Planeación de datos

SBS

FORMULARIO PÓLIZA CYBER

Este cuestionario es confidencial, la firma o diligenciamiento de este formulario no obliga a SBS Seguros Colombia S.A. a formalizar este seguro. Está diseñado para proporcionar una visión completa de la eficacia y la madurez de TI así como de la seguridad de datos dentro de su compañía.
Las respuestas a este cuestionario son muy importantes para evaluar el riesgo y hacer la suscripción con el fin de proporcionar un seguro cibernético para su compañía. Las declaraciones hechas en el cuestionario formarán parte integral del contrato de seguro, por ende, una persona responsable para la seguridad informática de su compañía debería responder a las preguntas, o al menos apoyar este proceso.
Favor anexar cualquier información complementaria que resulte significativa para las respuestas de las preguntas de este documento. En caso de estarse proponiendo el seguro para más de un Solicitante, todas las respuestas deben darse como grupo, es decir para todos los Solicitantes. Si cualquier Compañía Subsidiaria[1] tiene respuestas distintas por favor suministrarlas en forma independiente.
El cuestionario debe ir acompañado del último informe anual de la Sociedad y de cada Subsidiaria que incluya sus estados financieros consolidados y el informe de auditoría externa.

¿Adjuntan alguna información o detalles adicionales con respecto a su seguridad informática como anexo? ☐ Sí ☒ No

Número de empleados de la Universidad Militar Nueva Granada:

Administrativos de Carrera. 515

Docentes de Carrera. 444

Docentes ocasionales. 161

Administrativos Provisional. 128

Docentes Hora Cátedra. 1049

Información del solicitante

Nombre de la Empresa Solicitante (Tomador)	UNIVERSIDAD MILITAR NUEVA GRANADA					
NIT:	800.225.340-8		Fecha de fundación		23 DE JULIO 1982	
Website:	https://www.umng.edu.co/					
Dirección principal de la Empresa Solicitante	CARRERA 11 No. 101-80					
Dirección de su página Internet	45.238.196.146					
Tipo de Sociedad	Pública	X	Privada	Mixta	Cooperativa	Sociedad Sin Ánimo de Lucro
Número de Empleados	2.297			Número de Predios		1
Subsidiarias						

1. Sector industrial

Por favor marque el sector / los sectores industriales aplicables.

- ☐ Alimentación & Agricultura
- ☐ Autoridad pública; ONG; sin fines de lucro
- ☐ Defensa / Contratista Militar
- ☒ Educación
- ☐ Energía
- ☐ Entretenimiento & Medios
- ☐ Servicios Financieros – Gestión de inversiones
- ☐ Servicios Financieros – Seguros
- ☐ Servicios profesionales
- ☐ Tecnología de la información - Hardware
- ☐ Tecnología de la información - Software
- ☐ Tecnología de la información – Servicios

[1] **Compañía subsidiaria** significa cualquier compañía en la cual el **tomador de la póliza,** ya sea directa o indirectamente a través de una o más de sus compañías subsidiarias: (i) controla la composición de su directorio; o (ii) controla más de la mitad del poder de voto; o (iii) posee más del 50% del capital o de las acciones de la empresa.

- ☐ Fabricación
- ☐ Minería & Industrias Primarias
- ☐ Productos farmacéuticos
- ☐ Propiedad Inmobiliaria & Construcción
- ☐ Salud
- ☐ Servicios Financieros - Bancos
- ☐ Telecomunicaciones
- ☐ Transporte / Aviación / Aeroespacial
- ☐ Turismo & Hospitalidad
- ☐ Utilidades
- ☐ Venta al por menor
- ☐ Otros: _____

Por favor especificar detalles de su actividad:

Institución de Educación Superior – Régimen Autónomo de Orden Nacional

2. Facturación, activos e información general

	Latinoamérica		Estados Unidos		Resto del mundo	
	Año anterior	Año actual	Año anterior	Año actual	Año anterior	Año actual
Facturación bruta	159.895.790.679	152.522.908.164				
Facturación bruta por Internet, p.ej. de comercio electrónico	8.028.549.052	4.968.603.209				

2.1 ¿Tiene activos en los EE.UU.? ☐ Sí ☐ No

2.2 Por favor indicar el número (estimado) de dispositivos individuales de TI que tiene:

Dispositivo	Número
Servidores	47
Computadores de escritorio	3534
Computadores Portátiles	273
Dispositivos Móviles	44

