Análisis de Riesgos y Diseño de Controles de Seguridad para una Institución de Educación Superior

MY. Fabián Esteban Cano Jaime
MY. Arturo Alexander Mahecha Virguez
MY. Manuel Ricardo Rey Ríos
CC. Rubén Contreras Caballero

Escuela Superior de Guerra
Cursos de Estado Mayor 2025
Gestión de Riesgos Cibernéticos (MAECI)
Jaider Ospina Navas

Bogotá D.C.
22 de Febrero del 2025

Introducción

La propuesta de este proyecto es llevar a cabo una evaluación de los riesgos cibernéticos en una institución educativa con varias sucursales y presencia nacional, teniendo como principal enfoque que cuenta con una plataforma de LMS, sistemas de base de datos académicos y administrativos, adicionalmente una plataforma de investigación que contienen información sensible como calificaciones, proyectos de investigación en desarrollo, datos personales de estudiantes y empleados.

Los enfoques y riesgos identificados se abordarán mediante una metodología estructurada que se inicia con un diagnóstico inicial para identificar los activos críticos dentro de la institución y proporcionar una evaluación de la infraestructura existente, luego se basa en herramientas ampliamente reconocidas, como la STRIDE y el NIST Cybersecurity Framework, para evaluar amenazas potenciales y clasificar los riesgos según su probabilidad e impacto potencial (Kohnfelder & Garg, desarrolladores del modelo STRIDE; Instituto Nacional de Estándares y Tecnología [NIST], 2020). Además, se plantearán recomendaciones mediante la aplicación de la norma ISO 27001, que establece requisitos para un sistema de gestión de seguridad de la información (SGSI) enfocado en la protección de activos críticos y el uso de medios de control adecuados (Organización Internacional de Normalización [ISO], 2013).

Finalmente, la implementación de salida del proyecto concluirá con un informe detallado sobre los principios riesgos reales dentro la institución educativa y un plan integral que combina controles técnicos adecuados con programas educativos dirigidos a toda la comunidad universitaria. Junto con el componente técnico-educativo mencionado anteriormente, también será crucial establecer políticas internas claras sobre uso seguro de correos electrónicos y dispositivos móviles conectados a redes universitarias, todo esto monitoreado constantemente por medio de auditorías periódicas para verificar las políticas establecidas.

1. Descripción del escenario

La institución educativa a evaluar maneja una cantidad considerable de información confidencial y sensible, incluyendo datos personales de estudiantes, registros académicos, información financiera, investigaciones científicas y de propiedad intelectual. Aunque ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger esta información, aún existen debilidades que la exponen a diversos riesgos cibernéticos.

Contexto Institucional

- **Población estudiantil**: Entre 3000 a 10000 estudiantes matriculados.
- **Personal académico**: 500 profesores.
- **Personal administrativo**: 100 empleados.
- **Sistemas implementados**: LMS (Learning Management Systems), bases de datos académicas/administrativas y plataformas de investigación.

Riesgos Identificados

- **Ataques cibernéticos**: Phishing, malware y ransomware son amenazas comunes que pueden interrumpir las operaciones diarias e incluso comprometer bases de datos sensibles.
- **Acceso no autorizado**: Debilidades en autenticación y control del acceso pueden permitir intrusiones maliciosas.
- **Vulnerabilidades internas**: La falta de conciencia sobre ciberseguridad entre el personal de docentes, administrativos y los estudiantes aumenta significativamente los riesgos internos.

Metodología del Análisis de Riegos y Diseño de Controles

- Fase 1: Análisis Preliminar

- Identificar activos críticos como bases de datos sensibles y sistemas LMS.
- Realizar un diagnóstico inicial sobre la infraestructura existente.

- Fase 2: Evaluación del Riesgo

Utilizar herramientas reconocidas como el modelo STRIDE o NIST Cybersecurity Framework para evaluar amenazas potenciales. Clasificar los riesgos según su probabilidad e

impacto potencial (Kohnfelder & Garg; National Institute of Standards and Technology [NIST], 2020).

- Fase 3: Diseño e Implementación Controles

- Implementar medidas técnicas.
- Políticas Internas

- Fase 4: Monitoreo Continuo

Auditorías periódicas para verificar cumplimiento con las políticas establecidas. Revisión continua por parte del equipo directivo (revisión gerencial).

