FORMULARIO PÓLIZA CYBER

Este cuestionario es confidencial, la firma o diligenciamiento de este formulario no obliga a la aseguradora 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

Información del solicitante

Nombre de la Empresa Solicitante (Tomador)	SENADO DE LA REPUBLICA					
NIT:	899999103-1	**Fecha de fundación**				
Website:	www.senado.gov.co					
Dirección principal de la Empresa Solicitante	Capitolio nacional carrera 7 No 8-68					
Dirección de su página Internet	Senado.gov.co					
Tipo de Sociedad	Publica x	Privada	Mixta	Cooperativa	Sociedad Sin ánimo de Lucro	
Número de Empleados		**Número de Predios**				
Subsidiarias						

1. Sector industrial

Por favor marque el sector / los sectores industrial (es) aplicables. Detalles hacia los sectores se encuentran en el anexo.

☐	Alimentación & Agricultura	☐	Servicios Financieros – Gestión de inversions
☐	Autoridad pública; ONG, sin fines de lucro	☐	Servicios Financieros – Seguros
☐	Defensa / Contratista Militar	☐	Servicios profesionales
☐	Educación	☐	Tecnología de la información – Hardware
☐	Energía	☐	Tecnología de la información – Software
☐	Entretenimiento & Medios	☐	Tecnología de la información – Servicios
☐	Fabricación	☐	Telecomunicaciones
☐	Minería & Industrias Primarias	☐	Transporte/Aviación/Aerospacial
☐	Productos farmaceúticos	☐	Turismo & Hospitalidad
☐	Propiedad Inmobiliaria & Construcción	☐	Utilidades
☐	Salud	☐	Venta al por menor
☐	Servicios Financieros - Bancos	☒	Otros____SENADO DE LA REPUBLICA_____

[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.

Por favor especificar detalles de su actividad:

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						
Facturación bruta por Internet, p.ej. de comercio electrónico						

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:

107 Servidores 657 Escritorios 731 Portátiles 147 Dispositivos móviles

2.3 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
www.senado.gov.co
Kactusweb.senado.gov.co
Calidad.senado.gov.co
Leyes.senado.gov.co
Sgda.senado.gov.co
Cael.arca.senado.gov.co
Soporte.senado.gov.co

3. Información del seguro

3.1 Seguro solicitado

Limites asegurados a cotizar (Cifras en COP):

Opción 1:

Opción 2:

Opción 3:

3.2 Extensiones de cobertura solicitadas:

☐ Cyber Extorsión ☐ Contenido Multimedia ☐ 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	3000		
☐	Información de Tarjetas de Pago			
☐	Información de salud personal	1000		
☐	Propiedad intelectual			
☐	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 elfin de crear una major 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

Q-2 ¿Son revisadas y aprobadas anualmente por la alta gerencia sus políticas de seguridad de la información? ☒ 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-3 ¿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

Q-4 ¿Tiene una lista actualizada de autoridades y contactos externos, que deben ser informados en caso de un incidente de seguridad de la información? ☒ 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-5 ¿Usted provee al menos formación anual para aumentar la conciencia de sus usuarios (empleados y contratistas) hacia la seguridad y para preparar a los usuarios a ser más resilientes y vigilantes contra el phishing? ☒ Sí ☐ No

Q-6 ¿Controla e informa a la gerencia sobre los entrenamientos de concientización de seguridad? ☒ Sí ☐ No

Q-7 ¿Ha identificado los roles (p.ej. usuarios privilegiados, administradores, ejecutivos) que necesitan capacitación personalizada de conciencia de seguridad? ☒ 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-8	¿Usted tiene una base de datos de gestión de configuración integral que incluye: todos los activos de TI, activos de la nube, dependencias, criticidad, propiedad, software y versiones de parche?	☐ Sí ☒ No
Q-9	¿Usted clasifica información con respecto a su confidencialidad?	☒ Sí ☐ No
Q-10	¿Usted clasifica información con respecto a su integridad y disponibilidad?	☒ Sí ☐ No
Q-11	¿Se implementan y aplican los procedimientos de etiquetado de información de acuerdo con el esquema de clasificación?	☐ Sí ☒ No
Q-12	¿El etiquetado de información se revisa regularmente?	☐ Sí ☒ No
Q-13	¿Usted brinda orientación sobre cómo manejar la información clasificada?	☐ Sí ☒ No
Q-14	¿Se revisa regularmente el tratamiento de la información para garantizar la coherencia con su clasificación?	☐ Sí ☒ No
Q-15	¿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
Q-16	¿Se requiere una autorización para los medios extraídos de la organización y se mantiene un registro de dichas extracciones para mantener una pista de auditoría?	☐ Sí ☒ No
Q-17	¿Usted desecha de forma segura la información si ya no se utiliza?	☒ Sí ☐ No
Q-18	¿Usted impone directrices que establecen que el contenido – si ya no es necesario – de cualquier medio reutilizable que pueda ser extraído de la organización se hace irrecuperable?	☒ Sí ☐ No

