

CYBER
PROPOSAL
FORM



CONTENIDO / CONTENTS

1. INFORMACION GENERAL
GENERAL INFORMATION
2. INFORMACION FINANCIERA
FINANCIAL INFORMATION
3. DEPENDENCIA DE LA RED
NETWORK DEPENDENCE
4. CONTINUIDAD DEL NEGOCIO
BUSINESS CONTINUITY
5. SEGURIDAD DE LA RED
NETWORK SECURITY
6. INFORMACIÓN Y GESTIÓN DE DATOS
INFORMATION AND DATA MANAGEMENT
7. SINIESTROS Y CIRCUNSTANCIAS
CLAIMS AND CIRCUMSTANCES

1. INFORMACION GENERAL GENERAL INFORMATION

1. Empresa Solicitante:

Company or trading name

La Previsora S.A. Compañía de Seguros

2. Tipo de Sociedad:

Type of company (Public, private, Mix Company, Cooperative, Non-profit)

Pública Public	Privada Private	Mixta Mixed	Cooperativa Cooperative	Sin Ánimo de Lucro Nonprofit
		X		

3. Dirección de la Empresa Solicitante (Incluyendo ciudad y país):

Address (Including city and country)

Calle 57 No. 9-07

4. Correo Electrónico:

E-mail

contactenos@previsora.gov.co

5. Página web:

Website

WWW. PREVISORA.GOV.CO

6. Fecha de fundación:

Date of Foundation

06 de Agosto de 1954

7. ¿Ha estado involucrado en alguna fusión o adquisición en los últimos 3 años?
Have you been involved in any mergers and acquisitions within the last 3 years?

SI/YES

NO

En caso afirmativo, por favor facilite detalles completos, si es necesario utilice una hoja adicional.

If the answer is 'Yes', please provide full details, on a separate sheet if necessary

NO APLICA

8. Descripción de su principal actividad/ servicios:
Main services/activities description

Su objeto social principal es celebrar y ejecutar contratos de seguros, coaseguros y reaseguros que amparen los intereses asegurables que tengan las personas naturales o jurídicas privadas, así como los que directa o indirectamente tenga la Nación, el Distrito Capital de Bogotá, los Departamentos, los Distritos, los Municipios y las Entidades Descentralizadas de cualquier orden, asumiendo todos los riesgos que, de acuerdo con la Ley puedan ser materia de estos contratos.

9. Composición accionaria de la Empresa solicitante:
Shareholding structure of the applicant company:

Nombre Name	% de Participación % of participation
Grupo Bicentenario SAS	99.71%
Demás accionistas Minoritarios	0.29%
Total	100.00%

10. ¿En qué país tiene presencia la empresa solicitante?
In which countries does the applicant company has presence?

Colombia

11. Número de empleados:
Number of employees

754

12. ¿En qué país tiene presencia la empresa solicitante?
In which countries does the applicant company has presence?

COLOMBIA

13. Filiales, subsidiarias o subordinadas propiedad de la Empresa Solicitante que se van incluir dentro de la póliza

Subsidiaries, affiliates or subordinates owned by the applicant Company that will be included in the policy

Nombre	Actividad	País de Origen	% de Participación	Ingresos Último Año	# Registros
No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica

14. ¿La Empresa Solicitante o sus filiales / subsidiarias tienen actualmente contratado un seguro similar o complementario al que se solicita?

Does the applicant Company or its subsidiaries / subsidiaries currently have similar or complementary insurance to the one requested?

SI / YES

NO

En caso afirmativo, por favor informe ramo, vigencia y Compañía.

If the answer is 'Yes', please provide line of business, period and Insurer.

15. Límites asegurados a cotizar (Favor incluir la moneda):
Requested Insured Limit (Please include the currency)

Opción 1: \$ 5,000,000,000

Opción 2:

Opción 3:

2. INFORMACIÓN FINANCIERA FINANCIAL INFORMATION

1. Por favor contestar las preguntas en la siguiente tabla.
Please answer the questions in the following table.

Favor especificar la moneda de los valores que se informan.
Please specify the currency of the values that are reported.