2.2 Por favor indicar todos los sitios web (nombres de dominio establecidos que pueden ser accedidos a través de Internet) que deberían estar cubiertos por este seguro:

Nombre / Dominio
http://www.umng.edu.co/
http://radio.umng.edu.co/
https://www.youtube.com/user/militarnuevagranada
https://twitter.com/lamilitar
https://es-la.facebook.com

3. Información del seguro

3.1 Seguro solicitado

Límites asegurados a cotizar (Cifras en COP):

Opción 1: $ 3.500.000.000

Opción 2: $ 2.000.000.000

Opción 3: $ 1.500.000.000

3.2 Extensiones de cobertura solicitadas:

SBS

x Cyber Extorsión x Contenido Multimedia x Interrupción de la Red

Seguro anterior

3.3 ¿Ha cancelado o no renovado ante cualquier compañía de seguro una póliza con la misma cobertura o una cobertura similar a la del seguro solicitado? ☐ Sí ☒ No

3.4 ¿Actualmente tiene o ha tenido un seguro cibernético con la misma cobertura o una cobertura similar a la solicitada? ☐ Sí ☒ No

4. Cumplimiento de estándares

4.1 ¿Usted cumple con una o más de las siguientes leyes de seguridad / marcos de acción/ estándares / requisitos? ☐ Sí ☒ No

☐ ISO 27000 y siguientes ☐ NIST ☐ PCI-DSS (Nivel: _______)

☐ HIPAA/HITECH ☐ Regulación de protección de datos de la U.E. ☐ COBIT

☐ Otro: ____________________

5. Calidad y Cantidad de Datos

¿Qué tipo y cantidad de datos sensibles maneja/procesa su compañía?

	Calidad de datos	Número de registros únicos de ciudadanos no estadounidenses	Número de registros únicos almacenados en centros de datos en los EE.UU	Número de registros únicos de ciudadanos estadounidenses
☐	Información de Identificación Personal	1	1	1
☐	Información de Tarjetas de Pago			
☐	Información de salud personal	1	1	1
☐	Propiedad intelectual		1	
☐	Otros			

6. Seguridad informática

Las siguientes preguntas nos ayudan a evaluar la madurez de su seguridad informática. Por favor responda todas las preguntas y proporcione evidencia donde esté disponible (p.ej. informes, presentaciones, documentos, etc.). Las preguntas están estructuradas de acuerdo con las cláusulas de la norma ISO 27002. Por lo tanto, las preguntas centradas en un mismo objetivo de seguridad pueden aparecer en diferentes secciones de este cuestionario. Con el fin de crear una mejor comprensión acerca de por qué hacemos las preguntas, cada sección comienza con el objetivo de las categorías de seguridad de ISO 27002.

6.1 Políticas de seguridad informática

Objetivo Cláusula 5 de ISO 27002: Proporcionar dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos del negocio y las leyes y regulaciones relevantes.

Q-1 ¿Usted tiene una política formal de seguridad de la información desarrollada, implementada a nivel corporativo y permanentemente disponible para todos los empleados? ☒ Sí ☐ No

6.2 Organización de la seguridad informática

Objetivo Cláusula 6 de ISO 27002: Establecer un marco de gestión para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Q-2 ¿Tiene su compañía una persona responsable para la seguridad informática (p.ej. Chief Information Security Officer "CISO") o equipo que reporta regularmente a la alta dirección? ☒ Sí ☐ No

6.3 Seguridad de los recursos humanos

Objetivo Cláusula 7 de ISO 27002: Garantizar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las que se los considera. Garantizar que empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

Q-3	¿Usted provee formación regular para aumentar la conciencia de su personal hacia la seguridad y para preparar a los empleados a ser más resilientes y vigilantes contra el phishing?	☒ Sí ☐ No

6.4 Manejo de activos

Objetivo Cláusula 8 de ISO 27002: Identificar los activos de la organización y definir las responsabilidades de protección apropiadas. Asegurar que la información reciba un nivel apropiado de protección de acuerdo con su importancia para la organización. Evitar la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en los medios.

Q-4	¿Usted mantiene un inventario de dispositivos de software (incl. sistemas operativos) y hardware e sus redes?	☒ Sí ☐ No
Q-5	¿Usted clasifica información con respecto a su confidencialidad?	☐ Sí ☒ No
Q-6	¿Usted limita el acceso o encripta la información confidencial almacenada en medios extraíbles, como dispositivos de almacenamiento externos (p.ej. memorias USB, discos duros)?	☐ Sí ☒ No

6.5 Control de acceso

Objetivo Cláusula 9 de ISO 27002: Limitar el acceso a la información y a las instalaciones de procesamiento de información. Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Hacer responsables a los usuarios por salvaguardar su información de autenticación. Evitar el acceso no autorizado a sistemas y aplicaciones.

