SOLICITUD DE SEGURO DE RESPONSABILIDAD CIVIL
RIESGO CIBERNÉTICO - CYBER (GENERAL)

Se hace constar que el solicitante de este seguro declara conocer y aceptar íntegramente las Condiciones Generales y particulares que se aplicarán en la Póliza que solicita. Este cuestionario tiene el tenor de una declaración jurada.

Por favor diligencie todas y cada una de las siguientes preguntas que se le hacen ya que este cuestionario constituirá parte de la póliza según lo señalado en el artículo 1048 del Código de Comercio.

SUCURSAL

FECHA

04	11	2026

Todas las preguntas deben ser contestadas sin dejar espacios en blanco.

DATOS DEL SOLICITANTE

1. Datos Generales

Nombre de la entidad: Gobernación de Boyacá

Nit de la entidad: 891.800.498-1

Naturaleza jurídica de la entidad: Publica

Dirección / Ciudad: Tunja-CALLE 20 No 9-90

Página web: BOYACA.GOV.CO

Correo electrónico: contactenos@boyaca.gov.co

Número telefónico: (57 8) 7420150 (57 8) 7420220.

Cual es su principal servicio / Actividad? Publica

Nombre de las subsidiarias en caso de requerir que figuren como asegurados adicionales: N/A

Fecha de constitución:	Número de empleados:
	661

INFORMACIÓN RELACIONADA CON SEGUROS

1. Información relacionada con seguros

Informe si tiene actualmente contratadas alguna de las siguientes pólizas:

Ramo	Aseguradora	Límite asegurado	Vigencia desde	Vigencia hasta
Responsabilidad Civil Servidores Públicos	Seguros del Estado	6.000.000.000	30/11/2025	05/12/2026 24 :00 h
Manejo Global	Seguros del Estado	1.000.000.000	30/11/2025	05/12/2026 24:00 h
Infidelidad y Riesgos Financieros	Seguros del Estado	1.000.000.000	30/11/2025	05/12/2026 24:00 h
R. Civil Directores y Administradores	Seguros del Estado	5.000.000.000	30/11/2025	05/12/2026 24:00 h
Cyber	Previsora	500.000.000	01/12/2025	06/12/2026 24:00 h

2. Límite asegurado requerido (Indicar el monto requerido): 1.000.000.000

INFORMACIÓN FINANCIERA:

4. Por favor completar la siguiente tabla de ingresos

4.1. Moneda | pesos | (indicar el tipo de moneda)

Estados
Financieros para:

Geografía	Último año Contable	Año Actual (Estimado)	Próximo año (Estimado)
Colombia	2025	2026	2027
UK / Europa			
USA / Canada			
Resto del Mundo			

4.2. Porcentaje de ingresos anuales brutos contabilizados por ventas u operaciones a través de su sitio web	N/A
4.3. Valor promedio de las transacciones	N/A
4.4. Estimación del presupuesto anual para el área de Tecnología	N/A
4.5. Ingresos anuales por ventas en Internet (servicios de comercio	N/A

INFORMACIÓN DE RED:

5. Dependencia de la red

5.1. ¿Cuáles son las funciones de los sistemas de información subcontratados?

			Proveedor de servicios (subcontratista)
Gestión de Escritorio	SI ☐	NO ☒	El area de soporte de la dirección de sistemas
Gestión del servidor	SI ☒	NO ☐	Algunos servicios web están en la nube con terceros autorizados
Gestión de Red	SI ☒	NO ☐	Servicio de internet y telefonía IP con operador externo y adicionalmente el equipo de TI de la Dir de sistemas
Gestión de Seguridad de la Red	SI ☐	NO ☒	La gestión de la seguridad se hace internamente desde la Dir de sistemas
Gestión de aplicaciones	SI ☒	NO ☐	Algunas aplicaciones se encuentran en la nube y con soporte de terceros

