# DECLARACIÓN DE ASEGURABILIDAD

## Preguntas adicionales (SBS)

1. Los procedimientos internos de protección de datos cumplen con la legislación de protección de datos y privacidad aplicable en todas las jurisdicciones y con las normas/requisitos de la industria en la que operan (Explicar):

La para protección de datos personales de los estudiantes, funcionarios y contratistas, establece el manual integral de Protección de Datos Personales de la Universidad Militar Nueva Granada, la cual se rige por la ley 1581 de 2012.

2. ¿La empresa cumple con una o más de las siguientes leyes de Seguridad / marcos de acción / estándares / requisitos?
    i. ISO 27000 y siguientes
    ii. HIPAA/HITECH
    iii. NIST
    iv. PCI-DSS (Nivel)
    v. Regulación de protección de datos de la UE
    vi. COBIT
    vii. Otro:
    viii.

3. **Controles para publicación de contenidos multimedia**
    a. ¿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? (NO)

    b. ¿Tiene un proceso para revisar todo el contenido antes de que sea publicado por o en nombre de la compañía? (SI)

## Preguntas adicionales (Berkley)

4. Implementa la solución EDR (detección y respuesta de puntos finales) en todos los puntos finales críticos y servidores (SI)

5. **Implementación de autenticación multifactor para:**
    a) Acceso remoto a aplicaciones basadas en la nube (Microsoft O365, Microsoft Azure, Workday, SalesForce, etc.) (NO)
    b) Acceso remoto a cualquier sistema de correo electrónico corporativo (NO)
    c) Implementa la solución de administración de dispositivos móviles (MDM) para acceder al correo electrónico corporativo en dispositivos móviles (NO)

6. **Limitación y control de puertos de red:**
    a) El puerto RDP se ha desactivado / cerrado o no se ha expuesto a Internet (SI)
    b) El puerto SMB se ha desactivado / cerrado (SI)

7. **Implementa los siguientes controles de seguridad del correo electrónico:**
   a) Herramientas de filtrado de spam (SI)
   b) Autenticación de correo electrónico (SPF, DKIM, DMARC) (SI)
   c) Tecnología para alertar a los usuarios de correo electrónico de correos electrónicos externos vs internos (SI)
   d) Pasarela de correo electrónico segura (NO)
   e) Sandboxing para analizar y bloquear archivos adjuntos de correo electrónico entrantes con comportamiento malicioso (NO)

8. **Implementación de las mejores prácticas para usuarios de Microsoft Office 365 (si aplica, en caso de no aplicar indique la casilla NO APLICA)** (SI)
   a) Habilite el registro de auditoría unificado y el registro de auditoría del buzón (SI)
   b) Configura y habilita la prevención de pérdida de datos (DLP) (SI)
   c) Habilita la autenticación multifactor (MFA) (NO)
   d) Habilita la seguridad de las aplicaciones en la nube de Office 365 (NO APLICA)
   e) Habilita la puntuación de seguridad de Microsoft (NO APLICA)

9. **Privilegio administrativo deshabilitado en todos los puntos finales para usuarios habituales** (SI)

10. **Mejores prácticas de copia de seguridad y recuperación implementadas:**
    a) Copia de seguridad incremental y completa periódica de servidores clave, aplicaciones y bases de datos (SI)
    b) Cifra las copias de seguridad y la clave de cifrado de segmentos (SI)
    c) Objetivo de tiempo de recuperación para una restauración completa desde la copia de seguridad en menos de 24 horas (SI)
    d) Las copias de seguridad de servidores clave, aplicaciones y bases de datos son inmutables (SI)
    e) Plan establecido que prioriza las aplicaciones clave, los servidores y las bases de datos para la restauración a fin de minimizar el tiempo de inactividad (SI)
    f) Implementa varios métodos de respaldo, como almacenamiento en la nube y respaldo local (NO)

11. **Mantiene una gestión de parches periódica:**
    a) Sigue los parches de Microsoft Patch Tuesday dentro de los 30 días (SI)
    b) Análisis de vulnerabilidades mensuales para garantizar que se realicen los parches correctamente en los sistemas y aplicaciones (SI)
    c) Proceso para parchear los CVE más comúnmente explotados publicados dentro de los 30 días. (SI)
    d) Proceso para implementar parches críticos fuera del ciclo cuando se considere una amenaza inmediata por parte del fabricante o agencia gubernamental (SI)

12. **Formaliza y prueba el plan de respuesta a incidentes anualmente:**
    a) Libro de estrategias establecido para incidentes comunes que afectan a la industria, como BEC, ransomware, fondos Fraude de transferencia.
    b) Se testea el plan de respuesta a incidentes anualmente.

13. **Controles de fraude en transferencias de fondos:**
    a) Implementa un procedimiento de verificación establecido y documentado con respecto a todas las transferencias electrónicas de fondos. (SI)
    b) Exige la validación de cualquier cambio solicitado al beneficiario o detalles de pago con una persona que no sea la persona que solicita el cambio antes de realizar cualquier cambio. (SI)

    c) El proceso requiere la aprobación del supervisor o del siguiente nivel de todas las transferencias electrónicas de fondos, incluidas las transferencias electrónicas o ACH. (SI)

d) El proceso requiere que antes de iniciar una transferencia de fondos, la solicitud sea autenticada por (marque todo lo que corresponda): (SI)

*teléfono utilizando un número previamente registrado para la autenticación y que no sea un número de teléfono incluido en la solicitud recibida (SI/NO) (SI)
*correo electrónico utilizando una dirección de correo electrónico con un dominio de la empresa y previamente archivada para la autenticación, que no sea la dirección de correo electrónico desde la que se recibió la solicitud o cualquier otra dirección de correo electrónico adjunta a esa solicitud. (SI/NO) (SI)
* código de autenticación único (SI/NO) (SI)
Otro:

Yo, el abajo firmante, como la persona que actúa en representación del solicitante, DESPUÉS DE UNA INVESTIGACIÓN RAZONABLE, confirmo que:

- Piruvato si hay oxigeno pasa al ciclo de Ckeps
-
- No tengo conocimiento de ninguna circunstancia que (a su leal saber y entender) pudiera dar lugar a una reclamación en contra del solicitante, sus predecesores en el negocio o socio, director o empleado pasado o presente.

Fecha: Bogotá D.C, Septiembre de 2022

Firma: _____
NOMBRE: **BG. (R) 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: **Bogotá D, C septiembre de 2022**

Firma: _____
NOMBRE: **Coronel (RA) ENRIQUE LUIS COTES PRADO**
CARGO: **Jefe Oficina de Protección al Patrimonio**
**Oficial encargado de Seguridad Informática**

Vo.Bo.

- Oficina Asesora de las Tecnologías: (numerales 1,2,4,5,6,7,8,9,10,11) _____
- División de Publicaciones: (numeral: 3)_____
- Oficina de Protección al Patrimonio:( numeral: 12)_____
- División Financiera: (numeral:13) _____
- Oficina Asesora Jurídica: (revisión)_____