Q-7	¿Usted restringe los privilegios de empleados y usuarios externos en función de las necesidades comerciales (especialmente los permisos administrativos y el acceso a datos sensibles como PII)?	☒ Sí ☐ No
Q-8	¿Usted ha aplicado la autenticación de múltiples factores para el acceso remoto?	☒ Sí ☐ No ☐ N/A
Q-9	¿Usted tiene un proceso de aprovisionamiento de acceso para asignar y revocar los derechos de acceso?	☒ Sí ☐ No
Q-10	¿El propietario de la información autoriza el permiso de acceso?	☒ Sí ☐ No
Q-11	¿Usted mantiene una lista central de derechos de acceso otorgados a un usuario para acceder a sistemas y servicios de información?	☒ Sí ☐ No
Q-12	¿Usted prohíbe los derechos de administrador local en las estaciones de trabajo para los usuarios?	☒ Sí ☐ No
Q-13	¿Usted tiene un proceso para eliminar el acceso al sistema, las cuentas de usuarios y los derechos asociados de los usuarios después del despido del empleado, empleado temporal, contratista o proveedor?	☒ Sí ☐ No
Q-14	¿Usted ha implementado una política de contraseñas para garantizar que se utilicen contraseñas complejas y largas en su compañía?	☒ Sí ☐ No
Q-15	¿Se han cambiado todas las contraseñas predeterminadas en todos los dispositivos conectados al internet (p.ej. router)?	☐ Sí ☒ No

6.6 Encriptación

Objetivo Cláusula 10 de ISO 27002: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

Q-16	¿Está encriptada toda la información confidencial cuando se almacena en dispositivos móviles como laptops o móviles?	☐ Sí ☒ No
Q-17	¿Usted ha desarrollado e implementado una política sobre el uso, la protección y la duración de las claves criptográficas?	☒ Sí ☐ No

6.7 Seguridad física

Objetivo Cláusula de ISO 27002: Evitar acceso físico no autorizado, daño e interferencias a la información y a las instalaciones de procesamiento de información. Evitar la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Q-18	¿Usted ha implementado medidas básicas de seguridad física y controles ambientales (como cerraduras de puertas y armarios, alarmas antirrobo, alarmas contra incendio, extintores de incendios, CCTV)?	☒ Sí ☐ No
Q-19	¿Usted mantiene una lista del personal (empleados, proveedores y visitantes) con acceso autorizado a sus predios y áreas de seguridad sensible?	☒ Sí ☐ No

6.8 Seguridad operacional

Objetivo Cláusula 12 de ISO 27002: Garantizar operaciones correctas y seguras de las instalaciones de procesamiento de información. Garantizar que la información y las instalaciones de procesamiento de información estén protegidos contra el malware. Proteger contra la pérdida de datos. Registrar eventos y generar evidencia. Garantizar la integridad de los sistemas operativos. Evitar la explotación de vulnerabilidades técnicas. Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

Q-20	¿Usted ha implementado procedimientos de gestión de cambios para los sistemas críticos?	☒ Sí ☐ No
Q-21	¿Está separado el entorno de TI de desarrollo y prueba del entorno de TI productivo?	☒ Sí ☐ No ☐ N/A
Q-22	¿Usted utiliza protección contra malware en proxy web, puerta de enlace de correo electrónico (email-gateway), estaciones de trabajo y computadoras portátiles?	☒ Sí ☐ No
Q-23	¿Las actualizaciones de los archivos de firmas anti-malware se descargan y se instalan automáticamente?	☒ Sí ☐ No
Q-24	¿Usted realiza copias de seguridad periódicas de datos críticos para el negocio al menos una vez a la semana?	☒ Sí ☐ No
Q-25	¿Usted almacena las copias de seguridad físicamente separadas de su red (p.ej. fuera de los predios de la oficina)?	☐ Sí ☒ No
Q-26	¿Usted se asegura regularmente de que las copias de seguridad de datos se puedan restaurar lo más rápido posible con un impacto mínimo?	☐ Sí ☒ No
Q-27	¿Usted actualiza oportunamente - al menos mensualmente - los sistemas de TI y las aplicaciones relevantes para la seguridad ("parches de seguridad")?	☒ Sí ☐ No
Q-28	¿Usted ha desarrollado e implementado políticas que los usuarios no pueden instalar soft-ware en sus estaciones de trabajo por sí mismos?	☒ Sí ☐ No

