# FORMULARIO PARA LA EVALUACIÓN DEL RIESGO CIBERNÉTICO

## Introducción

Este cuestionario no es una oferta ni un contrato de seguro vinculante. Además, su diligenciamiento no obliga a la compañía de seguros a ofrecerle cobertura alguna. Las respuestas a este cuestionario son muy importantes para evaluar el riesgo con el fin de proporcionar un seguro cibernético para su compañía en base a esta información. Por lo tanto, confiamos en sus declaraciones hechas en el cuestionario, que son la base del contrato de seguro. Si no tiene un recurso de seguridad de la información, entonces el cuestionario debe ser complementado por un representante principal (propietario o miembro de la junta).

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

Moneda de las cifras en este cuestionario: ☐ USD ☐ EUR ☐X COP ☐ Otros: .....

## 1 Información del solicitante

| | | |
|---|---|---|
| Nombre de la compañía | Universidad Militar Nueva Granada | |
| Dirección | Carrera 11 No.101-80 | |
| País | Colombia | |
| Correo electrónico | tic@unimilitar.edu.co | |
| Número telefónico | 3214563155 | |
| Filiales a asegurar | No aplica | |
| Nombres de todos los sitios web que deberían ser cubiertos por este seguro | https://www.umng.edu.co/<br>https://noticias.umng.edu.co/<br>https://radio.umng.edu.co/<br>https://channel.umng.edu.co/<br>https://episio.umng.edu.co/<br>https://isashilpalaa.umng.edu.co/ | |

## 1.1 Actividad(es) industrial(es)

Por favor marcar todas las actividades industriales aplicables. Detalles y explicaciones se encuentran en el anexo en página 11.

- ☐ Alimentación & Agricultura
- ☐ Autoridad pública; ONG, sin fines de lucro
- ☐ Defensa / Contratista Militar
- ☐X Educación
- ☐ Entretenimiento & Medios
- ☐ Fabricación
- ☐ Minería & Industrias Primarias
- ☐ Productos farmacéuticos
- ☐ Propiedad Inmobiliaria & Construcción
- ☐ Salud
- ☐ Servicios Financieros - Bancos
- ☐ Otros
- ☐ Servicios Financieros – Gestión de inversiones
- ☐ Servicios Financieros – Seguros
- ☐ Servicios profesionales
- ☐ Tecnología de la información – Hardware
- ☐ Tecnología de la información – Servicios
- ☐ Tecnología de la información – Software
- ☐ Telecomunicaciones
- ☐ Transporte / Aviación / Aeroespacial
- ☐ Turismo & Hospitalidad
- ☐ Utilidades
- ☐ Venta al por menor

| | |
|---|---|
| En caso de "Otros", por favor especificar | El objeto principal es la educación superior y la investigación, dirigidas a elevar la preparación académica de los miembros de las Fuerzas Militares y de la Policía Nacional, en actividad o en retiro; los empleados civiles del sector defensa, los familiares de todos los anteriores, y los particulares que se vinculen a la universidad. |

## 1.2 Facturación/ingresos y huella regional

| | Local | EE.UU | Unión Europea | Resto del mundo |
|---|---|---|---|---|
| Su facturación / ingresos durante el último año fiscal | $ 350.634.221.875 | | | |
| Parte de su facturación / ingresos creados en línea durante el último año fiscal | $ 21.741.863.670 | | | |

| | Último año | Año anterior | Dos años anteriores |
|---|---|---|---|
| Su beneficio bruto (o equivalente) | $ 97.289.836.600 | $ 140.794.868.315 | $ 117.159.317.342 |

| | | | | |
|---|---|---|---|---|
| Por favor indicar número de empleados | | | | |
| Por favor indicar el número (estimado) de dispositivos individuales de TI implementados | 64 | Servidores | 3605 | Computadores de escritorio |
| | 399 | Ordenadores portátiles | 49 | Dispositivos móviles |

## 1.3 Tipo y cantidad de datos

Por favor estimar el tipo y volumen de las siguientes categorías de datos sensibles que su compañía maneja/procesa según su conocimiento:

| | Tipo de datos | Número de registros únicos | Número de registros únicos de ciudadanos de EE.UU. | Número de registros únicos almacenados en centros de datos en EE.UU. |
|---|---|---|---|---|
| ☒ | Información de Identificación Personal (PII) | 17228 | | |
| ☐ | Información de Tarjetas de Pago (PCI) | NA | NA | NA |
| ☒ | Información de salud personal (PHI) | 2263 | | |
| | | | | |
| ☒ | Propiedad Intelectual (IP) | No hay información disponible por actualización en herramienta SIVIN | | |

