Cyber Allianz Protect

Cuestionario

Para poder presentarles oferta será necesario que respondan todas las preguntas del presente cuestionario y fundamentalmente, las que están señaladas con una *. El hecho de rellenar y firmar este formulario de propuesta no obliga al (los) proponente(s) ni a la(s) aseguradora(s) a suscribir un contrato de seguro. Si no hubiera espacio suficiente para las respuestas a las preguntas, podrá utilizar una hoja adicional adjuntándola a este formulario (indique el número de la pregunta relacionado con la explicación adicional)

La póliza a que se refiere este cuestionario se aplica a reclamaciones realizadas contra el asegurado durante el período de seguro.

1. INFORMACIÓN GENERAL

Nombre del tomador del seguro: _____
Número de Identificación: _____
Dirección de la oficina principal: _____
Tipo de Compañía:

Pública	Privada	Mixta	Sin ánimo de lucro

País de constitución del tomador del seguro y fecha de constitución: _____
Dirección de su página en Internet: _____
Países en los que tiene operación (Ámbito Territorial):

Colombia	Mundial	Mundial, excepto USA y Canadá	Otra, ¿cuál?

Liste las sociedades Filiales y/o subsidiarias y/o Participadas que desea incluir en el seguro:

Nombre de la sociedad	Fecha de const.	Actividad	% Part.	Activos último año	Ventas último año	Utilidad último año

*Citar cifras expresadas en miles de pesos colombianos.
* Adjunte estados financieros consolidados del año inmediatamente anterior con el dictamen del revisor fiscal y las notas.

2. INFORMACIÓN DE LA ORGANIZACIÓN (*)

*¿Podría describir de manera clara y concisa las actividades principales de su organización?

_____
_____
_____
_____
_____

*Por favor, proporcione la siguiente información de su organización:

	Colombia	EE. UU.	Resto del mundo
Número de empleados			
Facturación procedente de transacciones basadas en Internet (online)			
Número aproximado de clientes			

*Facilite la siguiente información sobre el tratamiento de datos personales:

Procesados y Almacenados	Latino América	USA / Canadá	Europa
Número o volumen aproximado de datos de carácter personal tratados (PII)			
Número de datos de salud (PHI)			
Número de datos relacionados con información biométrica (BIPA)			
Número de registros de tarjetas de pago (PCI)			

*En caso de aplicación del estándar de tarjetas de pago PCI, por favor informe:
¿Aceptan ustedes información de tarjetas de crédito/débito o de otro tipo de tarjetas?
SÍ ☐ NO ☐
En caso afirmativo ¿qué porcentaje de la facturación representan? _____ %
¿Procesan ustedes pagos en nombre de alguna otra persona u organización?
SÍ ☐ NO ☐
En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Cumplen ustedes plenamente las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) aplicables?
SÍ ☐ NO ☐
¿Certifican ustedes mismos este cumplimiento?
SÍ ☐ NO ☐
En caso de realizar el tratamiento de datos biométricos, por favor detalle el tipo de tratamiento, su finalidad y las medidas de análisis de riesgo y mitigación adoptadas.

_____
_____
_____

_____
_____

En caso de realizar transferencias internacionales de datos a países fuera de la Unión Europea/Espacio Económico Europeo, ¿podría detallar las medidas técnicas y organizativas implementadas para garantizar su seguridad?

_____
_____
_____
_____
_____

3. SEGUROS ANTERIORES

*¿La Sociedad y/o sus Filiales y/o Subsidiarias y/o Soc. Participadas en este seguro, tiene o ha tenido cobertura de Seguro cibernético?

SÍ ☐ NO ☐

Si la respuesta es afirmativa, favor diligenciar lo siguiente:

Nombre compañía aseguradora	Limite asegurado	Deducibles	Fecha de vencimiento o cancelación

¿Alguna Compañía aseguradora ha rechazado o denegado la cobertura del riesgo para quien actualmente se solicita este seguro?

SÍ ☐ NO ☐

¿Se ha interrumpido la vigencia de la cobertura entre cualquiera de las vigencias desde la fecha del primer seguro?