6.9 Seguridad de la comunicación

Objetivo Cláusula 13 de ISO 27002: Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Q-29	¿Están protegidos por firewalls todos los puntos de acceso a Internet?	☒ Sí ☐ No
Q-30	¿Usted protege sus redes inalámbricas usando el estándar WPA2?	☒ Sí ☐ No ☐ N/A
Q-31	¿Están todos sus sistemas accesibles por Internet (p.ej. servidores web/de correo electrónico) segregados de su red de confianza (p.ej. dentro de una zona desmilitarizada "DMZ" o en un proveedor externo)?	☒ Sí ☐ No
Q-32	¿Está encriptada toda la comunicación confidencial (p.e. a través de correo electrónico)?	☐ Sí ☒ No

6.10 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo Cláusula 14 de ISO 27002: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que brindan servicios a través de redes públicas. Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información. Garantizar la protección de los datos utilizados para las pruebas.

Q-33	¿Su servidor web encripta los datos confidenciales (p.ej. HTTPS)?	☐ Sí ☒ No
Q-34	¿Usted hace pruebas de las funcionalidades de seguridad durante el ciclo de vida de desarrollo de los sistemas de información?	☐ Sí ☒ No ☐ N/A

Q-35	¿Usted está considerando aspectos de confidencialidad al utilizar datos operacionales para pruebas?	☐ Sí ☒ No

6.11 Relación con proveedores

Objetivo Cláusula 15 de ISO 27002: Garantizar la protección de los activos de la organización a la que pueden acceder los proveedores. Mantener un nivel acordado de seguridad de la información y entrega de servicios en línea con los acuerdos con los proveedores.

Q-36	¿Los acuerdos con proveedores externos de servicios requieren niveles de seguridad proporcionales al nivel de seguridad de su información?	☒ Sí ☐ No ☐ N/A
Q-37	¿La Empresa Solicitante subcontrata la gestión o algunas de sus operaciones tecnológicas?	☐ Sí ☒ No ☐ N/A
Q-38	¿La Empresa Solicitante o sus filiales subcontrata empresas para funciones de administración de seguridad de la información?	☐ Sí ☒ No ☐ N/A
Q-39	¿Exigen a los contratistas y subcontratistas el cumplimiento de las políticas de seguridad y protección de datos de la empresa? ¿Por medio de qué mecanismo exigen tal cumplimiento? Acuerdo de Confidencialidad UMNG.	☒ Sí ☐ No ☐ N/A
Q-40	¿Exige a los contratistas o subcontratistas tener vigente una póliza de responsabilidad para la protección de datos?	☐ Sí ☒ No ☐ N/A
Q-41	¿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?	☐ Sí ☒ No ☐ N/A
Q-42	¿Se auditan periódicamente las funciones de subcontratistas / prestadores del servicio para asegurar que cumplen con las políticas de seguridad del Solicitante?	☐ Sí ☒ No ☐ N/A
Q-43	¿Se requiere indemnización de los subcontratistas por cualquier responsabilidad que se les impute a los mismos? No es clara la pregunta	☐ Sí ☒ No ☐ N/A

6.12 Gestión de incidentes de la seguridad informática

Objetivo Cláusula 16 de ISO 27002: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Q-44	¿Usted tiene una persona asignada responsable para la respuesta a incidentes?	☒ Sí ☐ No
Q-45	¿Usted tiene implementado un plan de respuesta a incidentes de la seguridad de la información?	☐ Sí ☒ No
Q-46	En caso afirmativo, ¿este plan se prueba anualmente?	☐ Sí ☒ No
Q-47	¿Es conocida por todos los empleados y proveedores externos la línea de informes de un evento de seguridad de la información?	☐ Sí ☒ No
Q-48	¿Se documenta todos los eventos de la seguridad de la información?	☐ Sí ☒ No
Q-49	¿Usted ha establecido un proceso de escalación para incidentes de la seguridad de la información?	☒ Sí ☐ No
Q-50	¿Usted tiene una lista permanentemente actualizada de autoridades y contactos externos, a las que se tiene que o se debería informar en caso de un incidente de la seguridad informática?	☒ Sí ☐ No

6.13 Aspectos de seguridad de la información en la gestión de continuidad del negocio

Objetivos Cláusula 17 de ISO 27002: La continuidad de la seguridad de la información debe integrarse en los sistemas de gestión de la continuidad del negocio de la organización.