## 1.4 Cobertura de seguro solicitado

| | | | | |
|---|---|---|---|---|
| Período de la póliza | De | | a | |
| Límite agregado solicitado | | | | |

## 1.5 Seguro anterior

1 ¿Actualmente tiene o ha tenido un seguro de ciber con la misma cobertura o cobertura similar a la solicitada actualmente? ☐ Sí ☐ X No

2 ¿Alguna aseguradora ha cancelado o no ha renovado una póliza que proporcione la misma cobertura o cobertura similar a la que solicita el seguro? ☐ Sí ☐ X No

## 1.6 Incidentes de seguridad e Historial de pérdidas

**Por favor responda a las siguientes preguntas considerando cualquier momento durante los últimos tres años.**

1 ¿Ha tenido algún **incidente, reclamo o demanda** que involucren el acceso no autorizado o el uso indebido de su red, incluyendo malversación, fraude, robo de información de propiedad exclusiva, violación de información personal, robo o pérdida de computadoras portátiles, denegación de servicio, vandalismo electrónico o sabotaje, virus informático u otro incidente? ☐ Sí ☐ X No

2 ¿Ha experimentado una **interrupción de negocio no planeada** de más de cuatros horas causada por un incidente cibernético? ☐ Sí ☐ X No

3 ¿Ha experimentado un **intento o demanda de extorsión** con respecto a sus sistemas informáticos? ☐ X Sí ☐ No

4 ¿Ha recibido alguna **reclamación o queja** con respecto a denuncias de difamación, invasión o lesión de la privacidad, robo de información, violación de la seguridad de la información, transmisión de malware, participación en un ataque de denegación de servicio, solicitud para notificar a personas debido a un hecho real o sospecha de divulgación de información personal? ☐ Sí ☐ X No

| | | |
|---|---|---|
| 5 | ¿Ha estado sujeto a alguna **acción, investigación o citación gubernamental** con respecto a cualquier (supuesta) violación de alguna ley o regulación de privacidad? | ☐ Sí ☐ X No |
| 6 | ¿Está consiente de cualquier **publicación, pérdida o divulgación de información de identificación personal** en su cuidado, custodia o control, o en el control de cualquier persona que tenga dicha información en su nombre? | ☐ Sí ☐ X No |
| 7 | ¿Está consiente de **algún hecho, circunstancia, situación, error u omisión real o alegado, o un problema potencial** que pueda dar lugar a una pérdida o reclamación en su contra en virtud de la presente póliza de seguro cibernético o cualquier otro seguro similar actual o anterior? | ☐ Sí ☐ X No |

**Si se responde "sí" a una o más preguntas de esta sección 1.6, por favor adjuntar una descripción incluyendo detalles completos (causa, costos, notificación, tiempo hasta descubrimiento, tiempo de recuperación y pasos tomados para mitigar futuras exposiciones) de cada evento (incidente, reclamación, etc.).**

## 1.7 Marcos y estándares

Por favor marcar todos los marcos legales que tiene que cumplir.

| | | | |
|---|---|---|---|
| ☐ | Reglamento General de Protección de Datos (GDPR) de la Unión Europea (EU) | ☐ | US Federal Privacy Act |
| ☐ | US Health Insurance Portability and Accountability Act (HIPAA) y US Health Information Technology for Economic and Clinical Health (HITECH) Act | ☐ | Otros |

Por favor marcar todos los estándares para los que haya sido auditado con éxito o tenga una certificación válida.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ☐ | Payment Card Industry Data Security Standard (PCI DSS) | | | | | | |
| ☐ | Nivel mercantil 1 | ☐ | Nivel mercantil 2 | ☐ | Nivel mercantil 3 | ☐ | Nivel mercantil 4 |

| | | | |
|---|---|---|---|
| ☐ | ISO 27001:2013 Information security management systems | ☐ | NIST (US National Institute of Standards and Technology) Cybersecurity Framework |
| ☐ | Critical Security Controls | ☐ | Otros |

| | | | |
|---|---|---|---|
| ☐ | COBIT 5 (Control Objectives for Information and Related Technologies) | ☐ | Information Security Forum (ISF) The Standard of Good Practice for Information Security 2018 |

| | |
|---|---|
| Sí aplican otros estándares, por favor detallar | |

| | |
|---|---|
| Por favor detallar el ámbito de la certificación | La Universidad Militar Nueva Granada cuenta con un plan de implementación de la ISO 27001:2022 para obtener el 100% de la implementación en noviembre de 2025 |

# 2 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/IEC 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 controles de seguridad de ISO.