SÍ ☐ NO ☐

Si alguna de estas respuestas es afirmativa, favor proporcione detalles:

_____
_____
_____

4. PÓLITICAS Y PROCEDIMIENTOS ORGANIZACIONALES.

*¿Cumple su organización con las siguientes normas, marcos o mejores prácticas en ciberseguridad?, por favor señale con una x las opciones que corresponda:

ISO 27001:2013/2022 ☐

NIST (US National Institute of Standards and Technology) Cybersecurity Framework ☐

HIPAA/ HITECH ☐

Payment Card Industry Data Security Standard (PCI DSS) (especificar nivel certificado) ☐

Otras:

_____
_____

¿Cuál es el presupuesto total de su organización para tecnologías de la información y qué porcentaje está destinado a la seguridad de la información y ciberseguridad? Por favor, proporcione detalles.

_____
_____
_____
_____
_____

¿Cuenta su organización con un Director de Seguridad de la Información (CISO), Director de Seguridad (CSO) o un equivalente funcional?

SÍ ☐ NO ☐

En caso negativo, por favor proporcione detalles:

_____
_____
_____

En función del riesgo de seguridad de datos y tecnología de la información, ¿ha implementado su organización las siguientes políticas y programas? Marque todas las opciones que correspondan:

- Política de seguridad de la información y ciberseguridad.
  SÍ ☐ NO ☐
- Política de Uso Aceptable (AUP) con rangos de uso permitidos y consecuencias por incumplimiento.
  SÍ ☐ NO ☐
- Restricciones para el uso de redes sociales desde dispositivos de la organización, salvo necesidad organizacional.
  SÍ ☐ NO ☐
- Programa de amenazas internas para prevenir, detectar y mitigar riesgos.
  SÍ ☐ NO ☐

En caso negativo, por favor proporcione detalles:

_____
_____
_____
_____
_____

¿Proporciona su política, o usted mismo en caso de ausencia de política, orientación sobre los siguientes aspectos?, por favor señale con una X las opciones que corresponda e incluya comentarios si así lo requiere.

	Sí	No	Comentarios
Funciones del responsable de seguridad de la información o equivalente			
Seguridad de la red (derechos de acceso, contraseñas, encriptado, etc.)			
Seguridad de los dispositivos móviles (incluyendo ordenadores portátiles, teléfonos inteligentes y dispositivos de memoria)			
Uso y almacenamiento de información identificable personalmente y notificación en caso de violación			
Uso de redes sociales por los empleados			
Uso de redes Wifi no seguras			
Procedimientos de copiado de seguridad de datos (indiquen con qué frecuencia se produce dicho copiado y si se hace a distancia)			

*¿Realiza su organización acciones formativas en materia de protección de datos y seguridad de la información?
SÍ ☐ NO ☐

Es requisito obligatorio que sus empleados, proveedores, contratistas y socios externos con acceso a la red corporativa reciban capacitación en ciberseguridad? En caso afirmativo, especifique la periodicidad.
SÍ ☐ NO ☐

Periodicidad: _____

¿Incluyen los materiales de su programa de concientización sobre ciberseguridad formación para evitar riesgos y amenazas cibernéticas comunes, como ingeniería social, spear phishing, hacking, phishing y otras vulnerabilidades? Especifique la periodicidad.

SÍ ☐ NO ☐

Periodicidad: _____

¿Su organización lleva a cabo un análisis anual para identificar posibles deficiencias en sus capacidades de ciberseguridad, y elabora e implementa hojas de ruta de formación y/o planes de proyectos para abordar dichas deficiencias?

SÍ ☐ NO ☐

Señale con una X las medidas implementadas por su organización:

- Realizan evaluaciones de pruebas de penetración al menos una vez al año. ☐
- Utilizan agentes de penetración independientes para simular acciones de adversarios. ☐
- Ejercicios de simulación de las tácticas, técnicas y procedimientos de actores de ransomware ☐
- El alcance de las pruebas incluye tanto la red como los sistemas y aplicaciones críticos para el negocio. ☐
- Califican y/o priorizan los resultados de las pruebas de penetración y las recomendaciones según el riesgo para mitigar o remediar vulnerabilidades y debilidades identificadas. ☐
- Otros, por favor especifique cuales:

  _____

  _____

4.1 Gestión de Activos

*¿Podría confirmar si su organización mantiene un inventario actualizado y detallado de todos los dispositivos de software, incluidos los sistemas operativos, y hardware en sus redes?