Q-51	¿Usted ha realizado un análisis de impacto de negocio ("BIA"), teniendo en cuenta las amenazas relevantes de TI?	☐ Sí ☒ No
Q-52	¿Usted tiene implementado un plan de continuidad de negocio?	☐ Sí ☒ No
	En caso afirmativo, ¿este plan se prueba anualmente?	☐ Sí ☒ No
Q-53	¿Usted revisa y actualiza el plan de continuidad de negocio por lo menos cada 2 años?	☐ Sí ☒ No
Q-54	¿Usted tiene un sitio de conmutación en caso de un desastre?	☐ Sí ☒ No

6.14 Compliance

Objetivo Cláusula 18 de ISO 27002: Evitar incumplimientos de obligaciones legales, reglamentarias o contractuales relacionadas a la seguridad de la información y con los requisitos de seguridad. Garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.

Q-55	¿Usted tiene implementado un procedimiento para cumplir de manera permanente con requisitos legales (o contractuales) y regulaciones de privacidad?	☒ Sí ☐ No
Q-56	¿Usted tiene una persona responsable, como un Oficial de Privacidad, que brinda orientación y garantiza el conocimiento de los principios de privacidad?	☒ Sí ☐ No
Q-57	¿Usted escanea periódicamente los sistemas críticos (incl. pruebas de seguridad, pruebas de penetración) - ya sea por su cuenta o con el apoyo de terceros en particular cuando se introducen nuevos sistemas y los cambios subsecuentes?	☐ Sí ☒ No

7. RC por Contenido Multimedia

Por favor responder a las siguientes preguntas en caso de solicitar cobertura de RC por Contenido Multimedia

M-1 ¿Qué tipo de actividades electrónicas / en línea realiza?

☒	Publicación de contenido electrónico propio	☒	Contenido bajo licencia de un tercero
☒	Transmisión de video o contenido de música bajo licencias por escrito / acuerdos de consentimiento	☒	Presentación de productos / servicios de terceros (publicidad, compra o venta)
☒	Colección de información sensible (PII/PCI/PHI, IP, otros)	☒	Contenido de terceros sin licencia (p.ej. salas de chat, blogs, tableros de mensajes, críticas de clientes, etc.)
☒	Dar aviso (p.ej. medico, legal, etc.)	☒	Archivos para descargar
☐	Contenido de adultos, juegos, juegos de apuestas	☐	Otros:..

M-2 ¿Qué servicios basados en web usa para la distribución de dicho contenido?

☒	Página web (propio y/o alojado por terceros))	☐	Redes sociales (Twitter, Facebook, etc.)
☒	Servicios de correos (p.ej. newsletter)	☒	Publicidad en línea

M-3 ¿Externaliza la producción de cualquier contenido electrónico (p. ej. publicidad)? ☒ Sí ☐ No

En caso afirmativo, por favor indicar qué parte y en qué medida.

Oferta Académica y Redes Sociales

M-4 ¿Tiene un proceso de selección y, si es necesario, elimina contenido calumnioso o difamatorio, contenido sin licencia o contenido que infringe los derechos de propiedad intelectual de terceros? En caso afirmativo, ¿con qué frecuencia? ☐ Sí ☒ No

☐ Mensualmente ☐ Trimestralmente ☐ Anualmente ☐ Irregularmente

M-5 ¿Tiene un procedimiento para responder a las acusaciones de que el contenido creado, se muestra o publicado por usted es difamatorio, infractor o en violación del derecho de un tercero? ☐ Sí ☒ No

M-6 ¿Tiene un proceso para revisar todo el contenido antes de que sea publicado por o en nombre de la compañía? ☒ Sí ☐ No

En caso afirmativo, ¿esta revisión es realizada por un abogado calificado? ☐ Sí ☒ No

En caso negativo, ¿qué procedimientos existen para evitar publicar contenido inapropiado o infractor?

Consulta y Concepto de la Oficina Jurídica UMNG y Corrector de Estilo Área de Publicaciones UMNG

M-7 ¿Ha recibido una queja o una demanda de cese y desista en los últimos tres años, alegando infracción de marca registrada o de copyright, invasión de privacidad o difamación con respecto a cualquier contenido publicado, exhibido o distribuido por usted o en su nombre? ☐ Sí ☒ No

En caso afirmativo, por favor adjuntar detalles.

