

# Chubb Cybersecurity

## Cuestionario de solicitud para la póliza de responsabilidad informática

Chubb de Colombia  
 Compañía de seguros S.A.  
**Nit. 860.034.520-5**  
 (En adelante conocido como el asegurador)

Cuestionario para ser estudiado por el **asegurador**. Por favor tenga presente que el limite de responsabilidad por el pago de daños y perjuicios se reducirá y podrá agotarse con el pago de los **“gastos de defensa”** los cuales serán aplicados contra el monto del deducible aplicable. La cobertura que otorga esta póliza difiere en algunos aspectos de las que otorgan otras pólizas. Antes de firmar, lea íntegra y cuidadosamente el **cuestionario de solicitud** de seguro.

### Instrucciones relativas al cuestionario de solicitud de seguro

- Siempre que se utilice en este **Cuestionario de Solicitud** de negocios nuevos, se entenderá por el término **“Solicitante”** la **Casa Matriz** y todas sus **Subsidiarias**, a no ser que se establezca lo contrario.
- Incluya toda la información de suscripción solicitada y sus anexos. Suministre una respuesta completa a todas las preguntas y anexe páginas adicionales de ser necesario.
- Anexe lo siguiente:
  - Estados Financieros anuales más recientes, auditados, si se realizan auditorías externas;
  - Experiencia del personal clave, si el **solicitante** ha estado activo en el negocio por menos de tres (3) años;

### I. Nombre, dirección e información de contacto

- Nombre del **solicitante**:
- Dirección del **solicitante**:
- Ciudad:  Dpto. / Estado:  País:
- Página web del **solicitante**:
- ¿Existen otras compañías subsidiarias, afiliadas o demás persona(s) jurídica(s) relacionadas (incluyendo las que operan bajo el nombre comercial) para las que se desee cobertura?  
 Sí  No

Si la respuesta es afirmativa, enumere todas las ubicaciones en una hoja aparte y adjúntela a este **Cuestionario de Solicitud**.

**Nota: No se ampara persona jurídica alguna que no esté enumerada en esta sección del “Cuestionario de Solicitud de Seguro” y que no sea nombrada específicamente como “Asegurado” en la “Póliza”.**

### II. Información de seguro

- Límites de Indemnización solicitados:   
 Para cada **Reclamo** o **Reclamos relacionados**: \$
- Período del seguro solicitado: Desde el:  hasta el:   
 ambas fechas a las 00:00 horas, en el domicilio de la **Casa Matriz**

### III. Información general del riesgo

#### 1. El solicitante es:

- Organización sin ánimo de lucro  Sociedad Limitada  
 Sociedad Anónima  Sociedad con oferta pública  
 Sociedad sin oferta pública  Otro:

2. Año de constitución:

#### 3. Actividad y naturaleza de los negocios del solicitante:

4. El **solicitante** opera alguna **Subsidiaria**, afiliada u otra(s) entidad (es) relacionadas (incluyendo Administradores de Bases de Datos - "Data Base Administrator - DBA")  Sí  No

Si la respuesta es "Sí", responder las siguientes preguntas:

- a) ¿Se desea cobertura para alguna de estas entidades?  Sí  No  
b) ¿Alguna de estas entidades participa en operaciones que no están relacionadas con la actividad principal del **solicitante**?  Sí  No

Si se respondió "Sí" a alguna de las anteriores preguntas:

Suministre una lista de todas esas entidades y sus operaciones en una hoja separada y anéxela a esta solicitud.

5. a) ¿Durante los últimos cinco años el **solicitante** ha realizado alguna fusión, adquisición o desinversión, o ha salido de una situación de quiebra (bancarrota)?  Sí  No  
b) ¿El **solicitante** cree que completará alguna de las operaciones anteriormente mencionadas en los próximos 12 meses?  Sí  No

Si la respuesta a alguna de las anteriores preguntas es "Sí":

Incluya una explicación en una hoja separada y adjúntela a esta solicitud. Incluya una descripción resumida del proceso de due diligence (debida diligencia) realizado en conexión con las responsabilidades y reclamaciones potenciales surgidas de cualquier evento anterior.

Si el **solicitante** adquirió a otra entidad, indique si la compra fue:

- Compra de activos únicamente o  
 Compra de activos y pasivos.