SÍ ☐ NO ☐

¿Cuenta con una base de datos de gestión de configuración integral (CMDB - Configuration Management Database) que abarque todos los activos de TI, activos de la nube pública, sus dependencias, niveles de criticidad, propiedad, así como el software y sus versiones de parches?

SÍ ☐ NO ☐

Por favor, indique si clasifica la información según su nivel de confidencialidad:

SÍ ☐ NO ☐

Por favor, indique si clasifica la información según sus requisitos de integridad y disponibilidad:

SÍ ☐ NO ☐

¿Implementa procedimientos seguros para el desecho de medios que contienen información confidencial cuando ya no son necesarios?

SÍ ☐ NO ☐

4.2 Compliance

*¿Su organización ha implementado un procedimiento para asegurar el cumplimiento continuo con los requisitos legales, contractuales y las regulaciones de privacidad?

SÍ ☐ NO ☐

¿Dispone su organización de una persona responsable, como un Oficial de Privacidad, para brindar orientación y asegurar el conocimiento de los principios de privacidad

SÍ ☐ NO ☐

¿Realiza su organización escaneos periódicos, incluyendo pruebas de seguridad y pruebas de penetración, ya sea internamente o con soporte de terceros, especialmente al introducir nuevos sistemas o realizar cambios significativos?

SÍ ☐ NO ☐

4.3 Fusiones y Adquisiciones:

¿Aplica un procedimiento de auditoría legal (Due Diligence) y gestión de riesgos que se comprenda la evaluación de la ciberseguridad existente?

SÍ ☐ NO ☐

¿Los procesos de fusión y adquisición establecen una integración de las redes escalonada por etapas, para asegurarse de que la nueva entidad cuenta al menos con un nivel de ciberseguridad comparable al del tomador del seguro?

SÍ ☐ NO ☐

¿Las redes respectivas se mantienen totalmente separadas mientras la ciberseguridad no llega a alcanzar unos niveles equiparables?
SÍ ☐ NO ☐

5. GESTIÓN DE INCIDENTES

*¿Cuenta su organización con recursos internos y/o contratos vigentes con proveedores especializados para la contención, erradicación y recuperación ante incidentes, incluyendo la eliminación de malware y restauración de sistemas?
SÍ ☐ NO ☐

*¿Dispone su organización de un plan de respuesta a incidentes (IRP) escrito e implementado que contemple la gestión de crisis, violaciones de datos y seguridad de la red, incluyendo entrenamiento en mitigación de DDoS??
SÍ ☐ NO ☐

*¿Incluye su plan (IRP) cláusulas contractuales o términos acordados que establezcan instrucciones de respuesta y notificación de incidentes para colaboradores y proveedores que gestionan o acceden a datos corporativos?

SÍ ☐ NO ☐

*¿Están formalizados, actualizados y probados sus Planes de Continuidad del Negocio (BCP) y Planes de Recuperación ante Desastres (DRP) para asegurar la continuidad operativa durante interrupciones y desastres?

SÍ ☐ NO ☐

*¿Incluyen sus planes de (IRP), (DRP) y (BCP) a los proveedores externos como parte de las estrategias de continuidad y recuperación?

SÍ ☐ NO ☐

*¿Cuál es el tiempo de recuperación objetivo "RTO" (horas)?: _____

En caso de señalar alguna respuesta de la presente sección en forma negativa, por favor proporcione detalles:
_____
_____
_____

6. RECUPERACIÓN DE DATOS

*¿Cuenta con procesos integrales para copias de seguridad (Backups), recuperación y pruebas?
SÍ ☐ NO ☐

*¿Realiza una recuperación y prueba de las copias de seguridad de la información y sistemas críticos (considerando como tales los sistemas, aplicaciones, bases de datos, etc. que puedan provocar la paralización de la actividad empresarial)?
SÍ ☐ NO ☐