M-8 ¿Comparte (ya sea comercialmente o de forma gratuita) cualquier información sobre usuarios, suscriptores o visitantes de su sitio web internamente o con terceros? ☐ Sí ☒ No

M-9 ¿Su sitio web proporciona una política de privacidad (p.ej. sobre recopilación de datos, uso de cookies, etc.) y un aviso legal sobre el uso de los derechos de terceros y enlaces a sitios web externos, incluido un descargo de responsabilidad, y dicho contenido está aprobado por un abogado competente? ☒ Sí ☐ No

8. Eventos de seguridad e historial de pérdidas

7.1 ¿Alguna vez durante los últimos tres (3) años ha tenido incidentes, reclamos o demandas de acceso no autorizado, intrusión, incumplimiento, compromiso o mal uso de su red, incluidos malversación de fondos, fraude, robo de información patentada, violación de información personal, robo o pérdida de computadoras portátiles, denegación de servicio, vandalismo o sabotaje electrónico, virus informático u otro incidente?
En caso afirmativo, adjunte todos los detalles, incluida una descripción de cada incidente, reclamo o demanda y la causa, costos internos, costo para terceros, si se notificó a las personas afectadas, tiempo de descubrir, tiempo de recuperación y medidas adoptadas para mitigar la exposición futura. ☐ Sí ☒ No

7.2 ¿Conoce alguna liberación, pérdida o divulgación de información personal identificable bajo su cuidado, custodia o control, o bajo el control de cualquier persona que tenga dicha información en su nombre en los últimos tres (3) años desde la fecha de esta aplicación?
En caso afirmativo, adjunte una descripción completa. ☐ Sí ☒ No

7.3 ¿Alguna vez ha experimentado un intento de extorsión o demanda con respecto a sus sistemas informáticos?
En caso afirmativo, adjunte detalles completos. ☐ Sí ☒ No

7.4 ¿Alguna vez ha recibido reclamos o quejas con respecto a denuncias de difamación, invasión o lesión a la privacidad, robo de información, violación de la seguridad de la información (incluida información personal), transmisión de malware, participación en un ataque de denegación de servicio, o ha sido requerido para proporcionar una notificación a las personas debido a una divulgación real o sospechada de la información personal?
En caso afirmativo, adjunte detalles de cada uno de dichos reclamos, alegaciones o incidentes, incluidos los costos, pérdidas o daños incurridos o pagados, y cualquier cantidad pagada como pérdida en virtud de cualquier póliza de seguro. ☐ Sí ☒ No

7.5 ¿Ha estado sujeto a alguna acción gubernamental, investigación o citación con respecto a cualquier presunta violación de alguna ley o reglamento?
En caso afirmativo, adjunte detalles completos. ☐ Sí ☒ No

7.6 ¿Conoce algún hecho, circunstancia, situación, error u omisión real o presunta, o posible problema que pueda dar lugar a un reclamo en su contra en virtud del seguro que está solicitando o de un seguro similar vigente o previamente en vigencia o actualmente propuesto?
En caso afirmativo, adjunte detalles completos. ☐ Sí ☒ No

9. Comentarios adicionales y firma

¿Desea agregar más información o detalles sobre su seguridad de la información?

https://rnbd.sic.gov.co/sisi/consultaTitulares/consultas/ Registro Bases de Datos ante la SIC (NIT UMNG: 800225340)
ttps://autodiagnosticogobdigital.gov.co/ Autodiagnóstico Gobierno Digital (Estado: Medio Bajo)
http://www.umng.edu.co/seguridad-de-la-informacion
http://www.umng.edu.co/autorizacion-y-refrendacion-de-uso-de-datos-personales
http://www.umng.edu.co/pagos-en-linea
http://www.umng.edu.co/web/guest/la-universidad//division-de-gestion-de-calidad/sistema-de-gestion-de-calidad

Al firmar este documento (debe ser firmado por el funcionario, el propietario o el gerente), confirmo que soy un representante debidamente autorizado de la empresa con las habilidades técnicas suficientes para proporcionar, según mi conocimiento, respuestas ciertas, precias y completas con respecto a las preguntas dentro de este cuestionario en nombre de la empresa. El cuestionario completado y los anexos opcionales son la base de la cobertura y, por lo tanto, serán parte del contrato de seguro. Acordamos que si la información aquí contenida sufre cambios entre la fecha de diligenciamiento y la de iniciación de cobertura, notificaremos inmediatamente tales cambios al asegurador, y el asegurador podrá declinar o modificar cualquier cotización pendiente y/o autorización o acuerdo de cobertura.
Firmar esta aplicación no obliga ni al solicitante ni a la aseguradora a completar este seguro, pero es acordado que esta forma será la base del contrato de ser emitida una póliza, y se adjuntará y hará parte integrante de la póliza.

