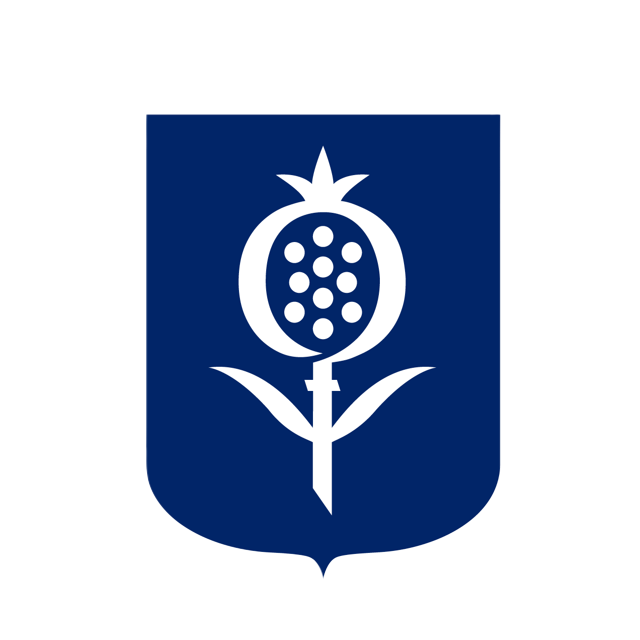
**TALLER 5 – Evaluación de seguridad con STRIDE**



**Julián Pinilla**

**Cristian Soto**

**Sergio Socha**

**Nicolás Rodriguez**

**Descripción general del trabajo**

Este taller tuvo como propósito aplicar la metodología STRIDE para identificar riesgos de seguridad en sistemas de información. Primero se trabajó un caso base (EdukIT, una plataforma educativa en línea) y después se trasladó el ejercicio a un cliente real, que corresponde a procesos críticos de posgrados en la Universidad de La Sabana.

El análisis buscó detectar amenazas como suplantación, fuga de información o alteración de registros, y proponer medidas concretas de mitigación que ayuden a proteger la información y asegurar la continuidad de los procesos.

**Proceso de desarrollo**

Comenzamos revisando el caso base de EdukIT. De los distintos flujos posibles, elegimos el de acceso de estudiantes a cursos y materiales porque involucra tanto autenticación como control de información académica. Sobre este flujo aplicamos STRIDE, construimos la tabla de amenazas y propusimos medidas como autenticación multifactor, cifrado y balanceo de carga.

Después pasamos al cliente real. Analizamos tres procesos que hoy en día tienen puntos débiles:

1. Carga de documentos de admisión (cédula, diplomas, certificados).
2. Sistema de facturación y notificación automática.
3. Consolidación de información regulatoria (SNIES).

Para cada proceso se construyó una tabla STRIDE con amenazas, impactos, nivel de riesgo y mitigaciones. También armamos diagramas para visualizar los resultados.

**Análisis del modelo propuesto**

El modelo se organizó en tablas STRIDE por proceso, complementadas con diagramas que sintetizan resultados.

El análisis respondió a tres problemas concretos: validación de documentos cargados por aspirantes, automatización y seguridad en el envío de facturas, e integridad y trazabilidad en la información regulatoria del SNIES.

Se asumió que los procesos actuales son manuales o semiautomatizados. También que la universidad debe cumplir con normativas nacionales (Ley 1581 de 2012) y buenas prácticas internacionales (GDPR, PCI DSS, ISO 27001). Se priorizaron amenazas de alto impacto sobre la disponibilidad, confidencialidad e integridad de la información.

En la parte de documentos de admisión vimos que el problema es bastante común. Muchos aspirantes suben cualquier cosa, incluso un archivo vacío, con tal de poder seguir en el formulario. Eso genera doble trabajo porque después alguien del área de admisiones tiene que abrir archivo por archivo. El riesgo está en que se cuele información falsa o que se pierdan datos personales. Para evitarlo lo lógico sería que el sistema mismo bloquee los archivos que no cumplen y que la validación sea inmediata, con algo más fuerte como firmas digitales o biometría.