	Año anterior <i>Last Year</i>	Año actual <i>Current Year</i>	Proyección próximo Año <i>Projection</i> <i>next year</i>
Ingresos Brutos Anuales Gros annual revenue	2,610,993,114,449.78	3,252,201,424,752.10	
% de los ingresos página web % of the Annual Income or operations that made using a website	%	%	%
% Anual de transacciones realizadas con tarjetas de plástico. %of annual transactions paid for by debit/credit card.	%	%	%
% de Ingresos generados por clientes en EE.UU/ Canadá US/Canadian clients subject to US/Canadian Law.	%	%	%
País donde se concentra el mayor número de operaciones Country where the largest number of operations is concentrated.			
Que presupuesto agregado anual tiene para TI What annual aggregate budget do you have for IT?	\$28,786,736,490 COP (Total presupuesto de Gastos Tecnológicos aprobado para la vigencia 2022)	\$31,298,741,886 COP (Total presupuesto de Gastos Tecnológicos aprobado para la vigencia 2023)	Aún no existe presupuesto aprobado para la vigencia 2024
% del presupuesto para la seguridad informática? % of budget for computer security?	4.1%	4.7%	NA

% del presupuesto para los sistemas de seguridad % of budget for security systems	%	%	NA
--	---	---	----

2. Que tan representativo para sus ingresos son las ventas de internet.
How representative for your income are internet sales.

3. DEPENDENCIA DE LA RED

Network dependency

1. Qué porcentaje de la operación de su empresa, incluyendo filiales y subsidiarias, depende de los sistemas de cómputo?
What percentage of your business operation, including affiliates and subsidiaries, depend on computer systems?

100%

2. Por favor indicar el número de dispositivos individuales que tiene de TI (Ej. Servidores, computadoras de escritorio, computadores portátiles, equipos móviles)
Please indicate the number of individual devices that have IT (i.e. Servers, desktop PC, Laptops, and mobile devices)

2409

3. ¿Dispone la Compañía de servicios en nube o cloud computing?
Does the company have services in cloud or cloud computing?

SI / YES

NO

En caso afirmativo, detallar política de seguridad en nube, para seguridad de los datos personales y corporativos:

If yes, detail cloud security policy for personal and corporate data security.

Alineados a norma ISO27001 (datacenter) y CE005 –2019 (Superintendencia Financiera de Colombia)

Si la respuesta es NO, favor aclarar si se tienen planes de utilizar éstos servicios el próximo año

If the answer is NO, please clarify if there are plans to use these services next year

4. Después de cuánto tiempo sin acceso a su Red o Plataforma Tecnológica por parte de sus empleados se ocasionaría un impacto significativo en su negocio:
After how long without access to your Network or Technology Platform by your employees a significant impact on your business would be caused:

Inmediatamente Immediately	Después de 6 Horas After 6 hours	Después de 12 Horas After 12 hours	Después de 24 Horas After 24 hours	Después de 48 Horas After 48 hours	Otro Other
					4 Horas

5. Cuánto tiempo sin que sus clientes tengan acceso a su página web supondría un impacto significativo para su negocio:
How long without your customers having access to your website would have a significant impact on your business:

Inmediatamente Immediately	Después de 6 Horas After 6 hours	Después de 12 Horas After 12 hours	Después de 24 Horas After 24 hours	Después de 48 Horas After 48 hours	Otro Other
	X				

6. ¿En el evento en que ocurra una falla en el sistema, cual es el tiempo estimado de recuperación para las aplicaciones críticas del negocio?
In the event of a system failure, what is the estimated recovery time for critical business applications?

Inmediatamente Immediately	Después de 6 Horas After 6 hours	Después de 12 Horas After 12 hours	Después de 24 Horas After 24 hours	Después de 48 Horas After 48 hours	Otro Other
					4 HORAS

7. Subcontrata la gestión o algunas de sus operaciones tecnológicas?
Do you outsource the management or some of your technological operations??

SI / YES NO

En caso afirmativo, por favor facilite detalles, si fuera necesario, usar una hoja adicional, incluyendo qué tipo de subcontratación y a quién:

If the answer is 'Yes', please provide full details, on a separate sheet if necessary including what is outsourced and to whom

El Servicio de Datacenter (hosting y colocation) Se efectuó por contratación Abierta y la misma fue otorgada al proveedor de Comcel S.A

8. La Empresa Solicitante o sus filiales subcontrata empresas para funciones de administración de seguridad de la información?
The applicant Company or its subsidiaries outsource companies for information security management functions?

SI / YES NO

En caso afirmativo, por favor facilite detalles, si fuera necesario, usar una hoja adicional, incluyendo qué tipo de subcontratación y a quién:

If the answer is 'Yes', please provide full details, on a separate sheet if necessary, including what is outsourced and to whom:

Para la administración y control de temas de seguridad informática se cuenta con el proveedor O4IT el cual fue contratado por Invitación abierta.

