de información a través de distancias significativas por medios electrónicos
Transporte / Aviación / Aerospacial	Empresas que facilitan el transporte de bienes o clientes. El sector del transporte está compuesto por aerolíneas, ferrocarriles y compañías de transporte.
Turismo & Hospitalidad	Empresas que prestan servicios de turismo, viajes, alojamiento, restauración y hostelería.
Utilidades	Este sector contiene empresas tales como empresas de electricidad, gas y agua y proveedores integrados.
Venta al por menor	Minoristas para el público en general, vendedores de bienes y servicios tanto en tiendas minoristas como en línea, mayoristas y distribuidores.
Otros	