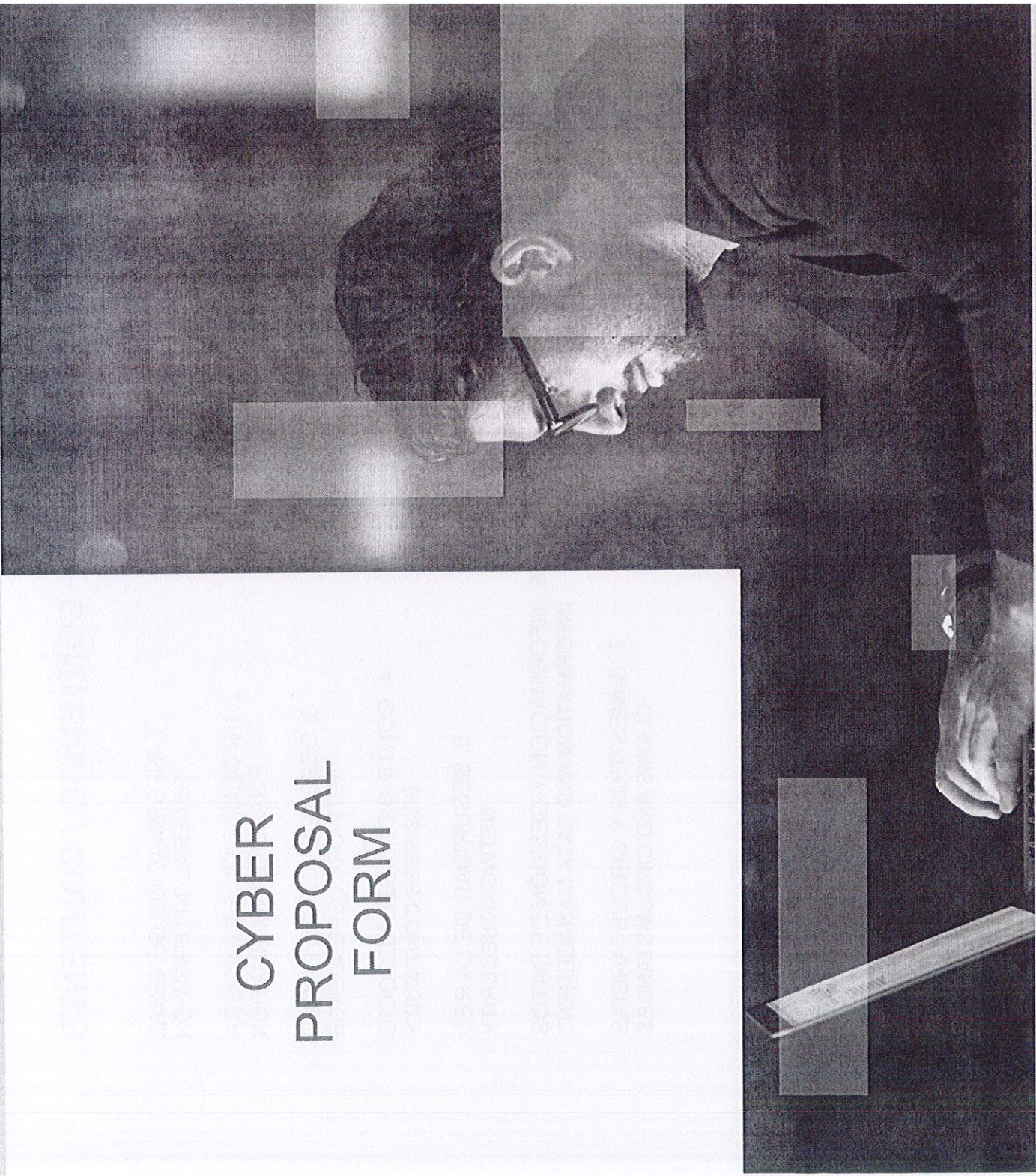


CYBER PROPOSAL FORM



1. INFORMACION GENERAL GENERAL INFORMATION

1. Empresa Solicitante:
Company or trading name

LA PREVISORA S.A. CIA 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

Martha.puerto@previsora.gov.co

5. Página web:
Website

www.previsora.gov.co

6. Fecha de fundación:
Date of Foundation

6 de agosto de 1954

7. Número de empleados:
Number of employees

730

8. Número de establecimientos/locales:
Number of premises

VER ANEXO No.1

14. ¿La Empresa Solicitante o sus filiales / subsidiarias tienen actualmente contratado un seguro similar o complementario al que se solicita? Si
Does the applicant Company or its subsidiaries / subsidiaries currently have similar or complementary insurance to the one requested?

SI / YES SI NO

En caso afirmativo, por favor informe ramo, vigencia y Compañía.
If the answer is 'Yes', please provide line of business, period and Insurer.