9. ¿Subcontrata el solicitante actividades de proceso o recogida de datos?

Does the applicant outsource the processing or data collection activities?

SI / YES

NO

En caso afirmativo, por favor detalle las funciones de proceso o recogida de datos que son externalizadas:

If yes, please detail the process functions or data collection that are outsourced

10. Exigen a los contratistas y subcontratistas el cumplimiento de las políticas de seguridad y protección de datos de la empresa?

Do you require contractors and subcontractors to comply with the company's security and data protection policies

SI / YES

NO

En caso afirmativo, favor indique por medio de qué mecanismo exigen tal cumplimiento:

If yes, please indicate by means of which mechanism you require such compliance:

A nivel contractual se efectúan cláusulas de seguridad de la Información y controles aleatorios por el área de riesgos.

11. Exige a los contratistas o subcontratistas tener vigente una póliza de responsabilidad para la protección de datos?

Do you require contractors or subcontractors to have an active liability policy for data protection?

SI / YES

NO

12. ¿Realiza revisiones periódicas a sus proveedores de servicios y socios para comprobar que cumplen con sus requerimientos para la protección de la información sensible que manejan?

Do you periodically review your service providers and partners to verify that they meet your requirements for the protection of the sensitive information they handle?

SI / YES

NO

13. Se auditan periódicamente las funciones de subcontratistas / prestadores del servicio para asegurar que cumplen con las políticas de seguridad del Solicitante

The functions of subcontractors / service providers are periodically audited to ensure that they comply with the Applicant's security policies?

SI / YES

NO

4. CONTINUIDAD DEL NEGOCIO

Business continuity

1. Dispone de un plan de continuidad de negocio?
Do you have a Business Continuity Plan BCP?

SI YES

NO

En caso afirmativo por favor dar detalles del PCN:

If yes, please give details of the BCP:

Previsora Seguros S.A. ha reconocido el riesgo social, estratégico, operacional y financiero que tendría una eventual interrupción de los servicios y productos que brinda. Igualmente, reconoce la importancia que tiene, para todas las partes interesadas el hecho de mantener la continuidad de los procesos críticos, durante eventos adversos y situaciones de fuerza mayor que pudieran afectar el curso normal de sus actividades. Por ello, ha establecido un Plan de Continuidad de Negocio a fin de salvaguardar la integridad física de las personas, cumplir con los niveles de servicio, la normatividad vigente, los lineamientos organizacionales y la viabilidad financiera de la compañía.

Como fortalecimiento de este Plan de Continuidad de Negocio, la compañía ha implementado el Sistema de Gestión de Continuidad de Negocio (SGCN), alineado con la norma técnica ISO 22301.

El SGCN de Previsora, tiene como alcance todos los ramos de la compañía y los procesos críticos identificados en el Análisis de Impacto al Negocio (BIA¹)

2. Dispone de un plan de recuperación de desastres?
Do you have a Disaster Recovery Plan DRP?

SI / YES

NO

En caso afirmativo por favor dar detalles del plan y del manejo de crisis:

If yes, please give details of the DRP and crisis management:

Previsora tiene el proceso de DRP a cargo del proveedor Claro, quien cuenta con un lugar alternativo donde se encuentra infraestructura que soporta las aplicaciones que están dentro del BIA establecido y se tiene procedimientos documentados para habilitar estos servicios. La plataforma virtual se réplica a través de SRM de VMware y para los servidores los físicos se tienen en DCA equipos con las mismas características y los datos se replican a través del almacenamiento (SAN to SAN).

¹BIA: *Business Impact Analysis*. Proceso administrativo por medio del cual la organización analiza todos los impactos cuantitativos (financieros) y cualitativos (no financieros), sus efectos y pérdidas que pueda sufrir la organización provocados por un incidente o evento imprevisto que afecte la continuidad del negocio.

3. Cada cuánto tiempo son revisados estos planes?
How often are these plans tested?

Anualmente

4. Indique la persona(s) encargada para la ejecución y supervisión de dichos planes
Indicate the person(s) responsible for implementing and monitoring these plans.