2. Análisis de riesgos

El seguimiento con el análisis, que tiene como objetivo evaluar y comprender el panorama de riesgos y amenazas cibernéticas a los que se exponen la institución de educación superior, se realizó a través de una matriz de evaluación, con el fin de facilitar la identificación de las principales debilidades en la seguridad de la información aplicando el modelo STRIDE para categorizar las amenazas, así como referencias a MITRE ATT&CK, ISO 27001 e ISO 27001:2022 “Anexo A” para alinear las medidas de mitigación, con los estándares y las prácticas existentes. El resultado de este análisis proporciona una serie de datos que permite la toma de decisiones y la implementación de controles de seguridad efectivos que protejan los activos críticos de la universidad.

MODELO STRIDE	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	MITIGACION
SPOOFING	ADMINISTRACION DE LA NUBE	ALTA	MEDIA	ALTA	Gestión de cuentas privilegiadas
TAMPERING		ALTA	MEDIA	ALTA	
REPUDIATION		MEDIA	BAJA	MEDIA	
INFORMATION DISCLOSURE		ALTA	ALTA	ALTA	
DENIAL		ALTA	MEDIA	ALTA	
ELEVATION OF PRIVILIEGE		ALTA	MEDIA	ALTA	
MODELO STRIDE	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	MITIGACION
SPOOFING	EMPLEO MODULOS COMPARTIDOS	ALTA	MEDIA	ALTA	Identifique y bloquee el software potencialmente malicioso ejecutado a través de esta técnica mediante el uso de herramientas de control de aplicaciones capaces de evitar que se carguen módulos desconocidos.
TAMPERING		ALTA	MEDIA	ALTA	
REPUDIATION		MEDIA	BAJA	MEDIA	
INFORMATION DISCLOSURE		ALTA	ALTA	ALTA	
DENIAL		MEDIA	MEDIA	MEDIA	
ELEVATION OF PRIVILIEGE		ALTA	ALTA	ALTA	
MODELO STRIDE	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	MITIGACION
SPOOFING	INFRAESTRUCTURA TECNOLÓGICA DESACTUALIZADA	ALTA	ALTA	ALTA	Siempre que sea posible, considere la posibilidad de restringir el acceso y el uso de las funciones sin servidor. Por ejemplo, las directivas de acceso condicional se pueden aplicar a los usuarios que intentan crear flujos de trabajo en Microsoft Power Automate.
TAMPERING		ALTA	ALTA	ALTA	
REPUDIATION		MEDIA	MEDIA	MEDIA	
INFORMATION DISCLOSURE		ALTA	ALTA	ALTA	
DENIAL		MEDIA	ALTA	ALTA	
ELEVATION OF PRIVILIEGE		ALTA	ALTA	ALTA	

Figura N-1: Matriz de Evaluación Modelo STRIDE

Analís la Matriz de Vulnerabilidades STRIDE

- SPOOFING (Suplantación)

- **Administración de la Nube:** Una mala gestión de las cuentas privilegiadas sobre la nube, como la falta de autenticación multifactor (MFA) o contraseñas débiles, permite la suplantación de identidad, en el ataque de MITRE ATT&CK: el T1078, Cuentas válidas, y en el acceso imposible se realiza utilizando los recursos y datos de sensibilidad. Para mitigar, la administración se orienta a las cuentas privilegiadas y la autenticación multifactor Alineado con ISO 27001, A.9.2.2 y Proteger la identidad – ISO 27001:2022 Anexo A, A.5.3.
- **Empleo de Módulos Compartidos:** La ejecución de software malicioso a través del empleo de módulos compartidos (MITRE ATT&CK: T1189, Drive-by Compromise) compromete la integración de la información. La mitigación implica identificar y bloquear software potencialmente malicioso, alineados con la protección contra software malicioso de ISO 27001 (A.12.4.2) y la gestión de vulnerabilidades técnicas de ISO 27001:2022 Anexo A (A.8.6).
- **Infraestructura Tecnológica Desactualizada:** La falta de actualizaciones y parches para la infraestructura tecnológica otorgan oportunidades a los atacantes que explotan las vulnerabilidades conocidas (NIST, 2020) (MITRE ATT&CK: T1190, Exploit Public-Facing Application). La propuesta de mitigación es restringir el acceso a las funciones y limitar el acceso a los alcances OAuth de alto riesgo, lo que coincide con ISO 27001 Technical Vulnerability Management A.12.6.1, A.12.6.2 e ISO 27001:2022 Information Access Control annex A A.8.29.

