

GESTIÓN DE RIESGOS CIBERNÉTICOS

**ANÁLISIS DE RIESGOS Y DISEÑO DE CONTROLES
DE SEGURIDAD**





ESDEG

INTEGRANTES



**MY MANUEL
REY**



CC RUBEN CONTRERAS



MY ARTURO MAHECHA



MY FABIAN CANO



INTRODUCCIÓN



Evaluación de riesgos cibernéticos en una institución de educación superior con múltiples sucursales.



Plataformas: LMS, bases de datos académicas y administrativas, plataformas de investigación.



Aplicación de estándares como STRIDE, NIST y ISO 27001.



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, aun existen debilidades que la exponen a diversos riesgos cibernéticos.



- > **Sistemas implementados: LMS (Learning Management Systems),**
- > **Población estudiantil: 10,000 estudiantes**
- > **•Personal académico: 500 profesores**
- > **Personal administrativo: 100 empleados**



ESDEG

RIESGOS IDENTIFICADOS



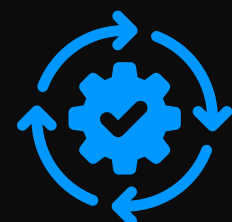
Ataques cibernéticos

Phishing, malware, ransomware



Acceso no autorizado

Débiles controles de autenticación



Interrupción de servicios

Ataques DDoS y fallos de infraestructura



Vulnerabilidades internas

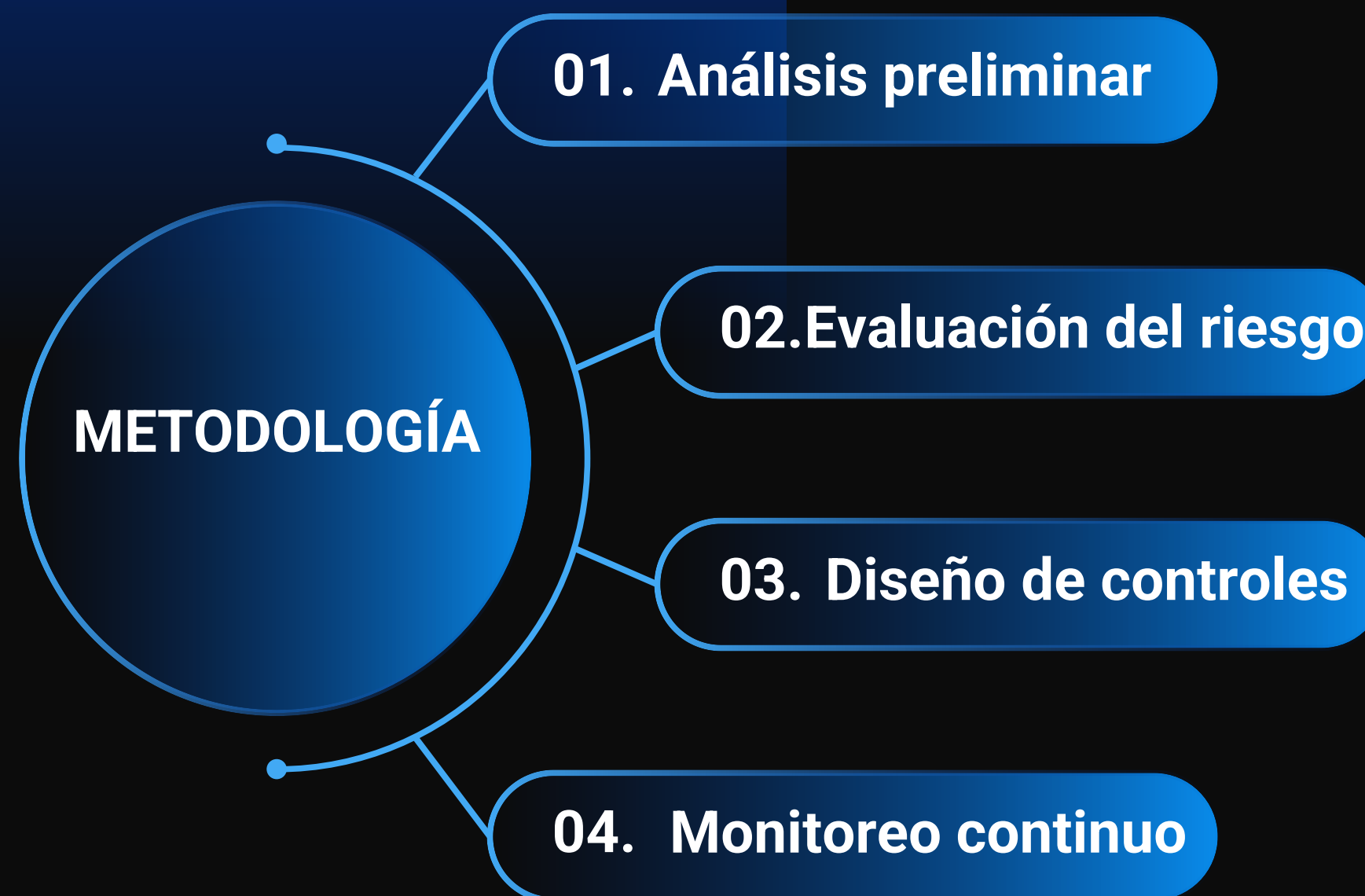
Falta de conciencia en ciberseguridad





METODOLOGÍA

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, aun existen debilidades que la exponen a diversos riesgos cibernéticos.