GERENTE DE RIESGOS / GERENTE DE TI

5. Realiza regularmente auditoría a sus sistemas tecnológicos.
Do you regularly audit your technological systems.

SI / YES

NO

En caso afirmativo indicar la frecuencia y cuándo fue la última auditoría realizada:
If yes, indicate the frequency and when was the last audit carried out:

A nivel de entidad se efectúan un promedio de 5 auditorías al año por parte de control interno y procesos de entes externos, la última fue finalizada el 30 de Agosto del 2023

6. Cuándo se llevó a cabo la última prueba de vulnerabilidad externa en sus sistemas?
Cada cuanto se realizan estas pruebas?
When was your last external penetration test carried out? How often do you conduct these tests?

La última prueba de vulnerabilidad se efectuó en el mes de Agosto 2023 y esta se realiza cada 6 meses

7. Le ha surgido alguna preocupación sobre cualquier aspecto de la red en la que se aconsejó una subsanación inmediata
Have you been sort of concern about the network where immediate correction was advised?

SI / YES

NO

En caso afirmativo favor dar detalles:

If yes, please give details:

8. ¿Se realizan copias de seguridad periódicas?
Do you make periodical security backups?

SI / YES

NO

En caso afirmativo, favor indicar la periodicidad:
If yes, please indicate the periodicity:

Se tienen establecidos un cronograma de respaldos de acuerdo a lo requerido por las Aplicaciones. Hay backups de cierres mensuales, backups semanales y backups diarios.

9. ¿Se realizan copias de seguridad automáticas?
¿Are automatic backup copies made?

SI / YES

NO

10. ¿Usted es capaz de restaurar copias de seguridad de datos lo más rápidamente posible y con el menor impacto?

Are you able to restore security data backups as fast as possible to make less impact?

SI / YES

NO

11. Donde son almacenadas las copias de seguridad?
Where are backup copies stored?

Cintoteca proveedor externo

12. Confirmar si las copias de seguridad están guardadas fuera de línea (offsite)
Confirm if the backup copies are saved offline (offsite)

SI / YES

NO

De ser necesario favor suministrar detalles:
If necessary, please provide details:

Proveedor externo se envían las Cintas después de realizado el backup.

13. Cuánto tiempo estima usted para su RPO (Recovery Point Objective), el periodo entre dos copias de seguridad con una pérdida aceptada /aceptable de datos?

How much time do you estimate for your RPO (Recovery Point Objective), the period between two backups with an accepted / acceptable loss of data?

Inmediatamente Immediately	Después de 6 Horas After 6 hours	Después de 12 Horas After 12 hours	Después de 24 Horas After 24 hours	Después de 48 Horas After 48 hours	Otro Other
			x		

14. ¿Ha ejecutado un análisis de impacto empresarial (Business Impact Analysis “BIA”) teniendo en cuenta las amenazas relevantes de TI
Have you run a Business Impact Analysis (BIA) taking into account the relevant IT threats?

SI / YES

NO

5. SEGURIDAD DE LA RED

Network security

1. Tiene un Director de Cumplimiento (Chief Compliance Officer), responsable o supervisor de seguridad, o un responsable de protección de datos, o un supervisor de información encargado de la protección y seguridad de los datos y/o el cumplimiento interno de la legislación en materia de protección de datos?
 Do you have a Chief Compliance Officer, responsible or security supervisor, or a data protection officer, or an information supervisor in charge of data protection and security and / or internal compliance with the legislation in terms of data protection?
- SI / YES NO

En caso negativo por favor indicar quien es responsable por la política de protección y seguridad de datos.

If the answer is no, who is responsible for data protection and privacy issues?

2. Maneja un contrato estándar con los proveedores, contratistas o subcontratistas que incluya una cláusula de confidencialidad, y donde se exija el cumplimiento de las políticas de seguridad
 Do you use a standard contract with suppliers, contractors or subcontractors which includes a confidentiality clause, and where security policies compliance is required?
- SI NO

3. Incluyen en sus políticas un proceso por escrito para el cumplimiento de las políticas de seguridad y protección de datos?
 Do you include in your policies a written process for compliance with security and data protection policies?
- SI NO

4. Incluyen en sus políticas de seguridad y protección de datos un curso de formación obligatorio para todos los empleados
 Do you include in your security and data protection policies a mandatory training course for all employees
- SI / YES NO

En caso afirmativo por favor indicar el contenido:

If yes, please indicate the content:

Privacidad de dato Data Privacy		Temas de responsabilidad legal Legal liability	
Seguridad y protección informática	X	Social Engineering (Ej.: Spear phishing, whaling)	

Security protection and information			
Tendencias regulatorias Regulatory trends		Otro Other	

5. Es diferente la capacitación de seguridad en términos de los participantes (P. Ej.: Usuarios estándares o privilegiados, gerente de TI, ejecutivos etc.)?
Is security training different in terms of participants (eg, standard or privileged users, IT manager, executives, etc.)?