5.2. Indique cuanto tiempo después de que sus empleados se encuentren imposibilitados para para acceder a su red y sistemas informáticos internos, tendría un impacto significativo en su negocio:

Inmediato ☒ Después 6 hrs ☐ Después 24 hrs ☐ Después 48 hrs ☐ Nunca ☐

5.3. Indique cuanto tiempo después de que sus clientes se encuentre imposibilitados para acceder a su sitio web, tendría un impacto significativo en su negocio:

Inmediato ☒X Después 6 hrs ☐ Después 24 hrs ☐ Después 48 hrs ☐ Nunca ☐

5.4. Proporcione una estimación del impacto financiero para su empresa (en porcentaje) si se presentara una interrupción o falla de su red tecnológica.

0 - 12h	12 - 24h	24h +
30 %	60 %	90%

5.5. En función de la pregunta anterior y en caso de presentarse una interrupción o falla de su red tecnológica, describa las acciones que tomaría para mitigar el impacto financiero de tal interrupción.

Plan de contingencia: acción inmediata a procedimientos establecidos para restablecer los servicios

Usar los backups diarios en servidores alternos, monitoreo con análisis del incidente, identificación de causas y medidas de mitigación adicionales

Garantizar servicio de internet y conexión a VPN seguras

Priorización de servicios como el correo institucional, sistemas financieros, SECOP, sistema de gestión documental, mesa de ayuda y soporte técnico extendido con el fin de atender incidentes de forma inmediata y reducir los tiempos de respuesta.

PLAN DE ACCIÓN

6. CONTINUIDAD DEL NEGOCIO

6.1. Usted tiene:

			Frecuencia del Test
Plan de respuesta a Indicentes	SI ☒X	NO ☐	Anual
Plan de recuperación de desastres	SI ☒X	NO ☐	Anual
Plan de continuidad del negocios	SI ☒X	NO ☐	Anual

6.2. ¿Estos planes abordan el potencial de interrupciones de la red / sistema? SI ☒X NO ☐

6.3. Indique el tiempo objetivo de recuperación para la restauración del sistema. (Ej 2 a 6 horas aproximadamente

6.4. ¿Ha realizado en el último año auditoría de seguridad informática? SI ☐ NO ☒X

Si la respuesta es "Sí", ¿quién lo hizo y cuándo se realizó?

Auditado por: Fecha:

6.5. Indique si en el informe de auditoría se identificaron hallazgos u oportunidades de mejora y remitir el plan de acción para las mismas

6.6. ¿Cuándo fue su última práctica (PEN TEST O TEST DE PENETRACIÓN) para poner a prueba su sistema informático o red para encontrar vulnerabilidades que un atacante podría explotar?

6.7. En función a la respuesta del numeral anteiror, se identificó algun hallazgo u oportunidad de mejora frente a algún aspecto de la red en el que se aconsejó una corrección inmediata?	SI ☐	NO ☒
6.8. En caso afirmativo, ¿se ejecutaron las recomendaciones?	SI ☐	NO ☒

SEGURIDAD

7. SEGURIDAD DE RED

7.1. ¿La empresa cuenta con un directivo responsable del manejo y cumplimiento de las Leyes de privacidad y protección de datos?	SI ☒	NO ☐
7.2. ¿Tiene política de seguridad y privacidad de datos o manejo de redes informáticas?	SI ☒	NO ☐
7.3. ¿Está capacitado el personal de su empresa respecto a las prácticas de seguridad de la información?	SI ☒	NO ☐
7.4. ¿Se analizan todos los cargos de trabajo y se asignan a los empleados derechos, privilegios e ID de usuario y contraseñas únicos, que se cambian periódicamente?	SI ☒	NO ☐
7.5. ¿Tiene procedimientos estrictos de revocación de usuarios en las cuentas de usuario y recuperación de inventario de todos los activos de información después de la terminación del empleo?	SI ☒	NO ☐
7.6. ¿El personal tiene que actualizar regularmente sus contraseñas?	SI ☒	NO ☐
7.7. ¿Se requiere autenticación dual / multifactor para acceder a sistemas críticos?	SI ☒	NO ☐
7.8. ¿Hace cumplir las disposiciones por incumplimiento por parte de empleados, contratistas y otros?	SI ☒	NO ☐
7.9. ¿Tiene software antivirus en todos los dispositivos informáticos, servidores y redes que se actualizan de acuerdo con las recomendaciones de los proveedores de software?	SI ☒	NO ☐
7.10. ¿Tiene firewalls y detección de monitoreo de intrusos en vigor para prevenir y monitorear el acceso no autorizado?	SI ☒	NO ☐