## 2.1 Políticas de seguridad informática

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted tiene una política formal de seguridad de la información desarrollada, implementada a nivel corporativo y permanentemente disponible para todos los empleados y partes externas relevantes? | ☐X Sí ☐ No |
| 2 | ¿Son revisadas anualmente y aprobadas por la alta gerencia sus políticas de seguridad de la información? | ☐ X Sí ☐ No |

## 2.2 Organización de la seguridad de la información

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Tiene su compañía una persona responsable para la seguridad informática (p.ej. Chief Information Security Officer "CISO")? | ☐ X Sí ☐ No |
| 2 | ¿Su persona responsable para la seguridad de TI reporta regularmente a la alta gerencia? | ☐ X Sí ☐ No |
| 3 | ¿Tiene una lista actualizada de autoridades y contactos externos, que deben ser informados en caso de un incidente de seguridad de la información? | ☐ X Sí ☐ No |

## 2.3 Seguridad de los recursos humanos

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted provee formación por lo menos 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? | ☐ X Sí ☐ No |
| 2 | ¿Controla e informa a la gerencia sobre los entrenamientos de concientización de seguridad? | ☐ X Sí ☐ No |
| 3 | ¿Ha identificado los roles (p.ej. usuarios privilegiados, administradores, ejecutivos) que necesitan capacitación personalizada de conciencia de seguridad? | ☐ X Sí ☐ No |

## 2.4 Manejo de activos

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted mantiene un inventario actualizado de dispositivos de software (incl. sistemas operativos) y hardware en sus redes? | ☐ X Sí ☐ No |
| 2 | ¿Usted tiene una base de datos de gestión de configuración integral (CMDB – Configuration Management Database) que incluye: todos los activos de TI, activos de la nube pública, dependencias, criticidad, propiedad, software y versiones de parches? | ☐ Sí ☐ X No |
| 3 | ¿Usted utiliza una solución de gestión de dispositivos móviles (MDM – Mobile Device Management) para todas las computadoras portátiles y smartphones? | ☐ Sí ☐ X No |
| 4 | ¿Usted clasifica información con respecto a su confidencialidad? | ☐ Sí ☐ X No |
| 5 | ¿Usted clasifica información con respecto a sus requerimientos de integridad y disponibilidad? | ☐ Sí ☐ X No |
| 6 | ¿Se implementan y aplican los procedimientos de etiquetado de información de acuerdo con el esquema de clasificación? | ☐ Sí ☐ X No |
| 7 | ¿Usted ha aplicado técnicamente el esquema de clasificación de la información? | ☐ Sí ☐ X No |
| 8 | ¿Usted brinda orientación sobre cómo manejar la información clasificada? | ☐ Sí ☐ X No |
| 9 | ¿Se revisa regularmente el tratamiento de la información para garantizar la coherencia con su clasificación? | ☐ Sí ☐ X No |
| 10 | ¿Usted o limita el acceso o encripta la información confidencial almacenada en medios extraíbles, como dispositivos de almacenamiento externos (p.ej. memorias USB, discos duros)? | ☐ Sí ☐ X No |
| 11 | ¿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 ☐ X No |
| 12 | ¿Los puertos de medios (p.ej. USB) se administran de manera central o son generalmente desactivados? | ☐ Sí ☐ X No |
| 13 | ¿Usted desecha de forma segura los medios que contienen información confidencial si ya no se utilizan? | ☐ Sí ☐ X No |
| 14 | ¿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 ☐ X No |