#### 6. a) Complete la siguiente información respecto al **solicitante**:

	Año fiscal anterior	Año fiscal actual proyección anualizada	Próximo año fiscal (Proyección)
i. Número de Empleados			
ii. Activos Totales	\$	\$	\$
iii. Ingresos Operacionales	\$	\$	\$
iv. Ingreso bruto derivado de servicios profesionales y productos y servicios tecnológicos (incluido en el punto iii. anterior)	\$	\$	\$

b) Informe el porcentaje de ingresos operacionales del año fiscal anterior que fueron recibidos fuera del país:  %

#### IV. Información del riesgo

##### A. Análisis operacional, políticas y procedimientos

1. ¿El **solicitante** recoge, almacena o procesa información de identificación personal u otra información confidencial? (ver las actividades listadas en el punto (b) siguiente)

Sí  No

Si la respuesta es “Si”:

- a) ¿Cuántos **registros** se mantienen, incluyendo pero sin limitarse a registros de los clientes, socios de negocios y empleados potenciales, actuales y pasados del **solicitante**?

- a) Marque todas las formas de información de datos personales o confidenciales que aplican:

- Información tarjetas crédito  Información Financiera  Información Personal  
 Información de clientes  Historia Clínica  Secretos Comerciales  
 Otra (Describe):

- c) ¿El **solicitante** tritura, destruye o elimina toda información de identificación personal u otra información confidencial escrita, impresa o electrónica una vez que se descarta o ya no se requiere?

Sí  No

- d) ¿El **solicitante** almacena información de identificación personal u otra información confidencial en dispositivos móviles?

Sí  No

Si la respuesta es positiva, ¿tiene el **solicitante** la capacidad de eliminar remotamente todo dato crítico de tales dispositivos?

Sí  No

2. ¿El **solicitante** ha implementado una política escrita de seguridad de la información que es aplicable a todas las unidades de negocio del **Solicitante**?

Sí  No

Si la respuesta es “Si”:

- a) ¿El **solicitante** somete a prueba la seguridad requerida por la política de seguridad al menos una vez por año?

Sí  No

- b) ¿El **solicitante** identifica y evalúa con regularidad nuevas amenazas y vulnerabilidades y realiza cambios a la seguridad de acuerdo a lo encontrado?

Sí  No

- c) ¿La política de seguridad de la información del **solicitante** incluye políticas para el uso y almacenamiento de información de datos personales u otra información confidencial en dispositivos móviles?

Sí  No

3. ¿El **solicitante** tiene un plan de continuidad del negocio y recuperación de desastres?

Sí  No

Si la respuesta es “Si”:

- a) ¿Se revisa y actualiza el plan al menos dos veces por año?

Sí  No

- b) ¿Se pone a prueba el plan al menos una vez por año?

Sí  No

- c) ¿Se han identificado problemas durante la revisión o la prueba del plan?

Sí  No

- d) ¿Cuánto tiempo le toma al **solicitante** restaurar las operaciones después de un ataque computarizado u otra pérdida/corrupción de datos?

4. ¿El **solicitante** tiene un plan de respuesta a incidentes por escrito, que establezca los procedimientos frente a incidentes de seguridad de la red o amenazas a la privacidad?

Sí  No

Si la respuesta es “Si” por favor liste los proveedores de servicios en caso de ataques informáticos y los consultores de seguridad y privacidad de las redes del **solicitante**:

5. ¿El **solicitante** usa actualmente o tiene planes de usar en el próximo año, los servicios de un proveedor de servicios de la nube (*cloud service provider*)?  Sí  No

Si la respuesta es “Si” complete lo siguiente:

- a) ¿Qué impacto tendría la interrupción o cesación de tales servicios en la capacidad del **solicitante** de cumplir con las obligaciones contractuales con sus clientes?

Ninguna  Leve  Significativa

- b) ¿El plan de continuidad del negocio y recuperación de desastres, contempla específicamente la restauración y recuperación de las operaciones del negocio suministradas por un proveedor de servicios de la nube (*cloud service provider*)?  Sí  No

## B. Cobertura de responsabilidad informática

1. ¿Cuántos servidores son de propiedad del **solicitante** o tiene dedicados para su uso?

2. ¿Los servidores web del **solicitante** tienen acceso directo a información de datos personales u otra información confidencial?  Sí  No

3. ¿El **solicitante** está sujeto a alguna ley o regulación respecto a privacidad o salvaguarda de información de identificación personal u otra información confidencial diferente a la Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales?  Sí  No

Si la respuesta es “Si”, indique las leyes o regulaciones

Si la respuesta es “Si”, ¿el **solicitante** cumple con las leyes o regulaciones?  Sí  No

Si la respuesta es “No” explique por qué se presenta el incumplimiento:

## Cumplimiento de los estándares PCI

1. ¿El **solicitante** está sujeto al estándar de seguridad de la Industria de Tarjetas de Pago - Payment Card Industry Data Security Standard, (PCI DSS)  Sí  No

Si la respuesta es “Si”:

- a) ¿El **solicitante** cumple con dichos estándares PCI DSS?  Sí  No

Si el **Solicitante** no cumple con los estándares, por favor anexe una explicación.

