Nombre de la TIA:	**Taller 1**: Análisis y Evaluación de riesgos de la seguridad de software mediante la matriz de riesgos
Caso de estudio de la TIA:	Universidad La NeuRona
Instrucciones:	**PROPÓSITO:** Esta TIA tiene como propósito que usted aplique todo lo estudiado en la Unidad 1 acerca del análisis de los riesgos a la solución de un caso de estudio y evaluación de los mismos. Identificando activos de información y amenazas a través de una matriz de riesgos en el contexto del caso de estudio propuesto. **ORIENTACIONES:** Este taller está relacionado con el caso de estudio "*Universidad La NeuRona"*, en la cual se debe elaborar una matriz de riesgos de acuerdo a lo solicitado por el decano para contemplar la seguridad de los módulos o interfaces Web del Sistema Académico y Gestión (SIAG) y para ello en forma grupal se debe realizar lo siguiente: 1. Contextualización de la seguridad de acuerdo a las normas de seguridad 2. Identificación de activos de información 3. Identificación de amenazas 4. Evaluación de riesgos 5. Construcción de la matriz de riesgos Desarrolle cada uno de los puntos solicitados en los apartados dispuestos para ello a continuación de este cuadro en el presente documento. *(**Aclaración**: **Si va a entregar un documento adicional, relacione el nombre del documento**. Por ejemplo: anexo documento Word, Excel, o Power Point, entre otros, llamado: **"Taller 1. Matriz de riesgos Nombre Apellido.extensión".)*** Analice los criterios de evaluación que puede consultar en "Guía de evaluación" y verifique que los cumpla; luego haga clic en la opción "**Agregar entrega**"; en el cuadro de texto, haga una corta reflexión indicando cómo le pareció la realización de esta TIA, destacando los aspectos positivos de la experiencia y las recomendaciones para mejorarla; luego, haga clic en la opción "**Guardar cambios**" para que el taller pueda ser valorado.

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO
TALLER 1

20%

Análisis y Evaluación de riesgos de la seguridad de software mediante la matriz de riesgos

INSTRUCCIONES:

- Cada uno ingrese sus nombres y apellidos completos.

# INTEGRANTE	NOMBRES Y APELLIDOS COMPLETOS (Cada integrante ingrese sus nombres y apellidos completos)
1	Samuel Alzate Echeverri
2	Maria Camila Rojas
3	Juan Jose Rivera V

- Definan quién de ustedes será el líder del grupo para este taller

# INTEGRANTE	NOMBRES Y APELLIDOS COMPLETOS (El líder escogido ingresa sus nombres y apellidos)
1	Samuel Alzate Echeverri

1. Contextualización de la seguridad de acuerdo a las normas de seguridad:

Como equipo van a identificar los aspectos de seguridad de las normas ISO 27001 e ISO 27005 a tener en cuenta para presentar la matriz de riesgos de la seguridad del software de interfaces solicitado por el decano.. Para esto cada uno haga una búsqueda en los documentos de apoyo y escriba a continuación al menos un aspecto para cada norma:

INTEGRANTE 1	INTEGRANTE 2	INTEGRANTE 3
Aspecto de la ISO 27001	**Aspecto de la ISO 27001**	**Aspecto de la ISO 27001**
9.1 Evaluación de riesgo Monitoreo , analisis , medicion y evaluacion Siempre hay que evaluar los posibles riesgos y amenazas que pueden pasar en un activo	10. Mejora No Conformidad y siempre estar mejorando y tomar acciones para corregirlo y controlarlo	7.4 Comunicación Siempre hay que saber en que momento comunicarse con el equipo para evitar falsas alarmas y siempre es al que mas sabe comunicarle esto y con quien comunicarlo
Aspecto de la ISO 27005	**Aspecto de la ISO 27005**	**Aspecto de la ISO 27005**
8.2 Análisis Del Riesgo Identificar el riesgo y tambien identificar que consecuencias trae ese riesgo si puede tener pérdidas	8.2.1.2 Identificación de los activos Primero identificar el activo que tiene valor para la organización y requiere proteccion por que si el activo es vulnerable puede ocasionar un daño más grave	8.2.1.3 Identificación de las amenazas Hay amenazas que ponen en riesgo el bien de la empresa por eso siempre hay que investigar que el origen sea humano o natural para evitar que esto amenace mas activos