## 2.5 Control de acceso

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿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 datos personales)? | ☐ X Sí ☐ No |
| 2 | ¿Usted ha aplicado la autenticación de múltiples factores para el acceso remoto? | ☐ Sí ☐ X No ☐ No aplica |
| 3 | ¿Usted tiene un proceso formal de aprovisionamiento de acceso para asignar y revocar los derechos de acceso? | ☐ X Sí ☐ No |
| 4 | ¿Usted ha implementado un sistema central de administración de identidades y accesos (IAM – Identity and Access Management) para asignar y revocar los derechos de acceso? | ☐ X Sí ☐ No |
| 5 | ¿El propietario de la información autoriza el permiso de acceso? | ☐ X Sí ☐ No |
| 6 | ¿Usted prohíbe los derechos de administrador local en las estaciones de trabajo para los usuarios? | ☐ Sí ☐ X No |
| 7 | ¿Usted utiliza Identidad Privilegiada y Administración de Cuentas (PIM – Privileged Identity Management; PAM – Privileged Access Management)? | ☐ Sí ☐ X No |
| 8 | ¿Usted revisa los derechos de acceso de los usuarios al menos una vez al año? | ☐ Sí ☐ X No |
| 9 | ¿Usted revisa las cuentas compartidas (p.ej. utilizadas para sistemas/aplicaciones de alto privilegio) al menos una vez al año? | ☐ Sí ☐ X No |
| 10 | ¿Usted revisa las autorizaciones para los derechos de acceso privilegiados a intervalos al menos cada dos años? | ☐ Sí ☐ X No |
| 11 | ¿Usted revoca todo el acceso al sistema, las cuentas de usuarios y los derechos asociados después de la terminación de los usuarios (incl. a empleados, empleados temporales, contratistas y proveedores)? | ☐ Sí ☐ X No |
| 12 | ¿Usted tiene un proceso para eliminar los derechos innecesarios de usuarios después de cambios de funciones en la organización? | ☐ Sí ☐ X No |
| 13 | ¿Usted ha implementado una política de contraseñas que impone el uso de contraseñas largas y complejas en su compañía? Contraseñas largas y complejas se definen como: 8 caracteres o más; no consiste en palabras incluidas en los diccionarios; libre de caracteres idénticos, numéricos o alfabéticos consecutivos. | ☐ X Sí ☐ No |
| 14 | ¿Se han cambiado todas las contraseñas predeterminadas en todos los dispositivos conectados al internet (p.ej. router)? | ☐ Sí ☐ X No |
| 15 | ¿Usted provee un software autorizado de administrador de contraseñas a todos los usuarios? | ☐ Sí ☐ X No |

## 2.6 Criptografía

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

| | | |
|---|---|---|
| 1 | ¿Está encriptada toda la información confidencial cuando se almacena en dispositivos móviles como laptops o móviles? | ☐ Sí ☐ X No |
| 2 | ¿Están encriptados los datos sensibles y la información confidencial almacenados en bases de datos y servidores de archivos? | ☐ Sí ☐ X No |
| 3 | ¿Usted ha desarrollado e implementado una política sobre el uso, la protección y la duración de las claves criptográficas? | ☐ Sí ☐ X No |
| 4 | ¿Su política sobre claves criptográficas se revisa y actualiza regularmente durante todo su ciclo de vida? | ☐ Sí ☐ X No |

## 2.7 Seguridad física y ambiental

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted mantiene una lista del personal (empleados, proveedores y visitantes) con acceso autorizado a sus predios y áreas de seguridad sensible? | ☐ Sí ☐ X No |
| 2 | ¿Usted ha instalado controles avanzados de entrada (p.ej. control de acceso biométrico)? | ☐ Sí ☐ X No |
| 3 | ¿Usted ha implementado controles avanzados de monitoreo de entrada (p.ej. 24/7 televisores de circuito cerrado (CCTV), documentación de cada acceso)? | ☐ Sí ☐ X No |