Firma autorizada del Solicitante: _____

Nombres y Apellidos: General(RA)Luis Fernando Puentes Torres

Representante legal de Razón Social: General(RA)Luis Fernando Puentes Torres

Correo electrónico alencionalciudadano@tcnimilitar.edu.co

Fecha: Marzo 02 de 2020

AVISO IMPORTANTE - LEY DE PROTECCIÓN DE DATOS

Con el propósito de proteger sus datos personales, SBS Seguros Colombia S.A ("SBS Seguros") ha diseñado una Política de Privacidad que nos permite manejar adecuadamente los datos personales que recolectemos, almacenemos o actualicemos, así como compartirlos, dentro o fuera del territorio nacional, con sociedades del grupo o con entidades con las cuales trabajamos. Aquella información que nos suministre la utilizaremos para comunicarnos con usted y enviarle información sobre: nuestros productos y servicios, las actividades comerciales de SBS Seguros, asuntos relacionados con el contrato de seguro y aspectos relativos a la seguridad de la información recolectada por SBS Seguros. Usted cuenta con los derechos establecidos en la Ley 1581 de 2012 o demás normas que la modifiquen, adicionen o complementen, y en especial tiene derecho a conocer, actualizar y rectificar los datos e información suministrados y podrá revocar las autorizaciones que aquí constan en cualquier momento. Adicionalmente, se le informa que son facultativas las respuestas a las preguntas que se le han hecho o se le harán sobre datos personales sensibles (incluidos los relativos a la salud y biométricos) o sobre datos de niñas, niños y adolescentes; por lo cual usted no se encuentra obligado a responderlas o a autorizar su tratamiento.

Dando aceptación a los términos de la cotización por Usted solicitada, Usted reconoce que ello constituye un comportamiento inequívoco mediante el cual acepta la Política de Privacidad de Datos que ha sido diseñada por SBS Seguros y así mismo autoriza de manera expresa, informada e inequívoca a SBS Seguros y a las demás sociedades del grupo y/o terceros y/o terceros con quienes SBS Seguros sostenga relaciones jurídicas y/o comerciales relacionadas con su objeto social (incluidos proveedores, FASECOLDA, INIF, INVERFAS S.A., entre otros), establecidos dentro o fuera del territorio nacional, para que utilice(n) los datos personales, incluidos los sensibles, que voluntariamente nos ha suministrado con los fines antes descritos. De igual forma, Usted autoriza de manera expresa, informada e inequívoca a SBS Seguros a consultar y reportar información relativa a su comportamiento financiero, crediticio y/o comercial a centrales de información y/o bases de datos debidamente constituidas y corroborar la información aquí suministrada por cualquier medio legal.

La Política de Privacidad de SBS Seguros se encuentra disponible en www.sbseguros.co, puede solicitar una copia en la línea de Atención al Cliente 01 8000 522 244 o en las oficinas de SBS Seguros y se le agradece poder revisarla periódicamente. Si por alguna razón ha entregado a SBS Seguros información de otra persona, Usted certifica que está autorizado para ello y que compartirá con esa persona la Política de Privacidad de SBS Seguros Colombia.

ESTE DOCUMENTO SÓLO CONSTITUYE UNA SOLICITUD DE SEGURO Y, POR TANTO, NO REPRESENTA GARANTÍA ALGUNA DE QUE LA MISMA SERÁ ACEPTADA POR LA ASEGURADORA.