SI / YES

NO

En caso afirmativo favor dar detalles:

If yes, please give details:

6. Ha implementado un procedimiento que prepare a los empleados a ser más cautelosos y vigilantes respecto a phishing o en general a suplantación de identidad (Ej.: vincular de forma automática a un curso obligatorio (en línea) después de responder a un ataque simulado)?

Do you have implemented a procedure that prepares employees to be more cautious and vigilant in respect of Phishing or in general to identity theft (eg.: automatically link to a mandatory course (online) after responding to a simulated attack)?

SI / YES

NO

7. Las políticas y procesos de seguridad y protección de datos que implementa cumplen con la legislación vigente;

Do security and data protection policies and processes that you implement comply with current legislation?

SI / YES

NO

8. A todos los puestos de trabajo analizados, se les asigna un único usuario de acceso y clave que se modifica periódicamente?

All the analyzed jobs are assigned with a single access user and password that is modified periodically?

SI / YES

NO

9. ¿Se revisa su política de protección de los datos y se ajusta en función de las nuevas amenazas?

Is your data protection policy reviewed and adjusted for new threats?

SI / YES

NO

10. ¿Cuándo fue actualizada por última vez la política de Seguridad de la información?

When was the last time that data security policy was update?

11. ¿Cuándo fue actualizada por última vez la política de privacidad de la información?
When was the last time that information privacy policy was update?

08/sep./2022

12. Tiene procedimientos estrictos de revocación de acceso a usuarios cuyo contrato de trabajo haya finalizado?

Do you have strict procedures for revocation of access to users whose employment contract has ended?

SI / YES

NO

13. De acuerdo con la pregunta anterior hay acceso al histórico de información utilizada por dicho empleado

According to the previous question, is there access to historical information used by the employee?

SI / YES

NO

14. Tiene software antivirus actualizado en todos sus ordenadores, servidores y redes de acuerdo con las recomendaciones de sus proveedores de software

Do you have updated antivirus software on all your computers, servers and networks according to the recommendations of your software vendors

SI / YES

NO

15. Utilizan Firewall (Sistemas de prevención de intrusiones)

Do you use Firewall

SI / YES

NO

16. Las subsidiarias, filiales o subordinadas de la empresa solicitante utilizan firewall

Do your affiliates or subsidiaries use Firewall?

SI / YES

NO

17. En qué equipos o dispositivos utilizan Firewall (Móviles, sitios web, computadores)

In which computers or devices does the company use Firewall (Phones, websites, computers)

En equipos, servidores y sitios web

18. Tiene política de aplicación de parches?

Do you have patch application policy?

SI / YES

NO

19. Cada cuanto aplica los parches?
How often do you apply the patches?

Automático Automatic	Mensual	Bimensual	Trimestal	Otro (favor especificar) Other (please specify)
			X	

20. ¿Tiene un plan de respuesta a incidentes de violaciones de datos, intrusiones de redes o infecciones de virus informático?
Do you have an incident response plan for data breaches, network intrusions or computer virus infections?

SI / YES NO

21. ¿Se revisa y actualiza regularmente este plan?
Do you regularly review and update this plan?

SI / YES NO

22. ¿Se llevan a cabo regularmente pruebas a este plan?
Are tests carried out regularly on this plan?

SI / YES NO

23. ¿Se eliminan los problemas identificados?
Are the identified problems eliminated?

SI / YES NO

24. ¿Incluye su plan de respuesta a incidentes, opciones alternativas en caso de que los proveedores de outsourcing de los que usted depende no estén disponibles?
Does your incident response plan include alternative options in case the outsourcing providers you depend on are not available?

SI / YES NO

En caso de que la pregunta anterior sea afirmativa, ¿han sido las recomendaciones llevadas a cabo?

If the answer is 'Yes' were the recommendations carried out?

SI NO

25. Tiene usted procedimientos de control de acceso y encriptado de disco duro para evitar la exposición no autorizada de datos en todos los ordenadores portátiles, PDAs, smartphones (p.ej. BlackBerry) y PC's en la oficina u ordenadores personales?
Do you have access control procedures and hard disk encryption to prevent unauthorized exposure of data on all laptops, PDAs, smartphones (eg BlackBerry) and PC's in the office or personal computers?