6.5. Control de accesso

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-19	¿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-20	¿Usted ha aplicado la autenticación de múltiples factores para el acceso remoto?	☒ Sí ☐ No ☐ N/A
Q-21	¿Usted ha definido e implementado una política para imponer la segregación de deberes?	☐ Sí ☒ No
Q-22	¿Usted ha implementado un sistema central de adiminstración de identidades y accesos para asignar y revocar los derechos de acceso?	☒ Sí ☐ No
Q-23	¿El propietario de la información autoriza el permiso de acceso?	☒ Sí ☐ No
Q-24	¿El propietario de la información revisa al menos anualmente los derechos de acceso?	☒ Sí ☐ No
Q-25	¿Usted prohíbe los derechos de administrador local en las estaciones de trabajo para los usuarios?	☒ Sí ☐ No
Q-26	¿Usted utiliza Identidad Privilegiada y Administración de Cuentas?	☒ Sí ☐ No
Q-27	¿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-28	¿Usted tiene un proceso para eliminar los derechos innecesarios de usuarios después de cambios de funciones en la organización?	☒ Sí ☐ No

Q-29	¿Usted ha implementado una política de contraseñas para garantizar que se utilicen contraseñas únicos, complejas y largas en su compañía?	☒ Sí ☐ No
Q-30	¿Se han cambiado todas las contraseñas predeterminadas en todos los dispositivos conectados al internet (p.ej. router)?	☒ Sí ☐ No
Q-31	¿Usted se asegura de que todos los usuarios tengan acceso a un software de administrador de contraseñas?	☐ 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-32	¿Están encriptados los datos sensibles y la información confidencial almacenados en bases de datos y servidores de archivos?	☐ Sí ☒ No
Q-33	¿Está encriptado todo tipo de datos sensibles e información confidencial cuando se almacena en dispositivos móviles como laptops o móviles?	☐ Sí ☒ No
Q-34	¿Usted utiliza una solución de gestión de dispositivos móviles para todas las computadoras portátiles y smartphones?	☐ Sí ☒ No
Q-35	¿Usted ha desarrollado e implementado una política sobre el uso, la protección y la duración de las claves criptográficas?	☐ Sí ☒ No
Q-36	¿Su poítica sobre claves criptográficas se revisa y actualiza regularmente durante todo su ciclo de vida?	☐ Sí ☒ No ☐ N/A

6.7. Seguridad física

Objetivo Cláusula 11 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-37	¿Usted ha implementado medidas avanzadas de seguridad física y controles ambientales (como cerraduras de puertas y armarios, alarmas antirrobo, alarmas contra incendio, extintores de incendios, CCTV)?	☒ Sí ☐ No
Q-38	¿Usted mantiene una lista del personal (empleados, proveedores y visitantes) con acceso autorizado a sus predios y áreas de seguridad sensible?	☒ Sí ☐ No
Q-39	¿Usted ha instalado controles avanzados de entrada (p.ej. control de acceso biométrico)?	☒ 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-40	¿Usted ha implementado y documentado procedimientos de gestión de cambios para los sistemas críticos?	☒ Sí ☐ No
Q-42	¿Sus procesos de gestión de cambios incluyen pruebas, escenarios de recuperación e informes?	☒ Sí ☐ No
Q-43	¿Al tomar decisiones de cambiar el entorno de TI siempre usted siempre tiene en cuenta los requisitos del negocio?	☒ Sí ☐ No
Q-44	¿Está separado el entorno de TI de desarrollo y prueba del entorno de TI productivo?	☒ Sí ☐ No ☐ N/A