*Por favor indique periodicidad:
Mensual ☐
Trimestral ☐
Semestral ☐
Anual ☐

*¿Almacena las copias de respaldo de manera offline y onsite?
SÍ ☐ NO ☐

*¿Almacena las copias de respaldo de manera offline y offsite?
SÍ ☐ NO ☐

*¿Realiza su organización pruebas de restauración de datos de manera regular para asegurar que los respaldos sean efectivos y puedan ser recuperados en caso de pérdida de datos?
*SÍ ☐ NO ☐

*¿Implementa su organización medidas de protección para los respaldos, asegurando que estén seguros contra accesos no autorizados y amenazas cibernéticas?
SÍ ☐ NO ☐

7. PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

7.1 Seguridad Física

¿Mantiene un registro actualizado del personal autorizado (empleados, proveedores y visitantes) con acceso a sus instalaciones y áreas de seguridad crítica?

SÍ ☐ NO ☐

*¿Ha instalado controles avanzados de acceso, como sistemas biométricos?

SÍ ☐ NO ☐

*¿Ha implementado sistemas avanzados de monitoreo, como CCTV 24/7 y documentación detallada de cada acceso?

SÍ ☐ NO ☐

7.2 Seguridad Operacional

*¿La organización implementa y actualiza regularmente soluciones antimalware, como antivirus, antispyware y seguridad avanzada para Endpoints?

SÍ ☐ NO ☐

*¿Las actualizaciones se realizan de manera automática?

SÍ ☐ NO ☐

En caso negativo, por favor proporcione detalles:

_____

_____

¿Tiene establecidas políticas y procesos de gestión de parches, incluida la gestión de parches críticos y el inventario de equipos y programas informáticos?

SÍ ☐ NO ☐

En caso afirmativo, detalle las políticas y procesos establecidos.

_____

_____

_____

*¿Cuánto tarda en instalar los parches críticos?

a) 24 horas ☐

b) 24-72 horas ☐

c) 3-7 días ☐

d) Más de 7 días ☐

*¿Fija hitos (*KPIs*) a lo largo del año para hacer seguimiento de su implantación efectiva?

a) >95% ☐

b) 90-95% ☐

c) <90% ☐

d) <80% ☐

e) No hay ninguno ☐

*¿Se encuentran aislados del resto de la red los programas y aplicaciones informáticas antiguas o en proceso de apagado (sistemas legacy sin soporte)?

SÍ ☐ NO ☐

*¿Se prueba y se jerarquiza la prioridad de los parches de seguridad antes de implantarlos?

SÍ ☐ NO ☐

*En relación con las herramientas de seguridad que aplica para los Endpoints, usted:

- Incluye antivirus con capacidades heurísticas.

  SÍ ☐ NO ☐

- ¿Su organización utiliza detección de comportamiento y mitigación de exploits?
  SÍ ☐ NO ☐
- ¿Emplea su organización una herramienta de respuesta y detección de amenazas (ETDR/EDR) con funciones avanzadas como monitorización, respuesta automática, alertas, capacidades forenses y análisis?
  SÍ ☐ NO ☐
- ¿Implementa su organización controles de aplicaciones para permitir solo aquellas que estén autorizadas, revisando estas aplicaciones al menos dos veces al año?
  SÍ ☐ NO ☐
- ¿Cuenta su organización con un equipo interno o un Proveedor de Servicios de Seguridad Gestionada (MSSP) que monitoriza y analiza anomalías?
  SÍ ☐ NO ☐
- ¿Su organización utiliza sistemas operativos, software o hardware que ya no cuentan con soporte o se consideran 'fin de vida' (EOL) por parte de los fabricantes?
  SÍ ☐ NO ☐

En caso afirmativo, por favor, resuma los casos específicos de tecnologías EOL en uso:

_____

_____

_____

* Indique si cuenta con:

a.	Centro de Operaciones de Seguridad (*SOC*) (¿interno o externo?)	SÍ ☐	NO ☐
b.	Gestión de incidentes y de seguridad de la información (*SIEM*)	SÍ ☐	NO ☐
c.	Prevención de fugas de datos (*DLP*)	SÍ ☐	NO ☐
d.	Sistema de prevención y detección de intrusiones (*IDS/IPS*)	SÍ ☐	NO ☐
e.	Cortafuegos de aplicaciones de cara a internet (*WAF*)	SÍ ☐	NO ☐
f.	Cortafuegos de última generación (*NGFW*)	SÍ ☐	NO ☐