- TAMPERING (Manipulación)

- **Alteración de Registros Académicos:** El acceso no autorizado a bases de datos conduce a la alteración no autorizada de registros académicos. Esto envía a la universidad a problemas mayores con consecuencias legales y reputacionales. La manipulación de datos se puede mitigar centrando la solución en la implementación de controles de integración de datos como las sumas de verificación (MITRE ATT&CK: T1565, Manipulación de datos). La mitigación se centra en la implementación de controles de integración de datos (sumas de verificación, hashes), audiencia de cambios en la base de datos y validación de entradas, alineados con la política de desarrollo de sistemas seguros

de ISO 27001 (A.14.1.1), la gestión de cambios de ISO 27001 (A.12.1.2) y la protección contra software malicioso de ISO 27001:2022 Anexo A (A.8.2).

- REPUDIATION (Repudio)

- **Negación de Transacciones Financieras:** La falta de auditoría y registros, así como la adulteración de los registros, pueden conducir a la negación de transacciones financieras (pagos de matrix), lo que daría como resultado conflictos financieros (MITRE ATT&CK: T1114, colección de correo electrónico; T1070, eliminación de indicadores). Las medidas de mitigación incluyen la necesidad de registros de auditoría centralizados detallados, firma digital de transacciones críticas y controles de acceso a registros, alineados con el registro de eventos de ISO 27001 (A.12.4.1), los controles de auditoría de los sistemas de información de ISO 27001 (A.12.7.1) y la información sobre amenazas a la inteligencia de ISO 27001:2022 Anexo A (A.5.14).

- INFORMATION DISCLOSURE (Divulgación de Información)

- **Exposición de Datos Personales de Estudiantes:** El acceso no autorizado a bases de datos, la falta de cifrado y las políticas de privacidad deficientes pueden resultar en la exposición de datos personales de estudiantes (nombre, dirección, histórico académico), lo que viola la privacidad y puede generar demandas legales (MITRE ATT&CK: T1081, Credenciales en archivos; T1555, Credenciales de tiendas de contraseñas). La mitigación se centra en el cifrado de datos en reposo y en tránsito, controles de acceso estrictos (RBAC) y políticas de privacidad claras y cumplimiento del RGPD/LOPD, alineados con la política de control de acceso de ISO 27001 (A.9.4.1), la gestión de activos de ISO 27001 (A.8.2.3) y el control de acceso a la información de ISO 27001:2022 Anexo A (A.8.29).

- DENIAL (Denegación de Servicio)

- **Interrupción de Servicios Académicos:** Ataques DDoS, fallos en la infraestructura y el consumo excesivo de recursos pueden resultar en la interrupción de servicios académicos (LMS, bases de datos), afectando la disponibilidad de los recursos educativos y la producción de estudiantes y profesionales (MITRE ATT&CK: T1498, Red Denegación de Servicio; T1499, Denegación de Servicio de Punto Final). La mitigación implica la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS), equilibrio de carga, planos de contingencia y recuperación ante desastres, y mitigación

DDoS en la nube, alineados con la planificación de la continuidad del negocio de ISO 27001 (A.17.1.1), la implementación de la continuidad del negocio de ISO 27001 (A.17.1.2) y el uso de los servicios en la nube de ISO 27001:2022 Anexo A (A.5.30).

- ELEVATION OF PRIVILIEGE (Escalada de Privilegios)

- **Acceso Administrativo No Autorizado:** La explotación de vulnerabilidades, las contraseñas débiles y los errores de configuración pueden permitir a los atacantes obtener privilegios administrativos no autorizados, compromiso la integración, confidencialidad y disponibilidad de la información (MITRE ATT&CK: T1068, Exploit OS for Privilege Escalation; T1548, Bypass Control de cuentas de usuario). La mitigación implica la implementación de autenticación multifactor (MFA), gestión de contraseñas robusta (políticas de complejidad, rotación), principio de mínimo privilegio, revisión periódica de privilegios y endurecimiento de sistemas, alineados con la gestación de acceso de usuarios de ISO 27001 (A.9.2.2), la seguridad del acceso a la red de ISO 27001 (A.9.1.2) y el control de acceso físico de ISO 27001:2022 Anexo A (A.5.15).