ESDEG

ANÁLISIS DE RIESGOS (MATRIZ STRIDE)



SPOOFING



TAMPERING



REPUDIATION



**INFORMATION
DISCLOSURE**



**DENIAL OF
SERVICE**



**ELEVATION OF
PRIVILEGE**

Modelo de amenazas para identificar y clasificar
riesgos en sistemas de información

DISEÑO DE CONTROLES DE SEGURIDAD



ESDEG

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 PRIVILEGE		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 PRIVILEGE		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 PRIVILEGE		ALTA	ALTA	ALTA	

VULNERABILIDADES Y AMENAZAS IDENTIFICADAS MODELO STRIDE



ESDEG



GESTIÓN DE LA NUBE

La gestión inadecuada de cuentas privilegiadas en la nube sigue siendo una vulnerabilidad crítica.



EMPLEO DE MÓDULOS COMPARTIDOS

La ejecución de software malicioso a través de viajes de módulos compartidos representa una amenaza importante.



INFRAESTRUCTURA TECNOLÓGICA DESACTUALIZADA

La falta de actualizaciones y parches.



ESDEG

DISEÑO DE CONTROLES DE SEGURIDAD



CONTROLES TÉCNICOS

MFA, cifrado de
datos, IDS/IPS



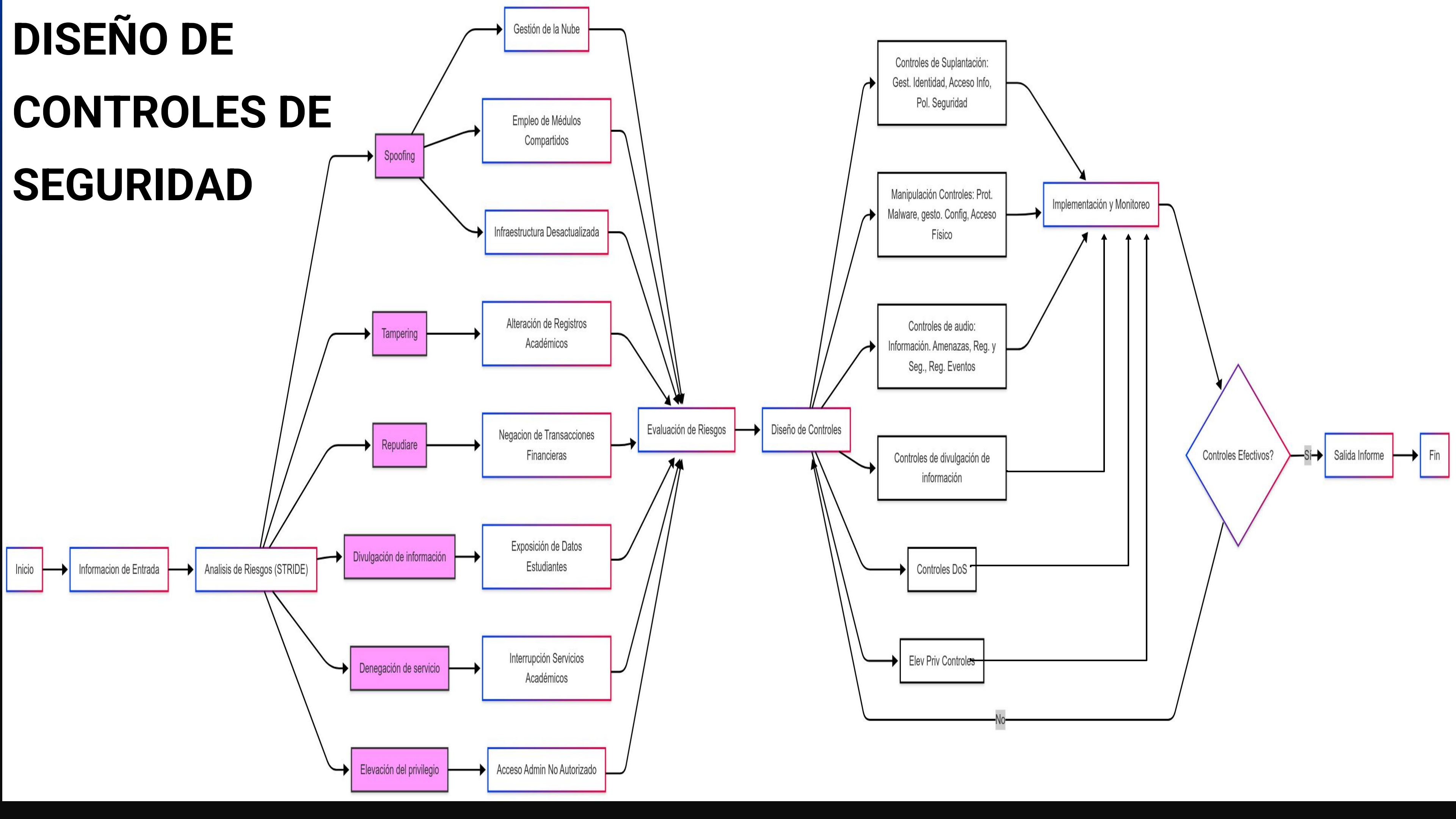
CONTROLES ADMINISTRATIVOS

Políticas internas,
auditorías regulares



CONTROLES FÍSICOS

Restricción de
acceso a servidores y
centros de datos.





ESDEG



CONCLUSIONES



Implementación de autenticación multifactor (MFA)



Gestión y mitigación de vulnerabilidades



Desarrollo de políticas de seguridad



Pruebas de penetración y auditorías de seguridad regulares.



ESDEG



GRACIAS