## 2.8 Seguridad operacional

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted ha implementado procedimientos de gestión de cambios para los sistemas críticos? | ☐ Sí ☐ X No |
| 2 | ¿Sus procesos de gestión de cambios incluyen pruebas, escenarios de recuperación e informes? | ☐ Sí ☐ X No |
| 3 | ¿Al tomar decisiones de cambiar el entorno de TI siempre usted siempre tiene en cuenta los requisitos del negocio? | ☐ Sí ☐ X No |
| 4 | ¿Está separado el entorno de TI de desarrollo y prueba del entorno de TI productivo? | ☐ X Sí ☐ No |
| 5 | ¿Utilizan sus desarrolladores diferentes cuentas para el desarrollo, las pruebas y las tareas cotidianas? | ☐ X Sí ☐ No |
| 6 | ¿Usted utiliza protección contra malware en proxy web, puerta de enlace de correo electrónico (email-gateway), estaciones de trabajo y computadoras portátiles? | ☐ X Sí ☐ No |
| 7 | ¿Las actualizaciones de los archivos de firmas anti-malware se descargan y se instalar automáticamente? | ☐ X Sí ☐ No |
| 8 | 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 ☐ X No |
| 9 | ¿Usted realiza copias de seguridad periódicas de datos críticos para el negocio al menos una vez a la semana? | ☐ X Sí ☐ No |
| 10 | ¿Usted almacena las copias de seguridad físicamente separadas de su red (p.ej. fuera de los predios de la oficina)? | ☐ Sí ☐ X No |
| 11 | ¿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? | ☐ X Sí ☐ No |
| 12 | ¿Usted produce y revisa regularmente registros de eventos que registran las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información (al menos desde sus firewalls y controlador de dominio)? | ☐ X Sí ☐ No |
| 13 | ¿Usted tiene un sistema de gestión de información y eventos de seguridad (SIEM – Security Information and Event Management) que incluya reglas para generar informes y alertas sobre la seguridad del sistema? | ☐ Sí ☐ X No |
| 14 | ¿Usted ha implementado un proceso de instalación de software centralizado? | ☐ Sí ☐ X No |
| 15 | ¿Usted aplica un enfoque estricto de administración de la configuración y desarrolla imágenes seguras que se utilizan para construir todas las estaciones de trabajo y servidores recientemente implementados? | ☐ X Sí ☐ No |
| 16 | ¿Usted aplica oportunamente - al menos dentro de un mes del lanzamiento – actualizaciones a sistemas aplicaciones de TI críticos ("parches de seguridad")? | ☐ X Sí ☐ No |
| 17 | ¿Usted instala oportunamente – al menos dentro de un mes del lanzamiento – parches de seguridad en sistemas y aplicaciones informáticas con acceso a Internet? | ☐ X Sí ☐ No |
| 18 | ¿Usted realiza regularmente exploraciones de vulnerabilidades, identifica el riesgo asociado y toma las medidas adecuadas? | ☐ Sí ☐ X No |
| 19 | ¿Usted garantiza técnicamente y organizativamente que los usuarios no deben instalar software en sus estaciones de trabajo por sí mismo? | ☐ X Sí ☐ No |

## 2.9 Seguridad de la comunicación

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Están protegidos todos los puntos de acceso a Internet por firewalls apropiadamente configurados? | ☐ X Sí ☐ No |
| 2 | ¿Están protegidos por firewalls de próxima generación todos los puntos de acceso a Internet? | ☐ X Sí ☐ No |
| 3 | ¿Usted ha implementado una tecnología de control de acceso a la red (NAC – Network Access Control) para acceder a las redes inalámbricas de su empresa? | ☐ Sí ☐ X No. |
| 4 | ¿Usted monitorea su red e identifica eventos de seguridad? | ☐ X Sí ☐ No |
| 5 | ¿Usted utiliza un sistema de detección de intrusiones (IDS – Intrusion Detection System)? | ☐ X Sí ☐ No |
| 6 | ¿Usted tiene un centro de operaciones de seguridad (SOC – Security Operations Centre) que supervise todos los eventos en base 24/7? | ☐ Sí ☐ X No |
| 7 | ¿Están segregados todos sus sistemas accesibles por Internet (p.ej. servidores web/de correo electrónico) de su red de confianza (p.ej. dentro de una zona desmilitarizada "DMZ" o en un proveedor externo)? | ☐ X Sí ☐ No ☐ No aplica |
| 8 | ¿Están segregados todos los segmentos de red de alto riesgo (p.ej. sistemas de punto de venta (PoS – Point of Sales), procesamiento de datos confidenciales, redes de producción de tecnología de oficina y operacionales, etc.)? | ☐ X Sí ☐ No |
| 9 | ¿Está encriptada la comunicación confidencial (p.ej., correos electrónicos seguros con SMIME (Secure Multipurpose Internet Mail Extensions) o SMTP-over-TLS (Simple Mail Transfer Protocol Secure))? | ☐ X Sí ☐ No |
| 10 | ¿Usted utiliza software de prevención de pérdida de datos (DLP – Data Loss Prevention)? | ☐ Sí ☐ X No |