SI / YES NO

26. En caso de pérdida o robo de los equipos portátiles o móviles donde los empleados pueden acceder a información no pública, ¿tiene la empresa un proceso a seguir determinado?

In case of loss or theft of portable or mobile equipment where employees can access non-public information, does the company have a specific process to follow?

SI / YES

NO

27. En caso afirmativo, por favor indicar cuál es el procedimiento a seguir para mitigar los daños.

If "yes" please indicate the process to follow in order to mitigate damages.

A nivel general se debe efectuar lo siguiente:

1. El usuario debe colocar la denuncia
2. Enviar correo a Jefe directo y generación de caso a Mesa
3. El proveedor valida y escala para que ellos puedan realizar la reclamación ante la póliza respectiva.

28. La información sensible y confidencial que se transmite dentro y desde su organización está encriptada?

Is all sensitive and confidential information that is transmitted within and from your organization encrypted?

SI / YES

NO

29. Se encuentra encriptada la información sensible y confidencial almacenada en sus bases de datos, servidores y archivos?

Is all sensitive and confidential information stored on your databases, servers and data files encrypted?

SI / YES

NO

30. Se encuentra encriptada la información contenida en dispositivos móviles (Portátiles, drivers, USB, etc...)?

Are all mobile devices content information encrypted (laptop, drivers, USB devices, etc....)?

SI / YES

NO

31. ¿Tienen una gestión de control de acceso con el principio de menor privilegio?

Do they have access control management with the principle of least privilege?

SI / YES

NO

6. INFORMACIÓN Y GESTIÓN DE DATOS

Information and data management

1. La empresa maneja datos de terceros, información confidencial, datos de información personal de clientes, o tarjetas de crédito?
 Does the company handle third-party data, confidential information, customer personal information data, or credit cards?

SI / YES

NO

2. **Número de Registros:**Cuál es la información que la Empresa Solicitante recolecta/gestiona/almacena como datos personales o confidenciales:
Number of Records: What is the information that the Requesting Company collects / manages / stores as personal or confidential data:

Tipo de datos Type of Data	# Registros de ciudadanos no estadounidenses # Records of non-US citizens	# Registros almacenados en centros de datos en los EEUU # Records stored in data centers in the US	# Registros de ciudadanos estadounidenses # Registers of US citizens
Información de tarjetas de crédito (PCI) Credit card information (PCI)			
Información financiera Financial information			
Información personal (PII) Personal Information (PII)	x		
Información de clientes Customer Information			
Historias Clínicas (PHI) Medical Records (PHI)	x		
Propiedad Intelectual (IP) Intellectual Property (IP)			
Otra (Describa) Other (Describe)			

3. Su programa de clasificación de información incluye una clasificación estándar de datos (por ejemplo "públicos", "solo para uso interno", "confidencial")
Does your information asset program include a data classification standard (E.g. public, internal use only, confidential?)
SI / YES NO
4. ¿Todos los sistemas accesibles a través de Internet (por ejemplo, servidores web / de correo) están segregados de su red confiable (por ejemplo, dentro de "DMZ" o en un proveedor externo)?
Are all systems accessible via the Internet (for example, web / mail servers) segregated from your reliable network (for example, within "DMZ" or an external provider)?
SI / YES NO
5. Los sistemas críticos cuentan con medidas adicionales de segmentación, autenticación segura?
Critical systems have additional segmentation, secure authentication?
SI / YES NO
6. ¿Todos los segmentos de alto riesgo de la red están segregados (por ejemplo, sistemas PoS, procesamiento / almacenamiento de datos PHI, etc.)?
Are all high-risk segments of the network segregated (for example, PoS systems, PHI data processing / storage, etc.)?
SI / YES NO
7. Contiene su página web una política de privacidad de datos, habiendo sido revisada por abogado / consultor jurídico?
Does your website contain a data privacy policy, and has it been reviewed by a lawyer / legal consultant?
SI / YES NO
8. ¿Usted realiza un seguimiento de datos mediante el uso de herramientas de rastreo (tracking tools)?
Do you track data through the use of tracking tools?
SI / YES NO
9. ¿Usted informa a los visitantes de sus sitios web que hace seguimiento de datos?
Do you inform your website visitors that you are tracking data?
SI / YES NO
10. ¿Usted tiene implementado un sistema de Gestión de Seguridad de la información (ISMS) basado en una norma/estándar internacional?
Do you have Implement information Security Management System (ISMS) based on international standard / guideline.
SI / YES NO

11. ¿Usted cumple con una o más de las siguientes leyes de seguridad / marcos de acción / estándares / requisitos?