- b) ¿Cuántas transacciones de tarjetas de crédito o débito procesa el **solicitante** anualmente?

### c) El **solicitante**:

- (i) ¿Oculta todos los dígitos salvo los últimos cuatro del número de una tarjeta cuando muestra o imprime datos del tarjetahabiente?  Sí  No

- (ii) ¿Se asegura de que los códigos de validación de la tarjeta no estén almacenados en ninguna de las bases de datos, archivos de registro (*log files*) del **solicitante** o en cualquier lugar dentro de su red?  Sí  No

- (iii) ¿Encripta toda la información de las cuentas que se encuentran en las bases de datos del **solicitante**?  Sí  No

- (iv) ¿Encripta o usa tokens para toda la información de las cuentas en el punto de venta (POS)?  Sí  No

## Entrenamiento y Evaluaciones de Seguridad de la Información

1. ¿El **solicitante** emplea un oficial designado de seguridad de la información o equivalente?  Sí  No

Si la respuesta es “No”:

¿Quién es la persona dentro de la organización que ha sido designada para administrar e implementar las políticas, procedimientos y procesos de seguridad?

2. ¿El **solicitante** emplea a un oficial encargado de la privacidad de datos o equivalente?  Sí  No

Si la respuesta es “No”:

¿Qué rol en la organización del **solicitante** es responsable por la administración y cumplimiento de las políticas de privacidad de datos del **solicitante**?

3. El **solicitante** tiene firewalls que filtran tanto el tráfico entrante como saliente?  Sí  No

4. ¿Se han instalado programas anti-virus en todos los computadores, redes, sistemas y dispositivos móviles del **solicitante**?  Sí  No

Si la respuesta es “Si”:

¿Qué tan frecuentemente se actualizan los programas de detección de virus?

5. ¿El **solicitante** emplea dispositivos de detección o protección de intrusiones en sus redes, o en el software de control de acceso - IDS o IPS ?  Sí  No

Si la respuesta es “Si”:

¿Qué tan frecuentemente se revisan los logs (registros)?

6. ¿El **solicitante** realiza tests de penetración o pruebas de vulnerabilidad en todas las partes de su red?  Sí  No

Si la respuesta es “Si”:

¿Con qué frecuencia se realizan estos tests o pruebas?

7. ¿El **solicitante** desarrolla parches de software?  Sí  No

Si la respuesta es “Si”:

¿Quién realiza esos parches de software y con qué frecuencia?

8. ¿El **solicitante** tiene herramientas de encriptación para mejorar la integridad y confidencialidad de la información de datos personales u otra información confidencial?  Sí  No

Si la respuesta es “Si”:

¿En cuáles escenarios se encriptan los datos? (marque todos los que aplican)

- Datos en reposo
- Datos en Tránsito
- Datos transferidos a medios de comunicación removibles (ej. CDs, Cintas de Backup, Dispositivos USB, etc.)

9. ¿El **solicitante** entrena a sus empleados y a otros usuarios autorizados, en temas de seguridad de redes y privacidad incluyendo responsabilidades legales y amenazas tales como ingeniería social (ej. Phishing), correo no deseado (spam), búsqueda en cestos de basura (dumpster diving) etc.?  Sí  No

Si la respuesta es “Si”:

Describe el método y la frecuencia del entrenamiento:

10. ¿Se ha realizado en los últimos doce (12) meses una evaluación externa de la seguridad del sistema, diferente a tests de penetración o pruebas de vulnerabilidad?  Sí  No

Si la respuesta es “Si”:

Indique quien llevó a cabo la evaluación, anexe copias del resultado e indique si todas las recomendaciones críticas han sido corregidas o se han cumplido.

Si la respuesta es “No” anexe una explicación

### Backup, Archivo y Proveedores de Servicio

1. ¿Qué tan frecuentemente el **solicitante** realiza back ups de datos electrónicos?

2. ¿El **solicitante** almacena los back ups de datos electrónicos con un tercero/proveedor de servicios en la nube (*cloud provider*)?  Sí  No

Si la respuesta es “Si”:

Indique el proveedor:

3. ¿El **solicitante** utiliza cualquier otro tercero proveedor de servicios de tecnología /proveedores de servicio en la nube (*cloud provider*)?  Sí  No

Si la respuesta es “Si”:

Indique el (los) proveedor (es) y el propósito:

Si la respuesta es “Si” a los puntos 2 o 3 anteriores:

¿Utiliza el **solicitante** contratos escritos con el (los) respectivo(s) proveedor (es) de servicio/proveedores de servicio en la nube (*cloud provider*)?  Sí  No