2. **Identificación de activos de información:**

Escriba una lista de activos de información del SIAG (tenga en cuenta que estos activos son exclusivos del módulo o interfaces)

Base de datos: Contiene información sensible como usuarios, registros administrativos y datos operativos

Archivos: Documentos generados o almacenados en el sistema

Software: Aplicaciones y programas que permiten la gestión del sistema

Equipos informáticos: Servidores y estaciones de trabajo utilizadas para el acceso y procesamiento de la información

Equipos de comunicación: Dispositivos de red que permiten la conectividad entre los sistemas

Servicios tecnológicos: APIs, servicios en la nube o infraestructura digital que soporta el sistema

Recurso humano: Personas con acceso a los activos de información

Documentación del sistema: Manuales técnicos y políticas de seguridad

2.1 Identifique los activos de información para las interfaces solicitadas - estudio de caso.

ACTIVOS DE LA AINFORMACIÓN	DESCRIPCIÓN	IMPORTANCIA
1. BASES DE DATOS ACADEMICA	Contiene información de estudiantes, docentes y proveedores.	**CRITICA**
2. CREDENCIALES DE ACCESO	Almacena notas, matrículas, historial académico y demás registros Usuarios y contraseñas de estudiantes, docentes y administrativos.	**CRITICA**

3. REGISTROS DE MATRICULA	Permiten autenticación en la plataforma.	**ALTA**
4. HISTORIAL ACADEMICO	Información de inscripción y asignación de cursos de los estudiantes.	**ALTA**
5. REGISTRO DE NOTAS	Datos sobre calificaciones, promedios ponderados y avances en los programas académicos.	**CRITICA**
6. INFORMACIÓN DE FALTAS DISCIPLINARIAS	Reporte de sanciones sobre el comportamiento de los estudiantes.	**ALTA**
7. MODULO DE EVALUACIÓN DOCENTE	Permite la calificación del desempeño de los profesores por parte de los estudiantes.	**ALTA**
8. REGISTROS DE PAGO Y LIQUIDACIÓN	Información financiera de estudiantes y transacciones relacionadas con matrículas.	**CRITICA**
9. DATOS PERSONALES	Información de identificación de estudiantes y docentes (nombres, direcciones, correos, teléfonos, etc.).	**CRITICA**
10. LOGS DE ACTIVIDAD	Registros de acceso y operaciones realizadas en el sistema por cada usuario.	**ALTA**
11. RED DE COMUNICACIONES	Infraestructura de switches, routers y firewalls que permite el acceso a la plataforma SIAG.	**ALTA**

2.2 Defina qué tan crítico o importante es cada activo identificado para la organización.

Módulo de usuarios: Datos personales, roles y credenciales

Módulo de reportes: Información analítica y registros históricos

Módulo administrativo: Datos financieros, operativos y logísticos

3. Identificación de amenazas

3.1 Desarrolle una lista con las amenazas contra los atributos de seguridad de la información (Confidencialidad, integridad y disponibilidad) teniendo en cuenta el contexto de desarrollo de las modificaciones al software

Errores en validación de entrada de datos: Si no se implementan correctamente validaciones en los nuevos formularios, los atacantes podrían inyectar datos maliciosos

Inyección SQL en nuevas consultas: Si las modificaciones en las interfaces incluyen interacciones con la base de datos sin sanitización de entradas, se pueden generar vulnerabilidades
Cross-Site Scripting (XSS) en nuevos campos de entrada : Si las nuevas interfaces permiten la ejecución de scripts maliciosos, los usuarios pueden ser víctimas de ataques

Falta de control de accesos en nuevas funcionalidades: Un error en los permisos podría permitir que usuarios sin autorización accedan a opciones restringidas