Principales Vulnerabilidades y Amenazas Identificadas Acuerdo Matriz de Vulnerabilidades Usando el Modelo STRIDE

- **Gestión de la Nube:** La gestión inadecuada de cuantas privilegiadas en la noche sigue siendo una vulnerabilidad crítica.
- **Empleo de Módulos Compartidos:** La ejecución de software malicioso a viajes de módulos compartidos representa una amenaza importante.
- **Infraestructura Tecnológica Desactualizada:** La falta de actualizaciones y parches.

3. Diseño de controles de seguridad

El diseño de controles de seguridad tiene como objetivo mitigar los riesgos y amenazas cibernéticas identificadas en la institución educativa, se utilizó la información extraída análisis de riesgos, basado en la matriz de vulnerabilidades la cual facilitó la identificación de las principales debilidades en la seguridad de la información. Para esto, se aplica el modelo STRIDE para categorizar las amenazas, así como referencias a MITRE ATT&CK, ISO 27001 e ISO 27001:2022 “Anexo A” para alinear los controles con los estándares y las mejores prácticas de la industria.

El diseño de controles se clasifica en técnicos, administrativos y físicos, teniendo como objetivo proporcionar un conjunto de controles de seguridad efectivos que protejan los activos críticos de la universidad y garantizar la continuidad de sus operaciones.

- Diseño de Controles de Seguridad

- **SPOOFING (Suplantación)**

  Riesgo: Gestión inadecuada de cuentas privilegiadas en la nube, empleo de módulos compartidos, infraestructura tecnológica desactualizada.

  Impacto: La suplantación puede tener consecuencias graves para la institución educativa, incluido la pérdida de datos sensibles, interrupción de servicios críticos como plataformas de gestión del aprendizaje (LMS) y sistemas administrativos, costos financieros significativos y daños a la reputación.

  - Controles Técnicos:
    - A.5.3 Gestión de la identidad: Implementar autenticación multifactor (MFA) para todas las citas privilegiadas.
    - A.8.6 Gestión de vulnerabilidades técnicas: Utilizar herramientas de control de aplicaciones para identificar y bloquear software malicioso.
    - A.8.29 Control de acceso a la información: Configurar listas de control de acceso (ACL) y segmentación de red para limitar el acceso a funciones sin servicio y alcances OAuth de alto riesgo. Implementar soluciones de gestión de identidades y accesos (IAM).
  - Controles Administrativos:
    - A.5.1 Política de seguridad de la información: Establecer una política clara sobre la gestión de cuentas privilegiadas y el uso de módulos compartidos, requiriendo revisiones periódicas.
    - A.8.10 Gestión de la información: Definir procedimientos para la gestión y el control de la información almacenada en la nube, asegurando su integridad y confidencialidad.
  - Controles Físicos:
    - A.5.15 Control de acceso físico: Restringir el acceso físico a los servidores y centros de datos que alojan la infraestructura en la nube.

- **TAMPERING** (Manipulación)

  Riesgo: Alteración de registros académicos.

Impacto: La manipulación de registros académicos puede tener consecuencias significativas para la institución educativa, como el compromiso de la integrad académica, consecuencias legales y regulatorias, pérdida de confianza en la institución.

- Controles Técnicos:
    - A.8.2 Protección contra software malicioso: Implementar soluciones de detección de intrusiones (IDS) y prevención de intrusiones (IPS) para detectar actividades sospechosas en las bases de datos.
    - A.8.8 Gestión de la configuración: Utilizar sumas de verificación y hashes para verificar la integridad de los datos, almacenados y las bases de datos.
- Controles Administrativos:
    - A.8.12 Gestión de cambios: Establecer un procedimiento de gestión de cambios para controlar las modificaciones en la base de datos y asegurar que sean autorizadas y registradas.
    - A.14.2.1 Política de seguridad en el desarrollo y la adquisición: Implementar políticas de seguridad en el desarrollo y la adquisición de sistemas que accedieron a las bases de datos, asegurando que se siguen prácticas seguras de codificación.
- Controles Físicos:
    - A.5.15 Control de acceso físico: Restringir el acceso físico a los servidores de bases de datos y asegurar que están ubicados en áreas seguras.

- **REPUDIATION** (Repudio)

  Riesgo: Negación de transacciones financieras.

  Impacto: La negación de transacciones financieras puede tener diversas consecuencias significativas para la institución educativa, incluido costos de remediación e interrupción de las operaciones dentro de la institución.

