CUESTIONARIO SOLICITUD DE SEGURO

SOLI CYBER EMPRESARIAL

SEGMENTO 1 (INGRESOS USD 0 a USD 5M)

LA PÓLIZA PARA LA CUAL ESTA ELABORADO ESTE CUESTIONARIO SOLICITUD DE SEGURO cubre únicamente LAS RECLAMACIONES que se formulen CONTRA EL ASEGURADO por primera vez DURANTE EL PERIODO de seguro O EL PERIODO DE DESCUBRIMIENTO ADICIONAL (EN caso de ser aplicable) Y que se notifiquen A LOS ASEGURADORES CONFORME A LO ESTIPULADO BAJO LA PÓLIZA. LOS GASTOS DE DEFENSA INCURRIDOS BAJO LA PÓLIZA REDUCIRÁN Y PODRAN AGOTAR EL LÍMITE AGREGADO DE INDEMNIZACIÓN Y QUEDAN SUJETOS A LAS FRANQUICIAS ESTIPULADAS BAJO LA MISMA.

Por favor responda de forma completa a todas las preguntas de este Cuestionario Solicitud de Seguro y presente toda la información/documentación complementaria solicitada. Los términos que aparecen en negrita y en cursiva en este Cuestionario Solicitud de Seguro se encuentran definidos en la Póliza y en el Suplemento adjunto a la misma y tienen el mismo significado tanto en la Póliza y en el Suplemento como en este Cuestionario Solicitud de Seguro. Si no tiene una copia de la Póliza, por favor, solicítela a su intermediario o corredor. La información obtenida mediante este Cuestionario Solicitud de Seguro y mediante toda la información/documentación complementaria será confidencial.

1. INFORMACIÓN DE LA EMPRESA

- Nombre legal: CORPORACIÓN PARA EL DESARROLLO SOSTENIBLE DEL SUR DE LA AMAZONIA
- Dirección comercial: Cra 17 N 14-85 Barrio La Esmeralda Mocoa Putumayo
- Industria: Sector Publico
- Sitio web: https://www.corpoamazonia.gov.co/index.php
- Ingresos anuales: $30.851.108.591,8

2. CONTROLES DE CIBERSEGURIDAD

1. ¿Tiene software antivirus instalado en todos los dispositivos? SI
2. ¿Utiliza Autenticación Multifactor (MFA) para accesos remotos? SI
3. ¿Realiza copias de seguridad de los datos regularmente? NO
4. ¿Cuenta con un firewall para proteger su red? SI
5. ¿Usa políticas de contraseñas seguras (ej., longitud mínima, complejidad)? SI

3. CONTINUIDAD DEL NEGOCIO Y RESPUESTA A INCIDENTES

6. ¿Tiene un plan formalizado de respuesta a incidentes? NO

7. ¿Ha realizado capacitación en ciberseguridad para los empleados en los últimos 12 meses? NO
8. ¿Utiliza un proveedor externo de servicios de TI o ciberseguridad? NO

4. PROTECCIÓN DE DATOS Y PRIVACIDAD

9. ¿Almacena información personal identificable (PII) o datos financieros? NO
10. Si la respuesta es sí, ¿cuántos registros maneja aproximadamente?

5. INCIDENTES CIBERNÉTICOS ANTERIORES

11. ¿Ha experimentado un incidente cibernético (ej., filtración de datos, ransomware) en los últimos 3 años? NO
12. Si la respuesta es sí, proporcione detalles:

6. NECESIDADES DE COBERTURA

13. Límite de póliza deseado: [COP $2.000.000.000]

7. DECLARACIÓN PARA SER LEÍDA, FIRMADA Y FECHADA POR EL SOLICITANTE:

El Solicitante establece que, en caso de que la información proporcionada a través de este Cuestionario Solicitud de Seguro cambiara entre la fecha en la que se firma este Cuestionario Solicitud de Seguro y la fecha de efecto de la Póliza, procederá a notificar inmediatamente a los Aseguradores dichos cambios, de cara a que la información sea precisa, y los Aseguradores podrán cancelar o modificar cualquier cotización excepcional o autorizaciones o acuerdos que comprometan el seguro.

La firma de este **Cuestionario Solicitud de Seguro** no obliga al Solicitante ni a los Aseguradores a suscribir el Contrato de Seguro, sin embargo, se acuerda que este **Cuestionario Solicitud de Seguro**, así como cualquier otra documentación adjunta, se incorporarán y formará parte de la Póliza emitida. **Los Aseguradores están autorizados a realizar cualquier investigación, que consideren necesaria, en relación con este Cuestionario Solicitud de Seguro.**

Yo/Nosotros declaro/declaramos que hemos leído este **Cuestionario Solicitud de Seguro,** incluyendo el "Anexo A" (en su caso), y que, de acuerdo con mi/nuestro saber y entender, las contestaciones contenidas en este **Cuestionario Solicitud de Seguro** y en el Anexo A (en su caso) son verdaderas y completas, que he/hemos revelado todos los hechos importantes y que no hemos falseado ningún dato. Yo/Nosotros declaro/declaramos que cualquier información facilitada por otra persona distinta a mi/nosotros, ha sido otorgada por mi/nuestro agente.