Divulgación de información sensible en respuestas del servidor: Si los nuevos componentes no manejan correctamente errores o excepciones, podrían exponer datos internos

Inyección de código en nuevas API o endpoints: Si el desarrollo de APIs no contempla validaciones estrictas, un atacante podría manipular peticiones y obtener acceso no autorizado

Uso de frameworks o bibliotecas obsoletas en los nuevos desarrollos: Si el código de los nuevos módulos usa versiones desactualizadas, se pueden introducir vulnerabilidades conocidas

Falta de cifrado en el intercambio de datos: Si las nuevas funciones transmiten información sin cifrado adecuado, podrían ser interceptadas por atacantes

Errores en la gestión de sesiones: Si los nuevos módulos no implementan correctamente la autenticación y cierre de sesión, se pueden generar accesos indebidos

Desbordamiento de buffer en nuevos formularios o campos de carga: Si los nuevos módulos no limitan correctamente la cantidad de datos ingresados, pueden ser explotados para ataques

3.2 Justifique por qué se consideran estas amenazas a la seguridad SIAG

Comprometen la confidencialidad Si una nueva función filtra datos sensibles, la información de los usuarios queda expuesta

Afectan la integridad errores en validaciones permiten modificar registros de forma no autorizada

Reducen la disponibilidad Implementaciones deficientes pueden generar fallas o interrupciones en el sistema

4. Evaluación de riesgos

4.1 Estime la amenaza según las metodologías de evaluación de riesgos estudiadas.

Bajo (1-3): Poco probable y con bajo impacto

Medio (4-6): Probabilidad moderada, impacto controlable

Alto (7-9): Muy probable o con impacto crítico

4.2 Considere los criterios de seguridad que proponen las metodologías estudiadas.

Confidencialidad: Protección de la información académica y financiera

Integridad: Evitar modificaciones no autorizadas en registros de notas, matrículas y pagos

Disponibilidad: Garantizar el acceso continuo a los servicios de la plataforma

4.3 Considere las vulnerabilidades para asignar la probabilidad (posibilidad de ocurrencia) de cada amenaza.

- **Acceso no seguro a la interfaz del SIAG:** Ya que se podría acceder fácilmente a la información que se tiene registrada (**ALTA**).
- **FALTA DE SEGMENTACIÓN EN LA RED:** Si la red no está segmentada adecuadamente cualquier equipo puede estar comprometido y puede ser un punto de acceso a la información (**Mediana**).
- **FALTA DE MONITOREO EN ACCESOS Y REGISTROS DE ACTIVIDAD:** Si no se tienen registros detallados de los accesos y operaciones realizadas un atacante puede hacer operaciones maliciosas sin ser detectado (**Mediana**).

5. Construcción de la matriz de riesgos

5.1 Diseñe y construya una “matriz de riesgos”, donde pueda presentar los riesgos de acuerdo a su criticidad o importancia.

Se tendrá en cuenta la creatividad para su diseño, es decir, las facilidades que brinde para priorizar los riesgos a gestionar o controlar por el sistema de gestión de la seguridad.

La matriz de riesgos puede ser realizada en alguna herramienta ofimática.

En los documentos de apoyo, se presenta un ejemplo de matriz de riesgos aunque cada equipo de estudio está en libertad de utilizar otro diseño.