El proceso de facturación también dio mucho de qué hablar. La idea es que sea automático, pero en la práctica no lo es. Los estudiantes nuevos casi nunca entran a revisar, así que al final alguien tiene que enviar recibos manualmente. Eso no solo retrasa todo, también abre espacio a correos falsos con facturas manipuladas. Lo que se planteó fue usar PDFs firmados digitalmente, correos autenticados y un bot que se encargue de los envíos. No es nada del otro mundo, pero haría la diferencia.

Sobre el tema del SNIES, lo que encontramos es que buena parte de la información se sigue manejando en Excel. Esto trae un problema: no hay trazabilidad. Si alguien cambia un dato, no queda claro quién fue ni cuándo lo hizo. Esto puede terminar en errores en reportes oficiales o en que la universidad quede mal frente al gobierno. La alternativa es pasar a una base de datos con versiones, respaldos automáticos y registros de auditoría. Eso asegura que cualquier cambio quede registrado.

En los tres casos se ve que los problemas ya están ahí y afectan el día a día. No es inventado. Lo positivo es que hay soluciones relativamente simples de aplicar, solo falta dar el paso.

**Diagrama final entregado**

Se construyeron 3 diagramas STRIDE:

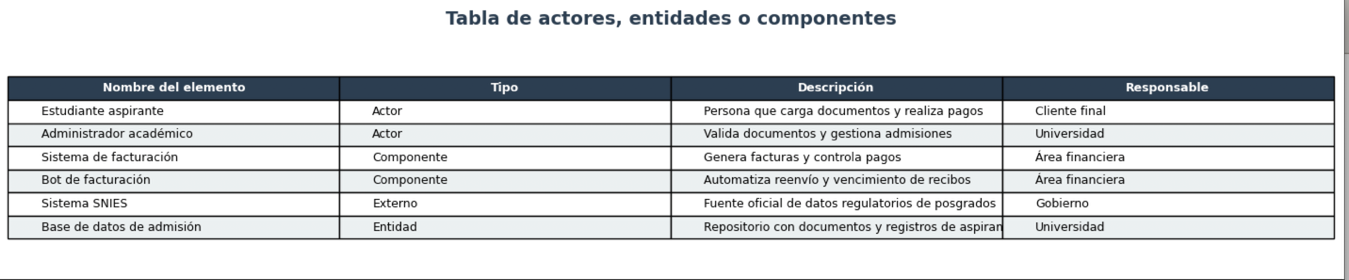
* Proceso 1: Gestión de documentos de admisión.
* Proceso 2: Sistema de facturación automatizado.
* Proceso 3: Información regulatoria (SNIES).







**Tabla de actores, entidades o componentes**



**Investigación complementaria**

Se revisaron marcos de referencia como OWASP Top 10 e ISO/IEC 27001, que destacan la importancia de la autenticación multifactor, el cifrado en tránsito y en reposo, el control de accesos basado en roles y la trazabilidad con auditorías y logs inmutables.

También se consideraron normativas relevantes:

* Ley 1581 de 2012 en Colombia sobre protección de datos personales.
* GDPR en Europa como referente de privacidad y transparencia.
* PCI DSS para la seguridad en pagos electrónicos.

Estas prácticas se alinearon con las propuestas de mitigación en los tres procesos analizados, garantizando confidencialidad, integridad y disponibilidad de la información.

**Referencias**

* OWASP Foundation. *OWASP Top 10 – Security Risks*.
* ISO/IEC 27001:2022. *Information Security Management Systems*.
* PCI DSS v4.0. *Payment Card Industry Data Security Standard*.
* NIST Cybersecurity Framework (CSF).
* Ley 1581 de 2012 (Colombia).