Asimismo, entiendo/entendemos que los Aseguradores establecen las condiciones basándose en la información contenida en este **Cuestionario Solicitud de Seguro**.

Firma del Solicitante: Sidaly Ortega Gomez

Nombre: SIDALY ORTEGA GOMEZ

Cargo: DIRECTORA GENERAL Fecha: 29/07/2026

GLOSARIO:

1. Sistema de pre-screen:

- Definición: Un sistema que filtra o analiza datos entrantes (como correos electrónicos o archivos) antes de que ingresen a la red interna de una organización.
- Relevancia: Un sistema de pre-screen efectivo puede ayudar a prevenir la entrada de malware y reducir el riesgo de un incidente de seguridad, lo cual puede influir en las primas de seguro y la cobertura.

2. Sandbox:

- Definición: Un entorno aislado y seguro donde se pueden ejecutar programas o archivos sospechosos sin riesgo de dañar el sistema principal.
- Relevancia: Las sandboxes permiten analizar el comportamiento de software desconocido y detectar amenazas potenciales antes de que puedan causar daños, lo que puede reducir los costos de respuesta a incidentes y mejorar la capacidad de recuperación.

3. SPF (Sender Policy Framework):

- Definición: Un mecanismo de autenticación de correo electrónico que permite a los propietarios de dominios publicar una lista de servidores autorizados a enviar correos electrónicos en su nombre.
- Relevancia: SPF ayuda a prevenir el envío de correos electrónicos fraudulentos (phishing) desde dominios falsificados, lo que reduce el riesgo de que los empleados caigan en trampas y se produzcan brechas de seguridad.

4. Usuarios EPP (Endpoint Protection Platform):

- Definición: Usuarios que utilizan una plataforma de protección de endpoints, que incluye software y servicios para proteger dispositivos como computadoras, laptops y dispositivos móviles de amenazas como malware, ransomware y ataques de phishing.
- Relevancia: El uso de EPP por parte de los usuarios puede reducir significativamente el riesgo de infección y los costos asociados a un incidente de seguridad, lo que puede influir en las primas de seguro y la cobertura.

5. Producto EDR (Endpoint Detection and Response):

- Definición: Una solución de seguridad que va más allá de la protección tradicional de endpoints al proporcionar capacidades avanzadas de detección, investigación y respuesta a amenazas.
- Relevancia: EDR permite a las organizaciones detectar y responder rápidamente a amenazas avanzadas, lo que puede minimizar el impacto de un incidente de seguridad y reducir los costos de recuperación.

6. MFA (Multi-Factor Authentication):

- Definición: Un método de autenticación que requiere el uso de dos o más factores de verificación independientes (como contraseñas, tokens, biometría) para acceder a sistemas o aplicaciones.
- Relevancia: MFA agrega una capa adicional de seguridad a las cuentas de usuario, dificultando el acceso no autorizado incluso si las contraseñas se ven comprometidas.

7. Sistemas Legacy:

- Definición: Sistemas informáticos antiguos o obsoletos que ya no reciben soporte del proveedor.
- Relevancia: Los sistemas legacy pueden presentar vulnerabilidades de seguridad significativas debido a la falta de actualizaciones de seguridad y parches. Las pólizas de seguro pueden tener exclusiones o condiciones especiales para sistemas legacy.

8. Host-based y Firewalls:

- Definición:
  - Host-based: Sistemas de seguridad que se instalan directamente en los dispositivos (hosts) para protegerlos de amenazas.
  - Firewalls: Dispositivos o software que controlan el tráfico de red entrante y saliente, bloqueando el acceso no autorizado.
- Relevancia: Tanto los sistemas host-based como los firewalls son componentes fundamentales de una estrategia de seguridad sólida y pueden ayudar a prevenir la entrada de amenazas y reducir el riesgo de un incidente de seguridad.

9. Sistema de Protección DNS:

- Definición: Un sistema que protege el sistema de nombres de dominio (DNS) de ataques como el envenenamiento de DNS, que puede redirigir el trafico web a sitios maliciosos.

- Relevancia: Un sistema de protección DNS ayuda a prevenir que los usuarios accedan a sitios web maliciosos y se infecten con malware, lo que reduce el riesgo de un incidente de seguridad.

10. Ataques de Ransomware:

- Definición: Ataques cibernéticos que cifran los archivos de un sistema y exigen un pago de rescate para descifrarlos.
- Relevancia: Los ataques de ransomware pueden tener un impacto significativo en las operaciones de una organización, incluyendo la pérdida de datos, la interrupción del negocio y los costos de recuperación. Las pólizas de seguro de ciberseguridad pueden cubrir los costos asociados a un ataque de ransomware, como el pago del rescate (en algunos casos), los costos de recuperación de datos y los gastos de respuesta a incidentes.

11. PCI - Payment Card Industry:

- Definición: Un conjunto de estándares de seguridad establecidos por el PCI Security Standards Council para proteger los datos de las tarjetas de pago.
- Relevancia: Las organizaciones que procesan datos de tarjetas de pago están obligadas a cumplir con los estándares PCI DSS. El incumplimiento de estos estándares puede resultar en sanciones financieras y legales, así como en un aumento en las primas de seguro de ciberseguridad.