Q-45	¿Utilizan sus desarrolladores diferentes cuentas para el desarrollo, las pruebas y las tareas cotidianas?	☐ Sí ☐ No
Q-46	¿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-47	¿Las actualizaciones de los archivos de firmas anti-malware se descargan y se instalan automáticamente?	☒ Sí ☐ No
Q-48	Además de la detección tradicional basada en firmas, ¿su protección contra malware utiliza también mecanismos avanzados de detección heurístico y basado en el comportamiento para proteger contra el malware moderno?	☒ Sí ☐ No
Q-49	¿Usted realiza copias de seguridad periódicas de datos críticos para el negocio según su política de copias de seguridad al menos diariamente?	☒ Sí ☐ No
Q-50	¿Usted almacena varias generaciones redundantes de archivos de copia de seguridad físicamente separadas de su red (p.ej. fuera de los predios de la oficina)?	☐ Sí ☒ No
Q-51	¿Usted se asegura regularmente de que las copias de seguridad de datos son completas y que se puedan restaurar lo más rápido posible con un impacto mínimo?	☒ Sí ☐ No
Q-52	¿Usted ha implementado un proceso de instalación de software centralizado?	☐ Sí ☒ No
Q-53	¿Usted instala parches de seguridad en sistemas críticos de TI y aplicaciones críticas al menos mensualmente?	☒ Sí ☐ No
Q-54	¿Usted instala parches de seguridad en sistemas de TI orientados a Internet al menos semanalmente?	☒ Sí ☐ No
Q-55	¿Usted realiza regularmente exploraciones de vulnerabilidades, identifica el riesgo asociado y toma las medidas adecuadas?	☒ Sí ☐ No
Q-56	¿Usted impone políticas que los usuarios no pueden instalar software en sus estaciones de trabajo por si mismo?	☒ 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-57	¿Están protegidos por firewalls de próxima genreación todos los puntos de acceso a Internet?	☒ Sí ☐ No
Q-58	¿Usted protege sus redes inalámbricas usando el estándar WPA2?	☒ Sí ☐ No ☐ N/A
Q-59	¿Usted ha implementado una tecnología de control de acceso a la red para acceder a las redes inalámbricas de su empresa?	☒ Sí ☐ No
Q-59	¿Usted ha implementado un sistema de prevención de intrusiones?	☒ Sí ☐ No
Q-60	¿Usted controla el tráfico entre las redes de confianza y las que no son de confianza (p.ej. con un sistema de detección de intrusiones?	☒ Sí ☐ No
Q-61	¿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 demilitarizada "DMZ" o en un proveedor externo)?	☒ Sí ☐ No
Q-62	¿Están segregados todos los segmentos de alto riesgo de la red (p.ej. sistemas PoS, procesamiento/almacenamiento de datos PHI, etc.)?	☒ Sí ☐ No
Q-63	¿Está encriptada toda la comunicación confidencial (p.e. a través de correo electrónico)?	☒ Sí ☐ No
Q-64	¿Usted ha implementado una Infraestructura de Claves Públicas y asegura correos con S/MIME?	☒ 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 sitemas 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-65	¿Su servidor web encripta los datos confidenciales (p.ej. HTTPS)?	☒ Sí ☐ No
Q-66	¿Usted protege sus servidores web contra ataques de denegación de servicio (p.ej. mediante la utilización de un proveedor de red de entrega de contenido)?	☒ Sí ☐ No
Q-67	¿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-68	¿Usted lleva a cabo pruebas automatizadas de seguridad o análisis de códigos?	☒ Sí ☐ No
Q-69	¿Usted realiza pruebas de penetración de sistemas de información antes de la puesta en marcha?	☐ Sí ☒ No
Q-70	¿Usted se asegura de que todos los detalles confidenciales de la información para fines de prueba estén protegidos por eliminación o modificación?	☐ 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-71	¿Usted ha identificado y ordenado controles de seguridad de la información para abordar específicamente el acceso de los proveedores a su información en una política?	☐ Sí ☒ No
Q-72	¿Los acuerdos con proveedores externos de servicios requieren niveles de seguridad proporcionales al nivel de seguridad de su información?	☒ Sí ☐ No ☐ N/A
Q-73	¿Usted revisa y actualiza periódicamente todos sus acuerdos con terceros?	☒ Sí ☐ No
Q-74	¿Usted estipula el derecho de auditorías a terceros dentro de sus acuerdos contractuales?	☐ Sí ☐ No
Q-75	Usted y sus filiales ¿requieren indemnización de los subcontratistas por cualquier responsabilidad que se les impute a los mismos?	☐ Sí ☒ No