7.3 Seguridad de la red

* ¿Configura su organización firewalls para prevenir accesos no autorizados y revisa sus configuraciones al menos una vez al año?
SÍ ☐ NO ☐

¿Ha adoptado soluciones de Control de Acceso a la Red (NAC) para gestionar de manera segura el acceso a las redes inalámbricas de su empresa?
SÍ ☐ NO ☐

¿Cuentan con las siguientes medidas de separación física o lógica de redes?:

a. Sistemas esenciales.	SÍ ☐	NO ☐
b. Centros de datos.	SÍ ☐	NO ☐
c. Ubicación	SÍ ☐	NO ☐
c. Entornos de copias de seguridad y de producción.	SÍ ☐	NO ☐
d. Redes Wi-Fi y de invitados.	SÍ ☐	NO ☐

¿Utiliza su organización dispositivos de seguridad en los puntos de salida de la red para la prevención y detección de intrusiones, empleando firmas, análisis de comportamiento en la red y otros mecanismos para detectar y evitar ataques?
SÍ ☐ NO ☐

En caso afirmativo, ¿se despliega en sus sistemas de prevención de intrusiones (IPS), el modo de bloqueo activo para bloquear firmas maliciosas conocidas, actividades/código malicioso y comportamientos de ataque sofisticados?
SÍ ☐ NO ☐

*¿Ha implementado la segregación de todos los segmentos de red considerados de alto riesgo, como los sistemas de punto de venta, el procesamiento de datos confidenciales y las redes de producción y operacionales?
SÍ ☐ NO ☐

¿Están sus sistemas accesibles desde Internet, como servidores web o de correo electrónico, adecuadamente segregados de su red interna de confianza, por ejemplo, ubicándolos en una zona desmilitarizada (DMZ) o gestionándolos a través de un proveedor externo?
SÍ ☐ NO ☐

7.4 Criptografía (*)

¿Su organización implementa medidas de seguridad, como la limitación de acceso o la encriptación, para proteger la información confidencial almacenada en medios extraíbles, tales como dispositivos de almacenamiento externos (por ejemplo, memorias USB, discos duros)?

SÍ ☐ NO ☐

*¿Aplica su organización cifrado obligatorio para proteger la información crítica y otros datos sensibles (como información de salud (PHI), datos personales (PII), etc.) de acuerdo con las políticas establecidas de clasificación y protección de la información en los siguientes contextos?

• Datos en reposo	Sí ☐	No ☐
• Datos en tránsito	Sí ☐	No ☐
• Computadoras portátiles o equipos de escritorio	Sí ☐	No ☐
• Datos en dispositivos removibles	Sí ☐	No ☐
• Dispositivos móviles	Sí ☐	No ☐
• Copias de respaldo	Sí ☐	No ☐

¿Ha establecido e implementado su organización una política para el uso, protección y duración de las claves criptográficas?

SÍ ☐ NO ☐

¿Utiliza su organización encriptación para toda la comunicación o información confidencial, por ejemplo, a través de correo electrónico?

SÍ ☐ NO ☐

*¿Emplea su servidor web cifrado para proteger los datos confidenciales, como HTTPS o AES?

SÍ ☐ NO ☐

7.5 Acceso al entorno OT

¿Los empleados acceden con las mismas credenciales que al entorno IT?

SÍ ☐ NO ☐

¿Existe posibilidades de acceso remoto?

SÍ ☐ NO ☐

¿Requiere MFA?

SÍ ☐ NO ☐

¿Requiere MFA para Empleados?

SÍ ☐ NO ☐

¿Requiere MFA para Proveedores?

SÍ ☐ NO ☐

8. CONTROL DE ACCESOS Y AUTENTICACIÓN SEGURA

8.1 Monitoreo de cuentas y revocación.

¿Su organización implementa y monitorea un sistema de expiración para las cuentas de usuario, asegurando que estas se desactiven automáticamente al alcanzar su fecha de vencimiento?