## 2.10 Adquisición, desarrollo y mantenimiento de sistemas

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Su servidor web encripta los datos confidenciales (p.ej. HTTPS)? | ☐ X Sí ☐ No ☐ No aplica |
| 2 | ¿Usted hace pruebas de las funcionalidades de seguridad durante el ciclo de vida de desarrollo de los sistemas de información, incluyendo actualizaciones de seguridad de TI? | ☐ Sí ☐ X No ☐ No aplica |
| 3 | ¿Usted está considerando aspectos de confidencialidad al utilizar datos operacionales para pruebas para garantizar que todos los detalles sensibles estén protegidos por eliminación o modificación? | ☐ X Sí ☐ No ☐ No aplica |

## 2.11 Relaciones con proveedores

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted ha identificado y documentado todos sus proveedores importantes (incluyendo a proveedores de servicios externos)? | ☐ X Sí ☐ No |
| 2 | ¿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? | ☐ X Sí ☐ No |
| 3 | ¿Los acuerdos con proveedores externos de servicios requieren niveles de seguridad proporcionales al nivel de seguridad de su información? | ☐ X Sí ☐ No |
| 4 | ¿Usted revisa y actualiza periódicamente los acuerdos con sus proveedores importantes (incluyendo proveedores de servicios externos)? | ☐ X Sí ☐ No |
| 5 | ¿Usted estipula el derecho de auditorías a terceros dentro de sus acuerdos contractuales? | ☐ Sí ☐ X No |
| 6 | ¿Usted monitorea las actividades de los proveedores de servicios externos para detectar eventos de seguridad a fin de mantener un nivel acordado de seguridad de la información? | ☐ Sí ☐ X No |
| 7 | ¿Usted realiza auditorías (evaluaciones de seguridad de la información) de proveedores (incluidos proveedores de servicios externos) y realiza un seguimiento de los problemas identificados? | ☐ Sí ☐ X No |

| | | |
|---|---|---|
| 8 | ¿Incluyen sus contratos escritos y firmados con los proveedores (incluyendo los proveedores de servicios externos) un acuerdo sin reservas (hold harmless agreement) o una renuncia de responsabilidad a su favor en caso de que dichos proveedores no protejan sus datos confidenciales? | ☐ X Sí ☐ No |

## 2.12 Gestión de incidentes de la seguridad informática

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted tiene implementado un plan de respuesta a incidentes de la seguridad de la información? | ☐ X Sí ☐ No |
| 2 | ¿Usted tiene una persona asignada responsable para la respuesta a incidentes? | ☐ X Sí ☐ No |
| 3 | ¿Se prueba anualmente su plan de respuesta a incidentes de seguridad? | ☐ Sí ☐ X No |
| 4 | ¿Es conocida por todos los empleados y proveedores externos la línea de informes de un evento de seguridad de la información? | ☐ Sí ☐ X No |
| 5 | ¿Conocen todos los empleados y contratistas su responsabilidad de informar eventos de seguridad de la información? | ☐ X Sí ☐ No |
| 6 | ¿Usted documenta todos los eventos de la seguridad de la información en un sistema central de la información de seguridad y gestión de eventos (SIEM – Security Information and Event Management)? | ☐ Sí ☐ X No |
| 7 | ¿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 servicios? | ☐ X Sí ☐ No |
| 8 | ¿Usted ofrece un programa de recompensas para informar errores o vulnerabilidades ("bug bounty program")? | ☐ Sí ☐ X No |
| 9 | ¿Usted ha establecido un proceso de escalación para incidentes de la seguridad de la información? | ☐ X Sí ☐ No |
| 10 | ¿Usted recolecta evidencia para el análisis forense? | ☐ Sí ☐ X No |
| 11 | ¿Usted informa regularmente a la gerencia sobre incidentes pasados? | ☐ Sí ☐ X No |
| 12 | ¿Usted utiliza el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros? | ☐ X Sí ☐ No |
| 13 | ¿Usted cuantifica y monitorea los tipos, volúmenes y costos de los incidentes de seguridad de la información? | ☐ Sí ☐ X No |

## 2.13 Aspectos de seguridad de la información en la gestión de continuidad del negocio

**Objetivo:** La continuidad de la seguridad de la información debe integrarse en los sistemas de gestión de la continuidad del negocio de la organización.