  - Controles Técnicos:
    - A.5.14 Información sobre amenazas a la inteligencia: Implementar registros de auditoría detallados y centralizados para todas las transacciones financieras, incluido la identidad del usuario, la fecha, la hora y los detalles de la transacción.
    - A.8.34 Registro y seguimiento: Utilizar firmas digitales para autenticar las transacciones críticas y asegurar que no puedo ser repudiadas.
  - Controles Administrativos:
    - A.12.4 Registro de eventos: Establecer procedimientos para la gestión y el análisis de los registros de auditoría, asegurando que sean revisados según.

        - A.12.1 Gestión de la cadena de suministro de servicios de información: Implementar políticas para la gestión de la cadena de suministro de servicios de información, garantizando que los probadores de servicios cambien cumplan con los requisitos de seguridad.
    - Controles Físicos:
        - A.5.15 Control de acceso físico: Restringir el acceso físico a los servidores que procesan las transacciones financieras y asegurar que están ubicados en estas áreas.

- **INFORMATION DISCLOSURE (Divulgación de Información)**

  Riesgo: Exposición no autorizada de información sensata, como datos personales de estudiantes y empleados, clasificaciones y proyectos de investigación.

  Impacto: La divulgación no autorizada puede comprometer la privacidad de los datos personales, lo que puede llegar a consecuencias legales y sanciones por violaciones a regulaciones de protección de datos.

    - Controles Técnicos:
        - Implementar cifrado para datos sensibles en reposo y en tránsito.
        - Utilizar herramientas de gestión de acceso e identidades (IAM) para controlar la atención de acceso a la información.
        - Monitorear y registrar accede a una información sensata para detectar accesos no autorizados.
    - Controles Administrativos:
        - Establecer políticas claras sobre el mango y protección de la información sensata.
        - Realizar capacidades periódicas sobre seguridad de la información para el personal.
    - Controles Físicos:
        - Restringir el acceso físico a áreas donde se maneje información sensible medio controles de acceso.
        - Implementar medidas de seguridad en las instalaciones, como cajas y personal de seguridad.

- **DENIAL (Denegación de Servicio)**

  Riesgo: Ataques que buscan interrumpir el acceso a servicios críticos, como plataformas LMS y sistemas administrativos.

Impacto: La interrupción de servicios puede afectar gravemente la capacidad operativa, impidiendo que estudiantes y personal accedieron a servicios esenciales.

- Controles Técnicos:
    - Implementar soluciones de mitigación DDoS (Negación de Servicio Distribuida).
    - Utilizar equilibradores de carga para distribuir el tráfico y evitar sobrecargas en los servidores.
    - Monitorear el tráfico en tiempo real para detectar patrones anómalos que pueden indicar un ataque.
- Controles Administrativos:
    - Desarrollar un plan de respuesta ante incidentes que incluyen procedimientos específicos para ataques DDoS.
    - Realizar simulacros periódicos para preparar al personal ante posibles incidentes.
    - Mantener actualizados los planos de continuidad del negocio.
- Controles Físicos:
    - Asegurar que las instalaciones donde se encuentran los servidores tengan medidas físicas adecuadas para prevenir accesos no autorizados que pueden facilitar ataques.

- **ELEVATION OF PRIVILIEGE (Elevación del Privilegio)**

  Riesgo: Acceso no autorizado a recursos mediante el acervo de vulnerabilidades en sistemas o aplicaciones.

  Impacto: Los atacantes pueden obtener acceso a una información crítica o realizar acciones no autorizadas dentro del sistema, comprometiendo datos sensibles.

  - Controles Técnicos:
    - Implementar políticas estrictas sobre el principio del menor privilegio (Principio de Privilegio Menor) para limitar los accesos innecesarios.
    - Utilizar autenticación multifactor (MFA) para cuentas con privilegios elevados.
    - Realizar auditorías regulares sobre los permisos asignados a usuarios.
  - Controles Administrativos:
    - Establecer procedimientos claros para la creación, modificación y eliminación de cuentas con privilegios elevados.

- Capacitar al personal sobre las mejores prácticas en seguridad informática y gestación de accesos.
- Realizar revisiones periódicas del acceso a sistemas críticos.

- Controles Físicos:
  - Restringir el acceso físico a servidores críticos o áreas donde se manejen datos sensibles mediante controles físicos robustos (tarjetas magnéticas, biometría).