Si la respuesta es “Si” a los puntos 2 o 3 anteriores:

¿Revisa el **solicitante** la auditoria de seguridad más reciente del (los) proveedor(es) de servicios/servicios en la nube (*cloud provider*)? (ej. SSAE-16)  Sí  No

Si la respuesta es “Si” a los puntos 2 o 3 anteriores:

Los contratos que tiene el **solicitante** con el (los) proveedor(es) de servicios en la nube establecen que el (los) proveedor(es) de servicios/servicios en la nube:

a) ¿Tienen la responsabilidad principal de la seguridad de la información del **solicitante**?  Sí  No

b) ¿Son responsables contractualmente por perdida o gastos asociados con la falla en salvaguardar los datos electrónicos del **solicitante**?  Sí  No

### V. Historia de incidentes y siniestros

---

1. Para los propósitos de la cobertura que se solicita, ¿ha habido reclamaciones hechas durante los cinco (5) años anteriores o incidentes (*incluyendo incidentes de Seguridad o Privacidad de la Red*) en los últimos dos (2) años o pérdidas que afecten al **solicitante**?  Sí  No

Si la respuesta es “Si”:

Anexe una descripción completa de las reclamaciones, incidentes o pérdidas incluyendo confirmación de si el **solicitante** reportó el (los) incidente(s) al asegurador.

2. En los últimos cinco (5) años, ¿ha habido alguna investigación administrativa o criminal al **solicitante** por alguna autoridad gubernamental o regulatoria?  Sí  No

## VI. Conocimiento previo de hechos / circunstancias / situaciones

---

El **solicitante** debe completar la siguiente declaración de garantía:

Ninguna de las personas o entidades que solicitan la cobertura conoce hecho, circunstancia o situación alguna por el cual él o ella tengan razón para suponer que se podría dar lugar a alguna reclamación que caería bajo el alcance de la cobertura solicitada:

Ninguno  o excepto

Sin perjuicio de cualesquiera otros derechos o recursos del **asegurador**, el **solicitante** entiende y acuerda que si existe cualquiera de tales hechos, circunstancias o situaciones, sea o no divulgado en la respuesta a la pregunta anterior de la presente Sección VI, cualquier reclamación o acción que surja de tal hecho, circunstancia o situación está excluido de cobertura bajo la póliza solicitada, si se emite por el **asegurador**

## VII. Cambio sustancial

---

Si hubiere un cambio sustancial en las respuestas a las preguntas contenidas en este **Cuestionario de Solicitud de Seguro** antes de la fecha de inicio de vigencia de la póliza, el **Solicitante** debe notificarlo de inmediato al **Asegurador** por escrito, y se podrá retirar o modificar toda cotización pendiente.

## VIII. Declaraciones, advertencias sobre fraude y firmas

---

La presentación de este **Cuestionario de Solicitud de Seguro** por parte del **solicitante** no obliga al **Asegurador** a emitir una póliza, ni al **solicitante** a contratar el seguro. Se le informará al **solicitante** si el Cuestionario de Solicitud de Seguro es aceptado. El solicitante por el presente autoriza al Asegurador a llevar a cabo una investigación en relación con este **Cuestionario de Solicitud de Seguro**.

Los abajo firmantes, agentes autorizados de la(s) persona(s) natural(es) y jurídica(s) propuestas para este seguro, declaran a su leal saber y entender, y luego de realizadas las indagaciones razonables, que las declaraciones vertidas en este **Cuestionario de Solicitud de Seguro** y en cualesquiera adjuntos o información presentados junto con ella son veraces y completas.

Los abajo firmantes acuerdan que este **Cuestionario de Solicitud de Seguro** y sus anexos constituirán la base de un contrato si es que se emite una póliza que otorgue la cobertura solicitada, y se los considerará adjuntos a la **Póliza** en cuestión y parte integral de ella. Al emitir la **Póliza** el **Asegurador** habrá tomado como base este **Cuestionario de Solicitud de Seguro**, sus anexos y toda otra información presentada con ellos.

La información provista en este **Cuestionario de Solicitud de Seguro** se brinda con fines de suscripción solamente, y no constituye aviso de Reclamo o Reclamo potencial al **Asegurador** en virtud de póliza alguna.

Fecha	Firma	Cargo
<input type="text"/>	_____	Gerente General
<input type="text"/>	_____	Gerente Financiero o Gerente de Sistemas

\*Este **Cuestionario de Solicitud de Seguro** debe ser firmada por el Gerente General y el Gerente Financiero o Gerente de Sistemas del **Solicitante** en calidad de representantes autorizados de la persona o personas naturales jurídicas propuestas para este seguro.