7.11. ¿Tiene procedimientos de control de acceso y encriptación de disco duro para evitar la exposición no autorizada de datos en todas las computadoras portátiles, PDA, teléfonos inteligentes (por ejemplo, BlackBerry) y PC en el hogar? SI ☒X NO ☐

7.11. ¿Ha configurado su red para garantizar que el acceso a datos confidenciales se limite a solicitudes debidamente autorizadas? SI ☒X NO ☐

7.12. ¿Se asegura de que todas las redes inalámbricas tengan acceso protegido? SI ☒X NO ☐

7.13. ¿Se instalan y actualizan los parches críticos de manera oportuna? SI ☒X NO ☐

SISTEMA DE INFORMACIÓN

8. MANEJO DE INFORMACIÓN Y

8.1. ¿Recopila y almacena información personal sobre sus clientes / proveedores? SI ☐ NO ☒X

En caso afirmativo, indique el número de registros por tipo de información que se recopila y almacena:

	No. Estimado de registros		**No. Estimado de registros**
Nombre		Detalles de tarjeta de crédito / pago	
Dirección		Licencia de conducir / pasaporte /	
Número de teléfono		Información de salud	
Detalles bancarios		Otros datos personales (descríbalos en una hoja aparte)	

8.2. Estime la mayor cantidad de información personal identificable (PII) almacenada en su base de datos.

8.3. Si actúa como procesador de pagos, indique la cantidad de registros procesados en el año anterior.

8.4. ¿Comparte alguna información personal identificable (PII) con terceros con fines comerciales? SI ☐ NO ☒X

8.5. ¿Su programa de activos de información incluye un estándar de clasificación de datos (p. Ej., Público, solo para uso interno, confidencial)? SI ☒X NO ☐

8.6. Publica una política de privacidad en su sitio web? SI ☒X NO ☐

8.7. ¿Tiene un inventario de activos de información que enumere los propietarios y las fuentes de todos los datos? SI ☒X NO ☐

8.8. ¿Tiene una Política de protección de datos para transmitir datos fuera de Colombia?	SI ☐	NO ☒X
8.9. ¿Tiene procedimientos vigentes para cumplir con las solicitudes de "exclusión voluntaria" de marketing específicas de sus clientes que sean consistentes con los términos de su política de privacidad publicada?	SI ☐	NO ☒X
8.10. ¿Tiene procedimientos vigentes para monitorear el período durante el cual se conservan los datos del cliente y tiene procesos para eliminar esta información al final de ese período?	SI ☐	NO ☒X
8.11. ¿Tiene procedimientos vigentes y establecidos para eliminar todos los datos sensibles de los sistemas y dispositivos de la empresa antes de su eliminación definitiva?	SI ☐	NO ☒X
8.12. ¿Toda la información almacenada en forma física (papel, discos, CD, etc.) se elimina o recicla mediante métodos confidenciales y seguros reconocidos en toda la organización?	SI ☒X	NO ☐
8.13. ¿Mantiene un registro de incidentes de todas las brechas de seguridad del sistema y fallas de la red?	SI ☒X	NO ☐
8.14. ¿Ha identificado todos los marcos de cumplimiento normativo y de cumplimiento de la industria relevantes?	SI ☒X	NO ☐
8.15. Detalle cualquier certificación / acreditación de seguridad obtenida, p. Ej. ISO27001, ISO3100 HIPAA	SI ☐	NO ☒X