SÍ ☐ NO ☐

¿Existe un proceso establecido en su organización para desactivar las cuentas de usuario en caso de cese de empleo o cambio de funciones de un empleado, contratista, consultor o usuario externo?

SÍ ☐ NO ☐

¿Se sigue un procedimiento para desactivar las cuentas del sistema al finalizar el empleo o cuando ocurre un cambio de funciones de un empleado, contratista, consultor o usuario de terceros?

SÍ ☐ NO ☐

¿Restringe su organización los privilegios de acceso de empleados y usuarios externos basándose en las necesidades comerciales, especialmente en lo que respecta a permisos administrativos y acceso a datos sensibles como la información de identificación personal (PII)?

SÍ ☐ NO ☐

¿Es el permiso de acceso autorizado por el propietario de la información?

SÍ ☐ NO ☐

¿El propietario de la información revisa y valida al menos anualmente los derechos de acceso otorgados a los usuarios?

SÍ ☐ NO ☐

*¿Requiere su organización la autenticación multifactor (MFA) para acceder a los datos , sistemas críticos y sensibles?

SÍ ☐ NO ☐

¿Implementa su organización soluciones de Gestión de Identidades y Accesos (IAM) o Gestión de Accesos Privilegiados (PAM) para asegurar y controlar el acceso a sus sistemas críticos y datos sensibles?

SÍ ☐ NO ☐

¿Se requiere autenticación multifactor (AMF/*MFA*) para el acceso a?:

a. Información o aplicaciones esenciales SÍ ☐ NO ☐

b. Administradores de dominio SÍ ☐ NO ☐

c. Usuarios con privilegio SÍ ☐ NO ☐

*¿Exige su organización autenticación multifactor (MFA) para todos los accesos remotos a la red corporativa por parte de empleados y/o terceros proveedores de servicio, como VPN, Protocolo de Escritorio Remoto (RDP) u otros métodos de acceso remoto seguro?

SÍ ☐ NO ☐

Por favor, indique el número de cuentas de administrador de dominio activas que tiene su organización:

_____

Indique el número de cuentas de servicios privilegiadas activas que tiene su organización:

_____

8.2 Política sobre Contraseñas

*¿Ha establecido su Organización una política que exige el uso de contraseñas seguras y complejas? Contraseñas largas y complejas se definen como: 8 caracteres como mínimo, no contenga sustantivos comunes: (Nombre, apellidos, marca, Organización...), no contenga palabras completas (susceptibles de ataques de diccionario), Compuestas por minúsculas, mayúsculas, símbolos, numéricos.

SÍ ☐ NO ☐

¿Implementa su organización políticas y programas de formación para educar a los usuarios sobre los riesgos de reutilizar contraseñas y las medidas para prevenirlo?

SÍ ☐ NO ☐

¿Ha reemplazado su Organización todas las contraseñas predeterminadas en los dispositivos conectados a internet (p.ej routers)?

SÍ ☐ NO ☐

(c) ¿Proporciona su Organización a todos los usuarios un software autorizado para la gestión de contraseñas?

SÍ ☐ NO ☐

9. OUTSOURCING / TERCEROS PROVEEDORES DE SERVICIOS

*La Compañía ¿utiliza terceros proveedores de servicios para realizar a distancia alguna actividad (p. ej., mantenimiento de páginas web, copiado de seguridad de datos, servicios de pago, etc.)?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____

_____

_____

_____

_____

*¿Los contratos con proveedores externos exigen medidas de seguridad que correspondan al nivel de protección para cada tipo de información, de acuerdo con las políticas establecidas y las regulaciones locales e internacionales aplicables?

SÍ ☐ NO ☐

¿Realiza auditorias, revisiones y actualizaciones regulares de todos sus contratos con terceros?