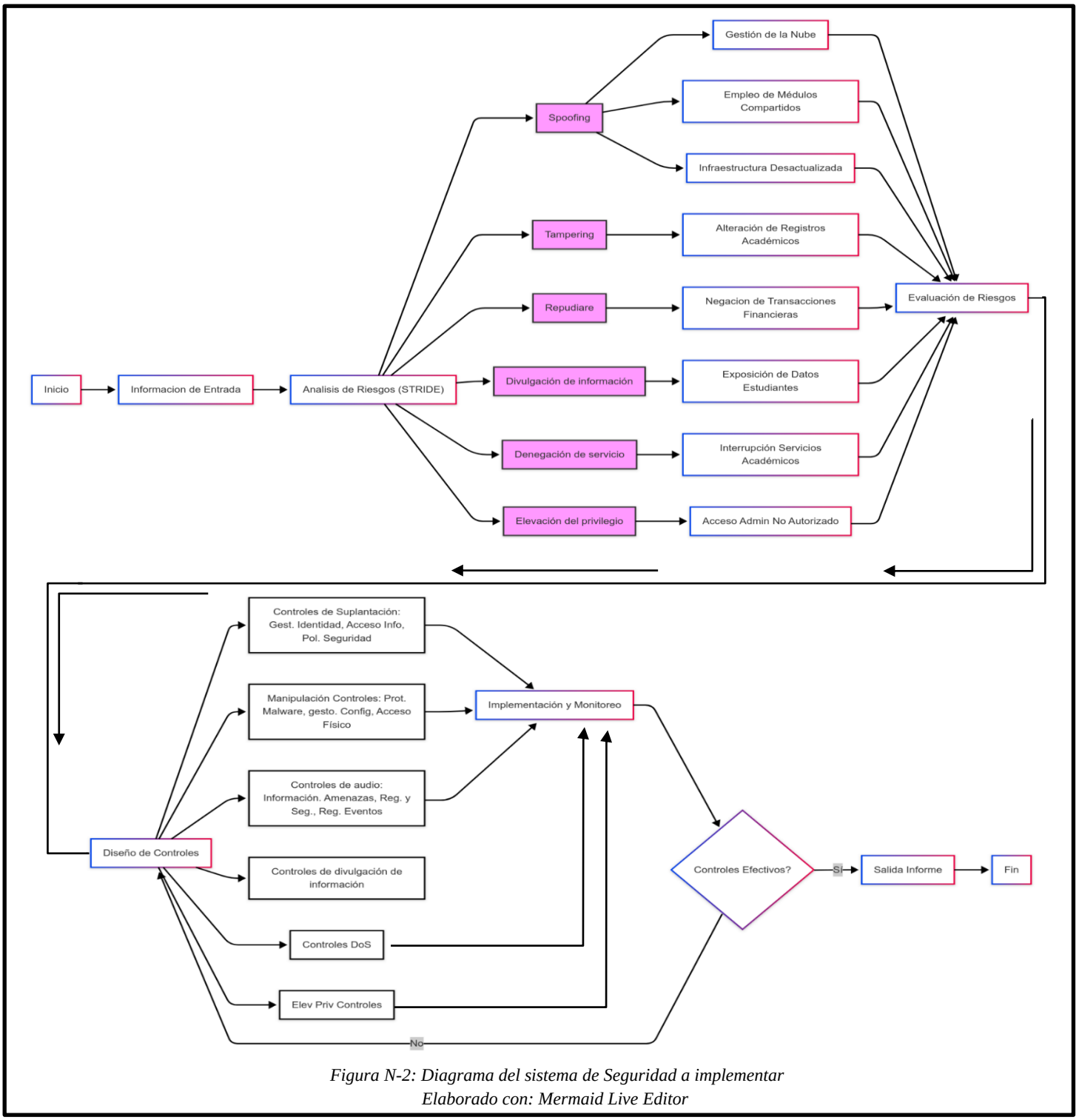

Figura N-2: Diagrama del sistema de Seguridad a implementar
Elaborado con: Mermaid Live Editor

4- Conclusiones y recomendaciones

A pesar de la implementación de un Sistema de Gestación de Seguridad de la Información (SGSI), la institución educativa aun presenta vulnerabilidades significativas en áreas críticas como la gestación de la noche, el uso de módulos compartidos y la infraestructura tecnológica desactualizada. Estas vulnerabilidades representan un riesgo real de suplantación, ejecución de código malicioso y explotación de sistemas.