| | | |
|---|---|---|
| 1 | ¿Usted ha realizado un análisis de impacto de negocio ("BIA")? | ☐ Sí ☐ X No |
| 2 | ¿Están definidos y documentados para los sistemas y procesos críticos los objetivos de tiempo de recuperación (RTO – Recovery Time Objectives) y los objetivos de punto de recuperación (RPO – Recovery Point Objectives)? | ☐ X Sí ☐ No |
| 3 | ¿Usted tiene implementado un plan de continuidad de negocio que se dirija específicamente a los incidentes cibernéticos? | ☐ Sí ☐ X No |
| 4 | ¿Usted tiene implementado un plan de recuperación de desastres de TI? | ☐ Sí ☐ X No |
| 5 | ¿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 ☐ X No |
| 6 | ¿Usted prueba por lo menos anualmente sus planes de continuidad de la seguridad de la información (p.ej. plan de gestión de continuidad de negocio, plan de recuperación d desastres? | ☐ Sí ☐ X No |
| 7 | ¿Usted revisa y actualiza por lo menos anualmente sus planes de continuidad de la seguridad informática (p.ej. Continuidad de negocio, Recuperación de desastre)? | ☐ Sí ☐ X No |
| 8 | ¿Los resultados de las actividades de la prueba de continuidad se revisan, documentar informan a la gerencia y se revisan los planes en base a las lecciones aprendidas? | ☐ Sí ☐ X No |
| 9 | ¿Sus instalaciones de procesamiento de información (i.e. cualquier sistema, servicio o infraestructura o ubicación física que lo albergue) están implementadas con redundancia? | ☐ Sí ☐ X No |

| | | |
|---|---|---|
| 10 | ¿Usted realiza regularmente – por lo menos anualmente - pruebas de redundancia para garantizar que la conmutación por error de un componente a otro funcione según lo previsto? | ☐ Sí ☐ X No |

## 2.14 Compliance

**Objetivo:** 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.

| | | |
|---|---|---|
| 1 | ¿Usted tiene implementado un procedimiento para cumplir de manera permanente con requisitos legales (o contractuales) y regulaciones de privacidad? | ☐ Sí ☐ X No |
| 2 | ¿Usted ha asignado un Oficial de Cumplimiento? | ☐ Sí ☐ X No |
| 3 | ¿Su Oficial de Cumplimiento reporta regularmente a la alta gerencia? | ☐ Sí ☐ X No |
| 4 | ¿Usted tiene pautas emitidas sobre la retención, almacenamiento, manejo y eliminación de registros e información? | ☐ Sí ☐ X No |
| 5 | ¿Usted tiene un cronograma de retención documentado para identificar los registros y el período de tiempo durante el cual deben conservarse? | ☐ X Sí ☐ No |
| 6 | ¿Usted tiene una persona responsable para brindar orientación y garantizar el conocimiento de los principios de privacidad (p. ej. Oficial de Privacidad)? | ☐ Sí ☐ X No |
| 7 | ¿Su Oficial de Privacidad reporta regularmente a la alta gerencia? | ☐ Sí ☐ X No |
| 8 | ¿Usted tiene una política de privacidad y protección de información personal identificable desarrollada e implementada? | ☐ Sí ☐ X No |
| 9 | ¿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? | ☐ X Sí ☐ No |

# 3 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 mejor conocimiento, respuestas ciertas 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.

FIRMA: _____

NOMBRE: **Mayor General (R) JAVIER ALBERTO AYALA AMAYA, Ph.D.**
C.C. No. 94.306.994 de Palmira
CARGO: Rector de Universidad Militar Nueva Granada
DIRECCIÓN: Carrera 11 N° 101- 80 /Edificio Administrativo.
TELÉFONO: 6500000 Ext. 1002
NIT: 800.225.340-8
FECHA: Bogotá, D.C, marzo de 2025

Vo.Bo.

- Tecnología de Información y Communications -Tic: (numeral 1-1.1-1.2-1.3-1.4-1.5-1.6-1.7-numeral 2-2.1-2.2-2.3-2.4-2.5-2.6-2.7-2.8-2.9-2.10-2.11-2.12-2.13-2.14. _____
  Correo electrónico: tic@unimilitar.edu.co
- División Financiera: (numeral 1.2 "Su facturación / ingresos durante el último año fiscal
  Su facturación /ingresos durante el último año fiscal
  Parte de su facturación / ingresos creados en línea durante el último año fiscal _____
- Oficina Protección de Patrimonio _____
  Correo electrónico: proteccion.patrimonio@unimilitar.edu.co
- Oficina Jurídica: (revisión) _____

# Anexo 1: Resumen – Actividades 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 farmacéuticos | 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 on 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 / Aeroespacial | 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 | |

Fuente: Cyber Insurance exposure data schema v1.0 by Cambridge Centre for Risk Studies