Anexo: Resumen Sectores industriales

Alimentación & Agricultura	Compañías involucradas en la industria alimentaria, incluyendo la producción, transformación, distribución y suministro al por mayor.
Autoridad pública; ONG, sin fines de lucro	Agencias gubernamentales nacionales o locales, organizaciones no-gubernamentales y sin fines de lucro
Defensa / Contratista Militar	La industria de la defensa incluye el gobierno y la industria comercial, incluyendo la investigación, el desarrollo, la producción y el servicio del material, del equipo y de las instalaciones militares.
Educación	Colegios y universidades, distritos escolares independientes y unificados, préstamos a estudiantiles y colegiaturas.
Energía	Empresas involucradas en la exploración, extracción y desarrollo de reservas de petróleo o gas, perforación de petróleo y gas o empresas de energía integrada.
Entretenimiento & Medios	Empresas que ofrecen noticias, información y entretenimiento: radio, televisión, cine, teatro.
Fabricación	Compañías fabricando o procesando bienes, sobre todo en grandes cantidades y a través de maquinaria industrial.
Minería & Industrias Primarias	Empresas involucradas en la minería, extracción y procesamiento de extracción de minerales, carbón, materias primarias y recursos naturales.
Productos farmaceúticos	La industria farmacéutica desarrolla, produce y comercializa fármacos para su uso como medicamentos. Las compañías farmacéuticas pueden tratar medicamentos genéricos o de marca y dispositivos médicos.

Propiedad Inmobiliaria & Construcción	Empresas que administran, desarrollan y realizan transacciones de propiedades que consisten en terrenos y edificios, junto con sus recursos naturales, como cultivos, minerales o agua.
Salud	Empresas proveedoras de bienes y servicios para el tratamiento de pacientes con atención curativa, preventiva, rehabilitadora y paliativa.
Servicios Financieros – Bancos	Empresas dedicadas a banca comercial, instituciones de ahorro, cooperativas de crédito, emisión de tarjetas de crédito, financiamiento, compañías y corredores de hipotecas y préstamos, procesamiento de transacciones financieras, actividades de reserva y cámara de compensación y banca central.
Servicios Financieros – Gestión de inversiones	Empresas dedicadas a la gestión de inversiones, negociación y corretaje de valores, negociación de contratos de productos básicos y corretaje, bolsas de valores e inversiones, fondos de inversión y capital de riesgo, administración de carteras, asesoramiento sobre inversiones y fondos y fideicomisos de entidades legales.
Servicios Financieros – Seguros	Aseguradoras directas, compañías de reaseguro y agencias de seguros y corredurías.
Servicios profesionales	Ocupaciones que ofrecen asesoramiento y servicios especializados de negocios. Algunos servicios profesionales requieren la tenencia de licencias o cualificaciones profesionales, tales como arquitectos, auditores, ingenieros, médicos y abogados.
Tecnología de la información – Hardware	Empresas dedicadas a la fabricación y/o montaje de ordenadores (mainframes, ordenadores personales, estaciones de trabajo, ordenadores portátiles y servidores) y equipos periféricos (p. ej. dispositivos de almacenamiento, impresoras, monitores; etc.)
Tecnología de la información – Servicios	Empresas proveedoras de servicios de almacenaje o de procesamiento de datos (incluyendo servicios cloud y streaming); Publicación en internet y contenido de radiodifusión (incluyendo medios sociales); Portales de búsqueda en Internet; Servicios relacionados con el diseño de sistemas informáticos, gestión de instalaciones informáticas, servicios de programación informática y consultoría en hardware o software informático.
Tecnología de la información – Software	Empresas que participan en el diseño, desarrollo, documentación y publicación de programas informáticos.
Telecomunicaciones	Empresas que facilitan el intercambio de información a través de distancias significativas por medios electrónicos.
Transporte/Aviación/Aerospacial	Empresas que facilitan el transporte de bienes o clientes. El sector del transporte está compuesto por aerolíneas, ferrocarriles y compañías de transporte.
Turismo & Hospitalidad	Empresas que prestan servicios de turismo, viajes, alojamiento, restauración y hostelería.
Utilidades	Este sector contiene empresas tales como empresas de electricidad, gas y agua y proveedores integrados.
Venta al por menor	Minoristas para el público en general, vendedores de bienes y servicios tanto en tiendas minoristas como en línea, mayoristas y distribuidores.

Firma: _____

NOMBRE: **BG. (RA) LUIS FERNANDO PUENTES TORRES Ph.D**
C.C. No. **3.181.609 de Bogotá D.C.**
CARGO: **RECTOR, UNIVERSIDAD MILITAR NUEVA GRANADA**
DIRECCIÓN: **Carrera 11 N° 101- 80 /Edificio Administrativo.**
TELÉFONO: **6500000 Ext. 1001 – 1002**
NIT: **800.225.340-8**
FECHA: Marzo 02 de 2020

Vo.Bo.

- Jefe Oficina de Protección del Patrimonio. _____
  Coronel(RA) Armando José Pinzón Rengifo