La inadecuada gestión de cuentas privilegiadas y la falta de autenticación multifactor (MFA) en la nube exponen a la institución a un alto riesgo de acceso no autorizado y robo de información. Es crucial reforzar los controles de identidad y acceso, alineándolos con las mejores prácticas y los estándares internacionales.

La alteración no autorizada de registros académicos es una amenaza seria que puede tener tumbas consecuencias legales y reputacionales. La implementación de controles de integración de datos, como sumas de verificación y hashes, es fundamental para garantizar la confianza de la información.

La falta de auditoría y registros adecuados en las transacciones financieras aumenta el riesgo de repudio y posibles pérdidas económicas. Es necesario implementar registros de auditoría detallados y firmas digitales para asegurar la no refutación de las transacciones y proteger los activos financieros de la institución.

Recomendaciones:

Implementar autenticación multifactor (MFA) en todas las cuentas de usuario, especialmente en las cuentas administrativas y las que tienen acceso a una información sensata. Esta medida mitigará significativamente el riesgo de acceso no autorizado y suplantación de identidad.

Establecer un programa formal de gestión de vulnerabilidades que incluye la identificación, evaluación y mitigación de las vulnerabilidades en la infraestructura tecnológica. Esto garantizará que los sistemas estén actualizados y protegidos contra las amenazas conocidas.

Desarrollo políticas de seguridad integrales que abarquen todos los aspectos de la seguridad de la información, incluido la gestión de identidades y accesos, la protección contra software malicioso, la gestión de la configuración, la seguridad en el desarrollo de sistemas, la

gestión de la cadena de suministro y la respuesta a incidentes. Estas políticas deben ser comunicaciones y aplicaciones de gestión efectiva en toda la institución.

Realizar pruebas de penetración y auditorías de seguridad periódicas para identificar y corregir las vulnerabilidades en los sistemas y las aplicaciones. Estas pruebas deben ser realizadas por profesionales capacitados y deben cubrir todos los aspectos de la seguridad de la información.

Al implementar estas conclusiones y recomendaciones, la institución educativa está en una mejor posición para proteger sus activos críticos, garantizar la continuidad de sus operaciones y cumplir con los requisitos legales y reguladores.

5- Lista de referencias

- Kohnfelder & Garg (desarrolladores del modelo STRIDE). Consultado en https://www.csirt-epn.edu.ec/como-tener/142-herramienta-de-modelado-de-amenazas-stride
- Instituto Nacional de Estándares y Tecnología [NIST]. (2020). Marco de ciberseguridad. Recuperado desde https://www.nist.gov/cyberframework
- Organización Internacional de Normalización [ISO]. (2013). ISO/IEC 27001:2013. Recuperado desde https://www.iso.org/standard/54534.html
- Kohnfelder & Garg (desarrolladores del modelo STRIDE). Consultado en https://www.csirt-epn.edu.ec/como-tener/142-herramienta-de-modelado-de-amenazas-stride
- Instituto Nacional de Estándares y Tecnología [NIST]. (2020). Marco de ciberseguridad. Recuperado desde https://www.nist.gov/cyberframework
- Conklin, W. A. y Blanco, GB. (2021). Principios de seguridad informática: CompTIA Security+ y más allá. Educación McGraw-Hill.
- Organización Internacional de Normalización [ISO]. (2013). ISO/IEC 27001:2013. Obtenido de https://www.iso.org/standard/54534.html
- Organización Internacional de Normalización [ISO]. (2022). ISO/IEC 27001:2022. Obtenido de https://www.iso.org/standard/81580.html
- Kohnfelder & Garg (desarrolladores del modelo STRIDE). Consultado en https://www.csirt-epn.edu.ec/como-tener/142-herramienta-de-modelado-de-amenazas-stride
- Corporación MITRE. (2024). Marco MITRE ATT&CK. Obtenido de https://attack.mitre.org/
- Instituto Nacional de Estándares y Tecnología [NIST]. (2020). Marco de ciberseguridad. Obtenido de https://www.nist.gov/cyberframework
- Perplexity. (s.f.). Perplexity AI $$Modelo de lenguaje]. Recuperado de https://www.perplexity.ai/
- Mermaid. (s.f.). Mermaid Live Editor $$Herramienta de diagramación]. Recuperado de https://mermaid.live/