SÍ ☐ NO ☐

¿Ha definido y establecido controles de seguridad de la información en una política específica para gestionar el acceso de los proveedores a su información?
SÍ ☐ NO ☐
¿La Organización lleva a cabo evaluaciones de seguridad y reevaluaciones periódicas de terceros y proveedores de servicios que tienen acceso a sus activos de información?
SÍ ☐ NO ☐
¿Cuenta la Organización con un proceso o solución técnica para identificar, evaluar, gestionar, monitorear y mitigar los riesgos asociados con socios externos y otros proveedores de servicios?
SÍ ☐ NO ☐
*Usted y sus subordinadas ¿utilizan servicios de computación en la nube? SÍ ☐ NO ☐
¿Nube Privada? SÍ ☐ NO ☐
¿Nube Pública? SÍ ☐ NO ☐
¿Combinación nube publica/privada? SÍ ☐ NO ☐

*Por favor suministre el nombre del proveedor(es) de este servicio:
_____
¿Exige la Organización a los proveedores que mantengan un seguro u otro mecanismo de indemnización para cubrir pérdidas ocasionadas por ellos, incluidas aquellas derivadas de violaciones de privacidad?
SÍ ☐ NO ☐
¿El proveedor de la nube utiliza soluciones de mitigación de DDoS?
SÍ ☐ NO ☐
El contrato ¿garantiza que el tercero proveedor de servicios asuma una responsabilidad contractual por toda pérdida sufrida por el asegurado debida al incumplimiento por parte de dicho tercero de la protección adecuada de sus datos?
SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:
_____
_____
_____
_____
¿Está limitada esa responsabilidad y, en caso afirmativo, a qué nivel?
_____
_____
_____
_____
¿Exige la Organización a los proveedores que mantengan un seguro u otro mecanismo de indemnización para cubrir pérdidas ocasionadas por ellos, incluidas aquellas derivadas de violaciones de privacidad?
SÍ ☐ NO ☐

10. CONTENIDO MULTIMEDIA

Las actividades de medios de su organización abarcan: (marque todas las opciones que correspondan):

Televisión	SÍ ☐	NO ☐
Radio	SÍ ☐	NO ☐
Imprenta	SÍ ☐	NO ☐
Publicidad en Internet	SÍ ☐	NO ☐
Los sitios web de la organización.	SÍ ☐	NO ☐
Medios de comunicación social	SÍ ☐	NO ☐
Elementos de marketing	SÍ ☐	NO ☐
Transmisión de audio o video	SÍ ☐	NO ☐

*Otro: por favor proporcione detalles:
_____
_____
_____

¿La organización realiza una revisión con un asesor legal para examinar y asegurar que la actividad en medios cumpla con las normas de propiedad intelectual antes de su publicación, transmisión, distribución o uso?
SÍ ☐ NO ☐
Las medidas de protección con proveedores de contenido y colaboradores externos, incluidos trabajadores independientes, contratistas y otros talentos, abarcan: (marque todas las opciones que correspondan)

- Se asegura la obtención de permisos o autorizaciones por escrito.
  SÍ ☐ NO ☐
- Se establecen acuerdos de indemnización o exención de responsabilidad en beneficio de la organización.
  SÍ ☐ NO ☐
- La organización cuenta con políticas y procedimientos establecidos para identificar, evaluar y mitigar contenido controvertido, potencialmente difamatorio o infractor en los sitios web de la organización
  SÍ ☐ NO ☐
- ¿La organización cuenta con una política de privacidad aprobada por el área legal y publicada en su sitio web que cumpla con las normativas de protección de datos, incluyendo detalles sobre la recopilación de datos, uso de cookies, un aviso legal sobre derechos de terceros y enlaces externos?
  SÍ ☐ NO ☐

11. PROGRAMAS MALGINOS

*¿Aplica herramientas de seguridad a los equipos terminales?
SÍ ☐ NO ☐
En caso afirmativo seleccione lo que proceda:
a) Detección y respuesta ampliadas multicapa (*Extended detectaron and response-XDR solution platform*) ☐
b) Detección y respuesta en terminales (*Endpoint Detection Response-EDR*) ☐
c) Plataforma de protección en terminales (*Endpoint Protección Platforms-EPP*) ☐

¿Realizan pruebas de integridad de las copias de seguridad antes de su restauración para asegurarse de que no están infectadas por programas malignos?