POLIZA DE SEGURO DE RESPONSABILIDAD PROFESIONAL POR PERDIDA DE DATOS. VIGENCIA 31 DE AGOSTO DE 2021 AL 31 DE AGOSTO DE 2022. COMPAÑIA SBS SEGUROS DE COLOMBIA S.A.

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:

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? NOTA: Únicamente dar respuesta de Previsora Seguros

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)

1472

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

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:

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 SI

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 SI

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 SI

NO

SI / YES SI 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:

Se efectuán auditorías Internas cada 2 meses aproximadamente de procesos alineados con las circulares externas de la Superfinanciera de Colombia y la ISO 27000. Última Fecha de auditoría 1/07/2022

6. Cuando 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?

Fecha: 7 y 14 de Noviembre 2021 y se efectuan una vez al año

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 SI NO 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 SI 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 SI 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 SI 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 SI 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
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 X 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 X 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)

30-11-2018

la política de protección de datos personales no se modifica, lo que se modifica según nuevos procesos y/o riesgos el manual de tratamiento de datos, para este caso la última modificación del manual fue en el primer semestre de 2022

- 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?
la política de protección de datos personales no se modifica, lo que se modifica según nuevos procesos y/o riesgos el manual de tratamiento de datos, para este caso la última modificación del manual fue en el primer semestre de 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 SI 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 SI 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 SI NO

- 15. Utilizan Firewall (Sistemas de prevención de intrusiones)
Do you use Firewall
SI / YES SI NO

- 16. Las subsidiarias, filiales o subordinadas de la empresa solicitante utilizan firewall
Do your affiliates or subsidiaries use Firewall?
SI / YES SI 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 computadores y sitios web

24. 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 SI NO

25. 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.

26. 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

27. 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

28. 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

29. ¿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

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 SI 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
--	---	--

(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 fulfillment of any compliance of the PCI(Payment Card Industry) if "Yes" Please Provide a copy of your 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?
21,101 Transacciones al año

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?
N/A

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?

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 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 X

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 X

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.

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 X

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

HA NO X

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

4. ¿Qué tipo de copias de seguridad están haciendo a raíz de la contingencia (por ejemplo sistemas críticos, datos e informaciones)? Y con frecuencia se hacen?
What kind of backups are you doing as a result of the contingency (eg critical systems, data and information)? And are they frequently made?

Se tienen políticas de Backup establecidas con los dueños de las aplicaciones con periodicidad de mensuales, semanales y diarias

5. Respecto a proveedores de IT (y de TO cuando aplique) para sistemas críticos, han confirmado ellos la continuidad en sus servicios?
Regarding IT providers (and OT when applicable) for critical systems, have they confirmed the continuity of their services?

SI / YES NO

7. Y han presentado planes de continuidad respecto a Covid-19?
And have they submitted continuity plans regarding Covid-19?

SI / YES NO

6. ¿Filtra / escanea los correos electrónicos entrantes en busca de archivos adjuntos y / o enlaces maliciosos?
Do you filter/scan incoming e-mails for malicious attachments and/or links?

SI / YES NO

7. Tiene medidas específicas en contra de ataques de "Phishing".
Do you have specific measures against "Phishing" attacks.

SI / YES NO

8. Ha implementado una comunicación proactiva a los empleados, con el fin de informarles sobre los posibles riesgos de "Phishing" que pueden generarse en el contexto de Covid-19?
Have you implemented proactive communication to employees, in order to inform them about the possible "Phishing" risks that may arise in the context of Covid-19?

SI / YES NO

15. Está permitido el uso de dispositivos personales?

Is the use of personal devices allowed (BYOD)?

SI / YES

NO X

En caso afirmativo, el solicitante garantiza que se implementan medidas de seguridad apropiadas a fin de que los empleados puedan acceder a la red corporativa de manera segura?

If yes, does the applicant ensure that appropriate security measures are in place so that employees can access the corporate network securely?

SI / YES

NO

Declaro que toda la información aquí contenida es verdadera y que no se ha ocultado o tergiversado ningún dato relevante que pueda influir en la suscripción de éste riesgo. Asimismo me comprometo a notificar cualquier cambio en la información suministrada desde la fecha del diligenciamiento del presente formulario, y comprendo que cualquier cambio en la información puede dar lugar a modificaciones en las condiciones presentadas.

I hereby declare that all the information is accurate and no information has been withheld nor any information has been manipulated in a way that could influence the underwriters' appreciation of the risk. I also accept to notify any change in the information provided from the date of this form, and I understand that any change in the information may lead to changes in the conditions presented.


Firma:
LEYDY VIVIANA MOJICA
Secretaría General
Agosto 22 de 2022

PROYECTO: MARLEHA ISABEL PUERTO

REVISÓ: LUIS FELIPE CASTILLO