Do you comply with one or more of the following security standards?

ISO 27000 y siguientes / and following	X	Regulación de protección de datos de EEUU Regulation of data protection of EEUU	
HIPAA / HITECH		PCI – DSS	
Sarbanes – Oxley		COBIT	
NIST	X	Otro / Other	

12. Dispone de un inventario sobre información que indique los propietarios y las fuentes de dichos datos?

Do you have an information asset inventory that lists the owners and sources of all data?

SI / YES NO

13. Tiene procedimientos en vigor para eliminar información y para controlar el periodo de tiempo que debe mantenerse la información en sus archivos?

Do you have procedures in place to delete information and to control the period of time that information should be kept in your files?

SI / YES NO

14. La información almacenada en formato físico (papel, discos duros, CD'S, etc.) se desecha o recicla con procedimientos confidenciales y seguros conocidos por toda la organización?

Is information stored in physical format (paper, hard drives, CD's, etc.) discarded or recycled with confidential and secure procedures known to the entire organization?

SI / YES NO

15. Mantiene un registro de incidencias (amenazas a sistemas de seguridad) y fallos en la red?

Do you maintain a record of incidents (threats to security systems) and network failures?

SI / YES NO

16. En el evento en que aplique, indique los controles que utiliza para identificar y reparar las fallas, debilidades e incidencias identificadas en la red.

In the event that applies, indicate the controls you use to identify and repair the failures, weaknesses and incidents identified in the network.

Se manejan controles por medio de las aplicaciones (fuga de información, navegación, perfiles de privilegio, monitoreo de seguridad SIEM, autenticaciones 802.1x entre otros que controlan cada aspecto de conexión e intercambio de información en la red.

17. La empresa y/o sus filiales, subsidiarias o subordinadas realiza procesos de pagos en nombre de terceros, u operaciones de comercio electrónico (e-commerce)?
Does the company and / or its affiliates, subsidiaries or subordinates perform processes payments on behalf of third parties, or operations of electronic commerce (e-commerce)?
- SI / YES NO

Información / Industria de tarjetas de pago Information / Payment Card Industry

(Solamente en caso que usted procese datos de tarjetas de pago)
(Only in case you process payment card data)

18. Está sujeto al cumplimiento de PCI (Payment Card Industry)? De ser así por favor suministre una copia del certificado de PCI-DSS.
Are you subject to fulfilment of any compliance of the PCI(Payment Card Industry) If "Yes" Please Provide a copy of you last certificate of the PCI-DSS.
- SI NO
19. ¿Usted acepta tarjetas de crédito?. En caso afirmativo, por favor indicar la facturación generada con tarjetas de crédito
Do you accept Credit Cards. In case the answer is yes please indicate credit cards receipt
- SI / YES NO
20. ¿Cuántas transacciones de tarjetas de crédito o débito procesa al año?
How many credit and debit card transactions do you make in a year?
-
21. ¿Qué nivel de comerciante (Merchant level) de acuerdo con la definición de PCI tiene actualmente
What Merchant level in terms of the definition of PCI do you have in this moment?
-
22. ¿Se enmascaran todos, menos los últimos cuatro dígitos de los números de tarjetas al mostrar o imprimir datos de titulares de tarjetas?
Do you show all, except the last 4 digits of the credit cards when you print the cardholder data
- SI / YES NO

23. ¿Usted Asegura que los códigos de validación de tarjetas no se almacenen en ninguna de sus bases de datos, archivos de registro o en cualquier otro lugar dentro de su red?
Do you ensure that validation code of your credit card is not storage in any data base, registry achieves or any other place on the network
SI / YES NO
24. ¿Se cifra toda la información de cuentas bancarias en sus bases de datos?
Do you encrypt account information in your data base?
SI / YES NO
25. ¿Usted usa terminales de punto de venta "POS"? En caso afirmativo, ¿Esta deshabilitado permanentemente el acceso remoto a todos los puntos de venta?
Do you use POS (Point of sales) Terminals In case the answer is Yes. Is the sales Access remote permanent Disable.
SI / YES NO
26. ¿Se cifra o se utilizan sistemas de token para toda la información de cuenta en el punto de venta?
Do you use any token system to encrypt account information in Point of Sales (POS)
SI / YES NO
27. ¿Emplea el cifrado punto a punto, comenzando con el hardware de tarjeta magnética?
Do you use point-to-point encryption starting with card magnets hardware
SI / YES NO
28. ¿Tiene un procedimiento estándar implementado para cumplir permanentemente con los requisitos o regulaciones legales (o contractuales) de privacidad?
Do you have a implement permanent standard Proceed to accomplish with the requirements for the legal regulations (o contractual) Privacy.
SI / YES NO