Si la respuesta es "Sí", especifique cuáles se han obtenido. _____

_____

_____

_____

8.16. Controles de protección de la información personal

a. El acceso a los datos personales está restringido solo a aquellos usuarios que los necesiten para realizar su tarea y las autorizaciones de acceso se revisan periódicamente.	SI ☒X	NO ☐
b. Los datos personales se cifran cuando se almacenan en sistemas de información y las copias de seguridad de datos personales están cifrados.	SI ☒X	NO ☐
c. Los datos personales se cifran cuando se transmiten a través de la red.	SI ☒X	NO ☐
d. Los dispositivos móviles y los discos duros de las computadoras portátiles están encriptados.	SI ☐	NO ☒X

e. La política de manejo e información de datos prohíbe la copia de datos personales no cifrados a dispositivos de almacenamiento extraíbles o la transmisión de dichos datos por correo electrónico. SI ☐ NO ☒

8.17. Si los registros personales que se conservan contienen información de tarjetas de pago (PCI), responda lo siguiente:

Su nivel de PCI DSS Nivel 1 ☐ Nivel 2 ☐ Nivel 3 ☐ Nivel 4 ☒

8.18. El procesador de pagos (usted mismo o un tercero) cumple con PCI DSS SI ☐ NO ☒

8.19. PCI se almacena encriptado o solo se almacena una parte de los números de tarjetas de pago.

N/A

8.20. El tiempo de retención de PCI no excede la duración del pago y los requisitos legales / reglamentarios. SI ☐ NO ☒

8.21. El procesamiento de los datos de las tarjetas de pago se terceriza. SI ☒ NO ☐

8.22. Usted requiere que el procesador de pagos le indemnice en caso de violación de seguridad. SI ☐ NO ☒

8.23. Indique el nombre del procesador de pagos, el tiempo de retención de PCI y cualquier medida de seguridad adicional: N/A

INFORMACIÓN SINIESTRAL

9. RECLAMACIONES Y CIRCUNSTANCIAS

9.1. Proporcione una descripción de cualquier incidente de seguridad o privacidad de la información que haya ocurrido en los últimos 5 años. Los incidentes incluyen cualquier acceso no autorizado a cualquier computadora, sistema informático, base de datos, intrusión o ataque, negación de uso de cualquier computadora o sistema, interrupción intencional, corrupción o destrucción de datos, programas o aplicaciones, cualquier evento de extorsión cibernética; o cualquier otro incidente similar a los anteriores, incluidos aquellos que han resultado en un reclamo, acción administrativa o procedimiento regulatorio.

(De ser necesario dar respuesta en hoja

FECHA	DESCRIPCIÓN DEL INCIDENTE

Comentarios

9.2. Confirme el impacto financiero que esto tuvo en su negocio. _____

9.3. Explique las medidas tomadas desde el incidente (s) para evitar que dicho evento vuelva a ocurrir.

ACLARACIONES

Es importante que el Representante Legal que firme esta declaración tenga un buen conocimiento del ámbito de esta cobertura para que las preguntas sean contestadas correctamente. En caso de duda rogamos contacten con La Previsora S.A. Compañía de Seguros, puesto que la no divulgación de información puede afectar a los derechos del Asegurado o pueda anular la Póliza

Previsora S.A. Compañía de Seguros queda autorizada para realizar cualquier indagación y consulta o solicitud de información que considere necesaria.

CIUDAD

FECHA 04 | 11 | 2026

NOMBRE DEL ORDENADO DEL GASTO

CARGO:SECRETARIA DE CONTRATACIÓN ENCARGADA

FIRMA ORDENADOR DEL GASTO

C.C. _____