SÍ ☐ NO ☐
¿Al menos anualmente realizan pruebas frente a intrusiones en los sistemas periféricos?
SÍ ☐ NO ☐
¿Contrata servicios de terceros (empresas de inteligencia sobre ciberamenazas u organismos públicos) para vigilar su superficie de ataque (sistemas periféricos o accesibles desde Internet)?
SÍ ☐ NO ☐

¿Aplica alguna de las siguientes soluciones de seguridad para el correo electrónico?
Seleccione las que aplique:
a) Protección frente a falsas identidades de correo electrónico (*Sender Policía Framework-SPF*) ☐
b) Autenticación de correo electrónico (*Domain Keys Identified Mail-DKIM*) ☐
c) Autenticación de mensajes, informes y conformidad basada en dominios (*Domain-based Message Authentication, Reporting and Conformance-DMARC*) ☐
d) Sandbox ☐

¿Las pasarelas de correo electrónico están configuradas para buscar enlaces y programas potencialmente dañinos y bloquear ejecutables?
SÍ ☐ NO ☐
¿Aplica filtro de contenidos en Internet, restringiendo el acceso a plataformas y páginas de redes sociales?
SÍ ☐ NO ☐
¿Los macros se encuentran desactivados por defecto?
SÍ ☐ NO ☐
¿Cuenta con un plan de emergencia específico para cibersecuestro de datos (*ransomware*), incluyendo pruebas anuales frente a incidentes de esta clase?
SÍ ☐ NO ☐

12. RECLAMACIONES Y CIRCUNSTANCIAS

En los 5 últimos años:

*¿Han notificado ustedes alguna reclamación o circunstancia, en virtud de una póliza de responsabilidad (p. ej., ciber-responsabilidad, responsabilidad general, responsabilidad de consejeros y directivos, responsabilidad por errores u omisiones, etc.) o de cualquier otra póliza de seguros (inmobiliaria, cese de actividad, etc.), como consecuencia de actos de violación de la privacidad, pérdida o robo de información personal o comercial o acceso no autorizado a su red de ordenadores?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Les ha investigado algún organismo regulador u otra entidad reconocida del sector en relación con información personal o le ha solicitado información al respecto?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Han recibido alguna queja de algún cliente, empleado o proveedor de servicios en relación con su información personal o corporativa?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Han sido objeto de algún ataque contra su sistema informático?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Se ha visto suspendido o interrumpido su red/sistema informático, voluntaria o involuntariamente, por cualquier razón (¿por ejemplo, ataque dirigido o generalizado, pérdida de datos, etc.?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

¿Cuánto duró la suspensión o interrupción? _____

¿Se produjo una pérdida de beneficios o un aumento de costes asociado con la suspensión o interrupción?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____
_____

DECLARACIÓN DE GARANTÍA

*Después de la investigación ¿conocen algún hecho o circunstancia que pudiera dar lugar a una reclamación en virtud de la póliza propuesta?

SÍ ☐ NO ☐

En caso afirmativo, proporcione detalles:

_____
_____
_____
_____

CUESTIONARIOS ANEXOS O COMPLEMENTARIOS

En caso de serle remitidos cuestionarios anexos o complementarios del presente, deberá igualmente diligenciarlos y sus preguntas y respuestas a las mismas se considerará parte integrante de este cuestionario a todos los efectos.

DECLARACIÓN **(Lea atentamente la siguiente declaración antes de firmar en el lugar indicado)**

El hecho de rellenar este formulario de propuesta no obliga a la(s) compañía(s) ni a la(s) aseguradora(s) a suscribir un contrato de seguro, pero, si se emite una póliza, este formulario de propuesta, junto a cualquier otra información proporcionada antes de la entrada en vigor de esta, formará parte del contrato de seguros que se suscriba.

Declaramos que la información contenida en este formulario de oferta es verdadera y que no se ha distorsionado o suprimido ningún hecho sustancial después de la investigación. Aceptamos que este formulario de propuesta, junto con cualquier otra información facilitada, formará parte del contrato de seguros que se suscriba. Nos comprometemos a informar a la(s) aseguradoras de cualquier cambio sustancial que se produzca antes de suscribir el contrato de seguro

Firma del representante Legal _____

Nombre: _____

Fecha: _____

Tomador de la Póliza: _____