MATRIZ DE RIESGO

Maria Camila Rojas
Juan Jose Rivera V
Samuel Alzate Echeverri

ID	ACTIVOS DE INFORMACION	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	MEDIDAS DE MITIGACION
1	**BASE DE DATOS ACADEMICA**	**ACCESO SIN AUTENTICACION FUERTE (SIN 2FA)**	**ROBO DE CREDENCIALES Y ACCESO NO AUTORIZADO**	ALTO	CRITICO	ALTO	**IMPLEMENTACION AUTENTICACION DE DOBLE FACTOR (2FA) RESTRICCIONES DE ACCESO**
2	**INFRASTRUCTURA**	**FALTA DE SEGMENTACION DE RED**	**ATAQUES INTERNOS O PROPAGACION DE MALWARE**	MEDIO	ALTA	MEDIO-ALTO	**SEGMENTAR LA RED Y ESTABLECER REGLAS DE ACCESO ESPECIFICAS**
3	**INTERFAZ DE WEB DEL SIAG**	**DATOS TRASNMITIDOS SIN CIFRADO ADECUADO**	**INTERCEPCION DE DATOS POR ATAQUES MAN-IN-THE-MIDDLE**	MEDIO	CRITICO	ALTO	**IMPLEMENTA HTTPS CON 1 Y CIFRADO EN TRANSITO**
4	**LOGS DE ACTIVIDAD**	**FALTA DE MONITOREO EN ACCESOS Y REGISTROS**	**MODIFICACION DE RESGISTROS ACADEMICOS SIN DETECCION**	ALTO	ALTA	MEDIO-ALTO	**IMPLEMENTAR AUDITORIAS AUTOMATICAS Y ALERTAS DE ACTIVIDAD SOSPECHOSA**
5	**SERVIDORES SIAG**	**FALTA DE ACTUALIZACIONES DE PARCHES DE SEGURIDAD**	**EXPLOTACION DE VULNERABILIDAES EN EL SISTEMA**	MEDIO	CRITICO	ALTO	**IMPLEMENTAR ACTUALIZACIONES PERIODICAS Y MONITOREO DE SEGURIDAD**
6	**CREDENCIALES DE USUSARIOS**	**USO DE CONTRASEÑAS DEBILES**	**ATAQUE DE FUERZA BRUTA PARA OBTENER ACCESO**	ALTO	ALTA	ALTO	**IMPLEMENTAR POLITICAS DE CONTRASEÑAS SEGURAS Y BLOQUEOS POR INTENTOS FALLIDOS**

Finalmente, cada integrante, elabore un resumen entre 5 y 10 renglones donde expresen la importancia de utilizar la matriz de riesgos para analizar y evaluar riesgos de seguridad de Software

INTEGRANTE 1	INTEGRANTE 2	INTEGRANTE 3
Samuel Alzate Echeverri La matriz de riesgos es una herramienta fundamental en la seguridad del software, ya que permite identificar, analizar y clasificar las amenazas que pueden afectar un sistema. A través de esta, es posible evaluar el impacto y la probabilidad de cada vulnerabilidad, priorizando aquellas que requieren una solución inmediata. En el caso de sistemas críticos como el SIAG, su uso garantiza la protección de datos sensibles, evitando accesos no autorizados, modificaciones ilegítimas y ataques cibernéticos. Además, facilita la toma de decisiones estratégicas para fortalecer la infraestructura tecnológica, implementando medidas de seguridad adecuadas y asegurando la continuidad del servicio.	**Maria Camila Rojas Ospina** La matriz de riesgos es una herramienta clave para identificar, evaluar y priorizar amenazas en la seguridad del software. Permite clasificar los riesgos según su impacto y probabilidad, facilitando la toma de decisiones y enfocando esfuerzos en los problemas más críticos. Su uso ayuda a prevenir vulnerabilidades, optimizar recursos y mejorar la seguridad desde el desarrollo del software.	**Juan Jose Rivera** El uso de una matriz de riesgos en la seguridad de software es clave para identificar vulnerabilidades y definir estrategias de mitigación ante posibles amenazas. Esta herramienta permite organizar y evaluar los riesgos con base en su probabilidad de ocurrencia y su impacto, asegurando una mejor gestión de la seguridad informática. Aplicada a un sistema académico como el SIAG, ayuda a proteger información vital como datos de estudiantes, registros de notas y accesos administrativos. Gracias a este análisis estructurado, es posible fortalecer la protección de los sistemas, prevenir incidentes y garantizar la integridad y confidencialidad de la información**.**

Por último, haga una copia de este archivo [Archivo/Hacer una copia] regrese a Classroom, adjunte la copia este archivo desde Drive y haga clic en Enviar, para que su Tutor pueda valorar su experiencia en este taller.