7. SINIESTROS Y CIRCUNSTANCIAS

Claims and circumstances

1. Usted o algún director antiguo o presente, socio, director o empleado de la empresa, o sus subsidiarias, filiales o subordinadas ha sido alguna vez sancionado, investigado o auditado por un mal uso de los datos o alteración en la red informática?
Have you or any former or current director, partner, director or employee of the company, or its subsidiaries, subsidiaries or subordinates ever been sanctioned, investigated or audited for misuse of data or alteration in the computer network?
- SI / YES NO

2. Ha sufrido alguna caída de la red o interrupción no programada en los últimos 24 meses?
Have you suffered any network outage or unscheduled interruptions in the last 24 months?
- SI / YES NO

En caso afirmativo, favor indicar (i) Valor del evento, o valor estimado del evento, (ii) descripción del evento, y (iii) medidas correctivas.

If yes, please indicate (i) Value of the event, or estimated value of the event, (ii) description of the event, and (iii) corrective measures.

Se presentó caída de interconexión con datacenter Claro. No se presentó afectación en costos y se debió a una masiva presentada por el proveedor por temas eléctricos.

3. Ha sufrido alguna vez un acceso no autorizado al sistema, alteraciones, virus o un ataque de código malicioso, pérdida de datos, incidente de hacking, robo de datos o un incidente similar
Have you ever suffered unauthorized access to the system, alterations, viruses or a malicious code attack, data loss, hacking incident, data theft or a similar incident
- SI / YES NO

En caso afirmativo, favor indicar (i) Valor del evento, o valor estimado del evento, (ii) descripción del evento, y (iii) medidas correctivas.

If yes, please indicate (i) Value of the event, or estimated value of the event, (ii) description of the event, and (iii) corrective measures.

4. Tiene conocimiento de hechos o circunstancias que puedan dar lugar a una reclamación contra usted y / o una reclamación bajo esta póliza de seguros?
Are you aware of facts or circumstances that may give rise to a claim against you and / or a claim under this insurance policy?

SI / YES

NO

5. Tiene usted conocimiento de hechos o circunstancias que puedan dar lugar a investigaciones por parte de las autoridades competentes, investigaciones o imposición de multas o sanciones?

Are you aware of facts or circumstances that may lead to investigations by the competent authorities, investigations or imposition of fines or sanctions?

SI / YES

NO

En caso afirmativo, favor indicar (i) Valor del evento, o valor estimado del evento, (ii) descripción del evento, y (iii) medidas correctivas.

If yes, please indicate (i) Value of the event, or estimated value of the event, (ii) description of the event, and (iii) corrective measures.

6. ¿Ha experimentado alguna vez un intento o un hecho de extorsión con respecto a sus sistemas informáticos? En caso afirmativo adjuntar una descripción completa.

Have you ever experienced an attempt or act of extortion with respect to your computer systems? If yes, attach a complete description.

SI / YES

NO

En caso afirmativo, favor indicar (i) Valor del evento, o valor estimado del evento, (ii) descripción del evento, y (iii) medidas correctivas.

If yes, please indicate (i) Value of the event, or estimated value of the event, (ii) description of the event, and (iii) corrective measures.

7. Le han declinado cobertura de seguro o su asegurador actual le ha impuesto alguna condición?
Have you ever been refused insurance or had any special terms or conditions imposed by any insurer?

SI / YES

NO

En caso de haber contestado afirmativamente cualquiera de las preguntas formuladas en dicho apartado, por favor facilite detalles en una hoja aparte si fuera necesario.
If the answer is 'Yes' to any questions within this section, please provide full details, on a separate sheet if necessary

Maria Lucia Lleras E

Firma: Signature

Nombre: MARIA LUCIA LLERAS ECHEVERRI

Cargo ocupado en la Compañía: Vicepresidente Desarrollo Corporativo (E)

Fecha: Noviembre 23 de 2023

Elaboró: Martha Puerto – La Previsora S.A. 

Visto Bueno: Lilia Manzano – La Previsora S.A.

Visto Bueno: Luis Felipe Castillo – La Previsora S.A.

Visto Bueno: Oscar Cortés – WTW 