6.12. Gestión de incidentes de la seguridad informática

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

Q-76	¿Usted tiene un equipo de respuesta a incidentes que cuenta con la capacidad para analizar y manejar incidentes (p.ej. coordinación, análisis forense, descontaminación del sistema, restauración, etc.)?	☒ Sí ☐ No
Q-77	¿Usted tiene implementado un plan de respuesta a incidentes de la seguridad de la información?	☒ Sí ☐ No
	En caso afirmativo, ¿este plan se prueba anualmente?	☐ Sí ☒ No
Q-78	¿Conocen todos los empleados y contratistas su responsabilidad de informar eventos de seguridad de la información?	☒ Sí ☐ No
Q-79	¿Es conocida por todos los empleados y contratistas la línea de informes de un evento de seguridad de la información?	☒ Sí ☐ No
Q-80	¿Usted documenta todos los eventos de la seguridad de la información en un sistema central de la información de seguridad y gestión de eventos?	☒ Sí ☐ No

Q-81	¿Se requiere a los empleados y contratistas que informen una debilidad de seguridad de la información (aún no un incidente o evento) en sistemas o sercvicios?	☒ Sí ☐ No
Q-82	¿Usted ha establecido un proceso de escalación para incidentes de la seguridad de la información?	☒ Sí ☐ No
Q-83	¿Usted recolecta evidencia para el análisis forense?	☐ Sí ☒ No
Q-84	¿Usted informa regularmente a la gerencia sobre incidentes pasados?	☒ 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. Garantizar la disponibilidad de las instalaciones de procesamiento de información.

Q-85	¿Usted ha realizado un análisis de impacto de negocio ("BIA")?	☐ Sí ☒ No
Q-86	¿Están definidos y documentados para los sistemas y procesos críticos los objetivos de tiempo de recuperación y los objetivos de punto de recuperación?	☐ Sí ☐ No
Q-87	¿Usted tiene implementado un plan de gestión de continuidad de negocio?	☐ Sí ☒ No
Q-88	¿Usted tiene implementado un plan de recuperación de desastres de TI?	☐ Sí ☒ No
Q-89	¿Usted tiene implementado controles avanzados de implementación para las capacidades de recuperación de desastres (p. ej. redundancia total o mecanismos automáticos de conmutación por error)?	☒ Sí ☐ No
Q-90	¿El plan de gestión de continuidad de negocio y el plan de recuperación de desastres se prueban anualmente?	☐ Sí ☒ No
Q-91	¿Usted revisa y actualiza el plan de gestión de continuidad de negocio y el plan de recuperación de desastes por lo menos anualmente?	☐ Sí ☒ No
Q-92	¿Los resultados de las actividades de la prueba de continuidad se revisan, documentan, informan a la gerencia y se revisan los planes en base a las lecciones aprendidas?	☐ Sí ☒ No ☐ Sí ☐ No
Q-93	¿Sus instalaciones de procesamiento de información están implementadas con redundancia?	☒ Sí ☐ No
Q-94	¿Usted realiza regularmente pruebas de redundancia para garantizar que la conmutación por error de un componente a otro funcione según lo previsto?	☒ 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-95	¿Usted protege los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de conformidad con los requisitos legales, regulatorios, contractuales y comerciales?	☒ Sí ☐ No
Q-96	¿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-97	¿Su Oficial de Privacidad informa regularmente a la alta gernecia?	☐ Sí ☒ No
Q-98	¿Usted tiene una política de privacidad y protección de información personal identificable desarrollada e implementada?	☒ Sí ☐ No
Q-99	¿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 electrónicos/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 clients, 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.

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? ☐ Sí ☒ No
En caso afirmativo, ¿con qué frecuencia?
☐ 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?

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

HIS-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
HIS-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
HIS-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
HIS-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
HIS-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 compeltos.	☐ Sí ☒ No
HIS-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(s)

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

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 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.

Firma autorizada del Solicitante: _____

Nombres y Apellidos:

Representante legal de Razón Social:

Correo electrónico

Fecha:

ELABORÓ:LENIN JOSE PALOMINO BLANCO –jefe Division Planeacion y Sistemas

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: Resúmen – Sectores industriales

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

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, television, cine, teatro.
Fabricación	Compañías fabricando o procesando bienes, sobre todo en grandes cantidades y a través de maquinaría 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. dispositivios 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.
Otros	