Campus Santa Fe

Ingeniería en Tecnologías Computacionales (ITC)

Semestre: 5°

Clase:

Integración de seguridad informática en redes y sistemas de software (Gpo 402)

Título:

Análisis de Riesgos

Equipo 6:

Fernando Adrián Fuentes - A01028796

Pedro Mauri Martínez - A01029143

Ricardo Alfredo Calvo - A01028889

Salvador Vaquero Becerra - A01027920

Profesores:

Carlos Enrique Vega Álvarez

Edith Carolina Arias Serna

Lizbeth Peralta Malváez **(Coordinadora)**

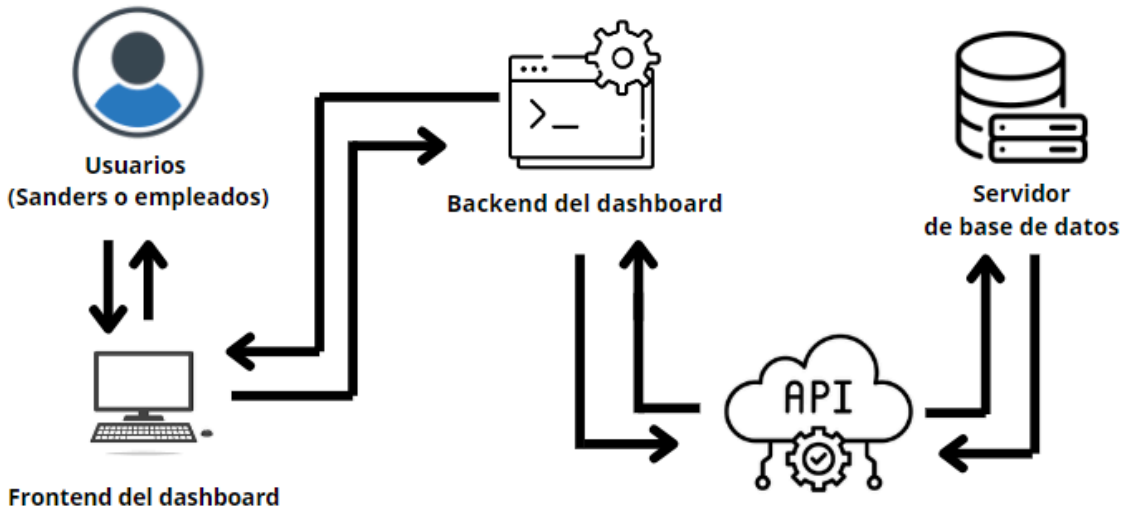
Osvaldo Cecilia Martínez

II. Índice

III. Objetivos

Identificar y evaluar los riesgos de seguridad asociados a la solución de software, priorizando aquellos que representan un mayor impacto y proponiendo medidas de mitigación eficaces.

IV. Descripción de los componentes de la solución de software y la interacción entre ellos + diagrama



1. Usuarios:
    a. Las personas que interactúan con el sistema son los administradores de la fundación Sanders con un rango alto de permisos, empleados de la fundación con rol de permisos medio, y por último; los donantes, los cuales únicamente tienen la acción de crear donaciones.

2. Frontend del dashboard:
    a. Interfaz gráfica por la que los usuarios interactúan con el sistema, comunicándose con el backend del dashboard a través de la API del sistema.

3. Backend del dashboard:
    a. Conjunto de funciones encargado de manejar la lógica y procesamiento de datos, recibiendo las solicitudes del frontend, validarlas para luego interactuar con la base de datos.

4. API:

a. Encargado de ser el intermediario entre el backend y el servidor de base de datos, define endpoints que el backend usa para aplicar sistema CRUD con los datos guardados.

5. Servidor de base de datos:
    a. Lugar donde se almacenan los datos utilizados en el sistema, las operaciones de CRUD se ejecutan por el usuario a través del API entre el frontend del dashboard hasta llegar a la base de datos.

V. Identificación de componentes críticos de la solución de software

Activo 1: CRM (Frontend y backend de dashboard):

- Activo principal del sistema, donde se gestionan los datos de los clientes y se realizan la mayoría de las operaciones.

Activo 2: Base de datos:

- Almacenamiento de datos personales de donantes que requieren ser guardados con seguridad, sin los datos que se guardan; no sería posible desarrollar esta solución de problema.

Activo 3: Reputación:

- Un fallo de seguridad afecta directamente la confianza de los donantes. Importante para la fundación, ya que sin la confianza de sus donantes no tendrían donaciones entrantes por medio del sistema desarrollado.

VI. Matriz CIA o STRIDE para la identificación de amenazas

	Confidencialidad	Integridad	Disponibilidad
CRM	-Falsificación de roles. -Intrusión.	-XSS. -Ransomware.	-Caída de servicio.
Base de datos	-Robo de datos personales. -Injection NoSQL.	-Ransomware.	-Pérdida de datos. -Bloqueo.
Reputación	-Robo de información.		

VII. Matriz de riesgos (heat map) para la estimación del nivel de riesgo

		Impacto		
		Alto	Medio	Bajo
Probabilidad	Alto	Muy Alto	Alto	Medio
	Medio	Alto	Medio	Medio / Bajo
	Bajo	Alto / Medio	Bajo	Bajo

Activo 1: CRM					
CIA	Riesgo	Descripción	Impacto	Probabilidad	Nivel de riesgo
Confidencialidad	Falsificación de roles	Un usuario no autorizado accede al CRM, utilizando el token de un usuario administrador, exponiendo la información del CRM y comprometiendo su integridad.	Fuga de información confidencial. (Alto)	63% (Medio)	Alto
Confidencialidad	Intrusión	Robo de credenciales para acceder al CRM	Fuga de información confidencial. (Alto)	75% (Muy Alto)	Muy Alto
Integridad	XSS	Uso de javascript para comprometer el contenido del CRM.	Confiabilidad en datos. (Alto)	29% (Bajo)	Alto / Medio

Integridad	Ransomware	Alteración de la información	Confiabilidad en datos. (Alto)	55% (Medio)	Alto
Disponibilidad	Caída de servicio	Interrupciones en el servicio debido a fallas del sistema, ataques DDoS o errores de configuración.	Pérdida de acceso a la aplicación, impacto en la experiencia del usuario y posibles pérdidas monetarias. (Medio)	55% (Medio)	Medio

Activo 2: Base de datos					
CIA	Riesgo	Descripción	Impacto	Probabilidad	Nivel de riesgo
Confidencialidad	Robo de datos personales	Un atacante o usuario interno accede y extrae datos sensibles del servidor.	Fuga de información confidencial. (Alto)	50% (Medio)	Alto
Confidencialidad	Injection NoSQL	Saltarse los protocolos de autenticación.	Acceso no autorizado al CRM. (Alto)	80% (Alto)	Alto
Integridad	Ransomware	Alteración de la información.	Confiabilidad en datos. (Alto)	55% (Medio)	Alto
Disponibilidad	Bloqueo	Bloqueo para acceder a la base de datos.	No poder acceder a los datos. (Bajo)	20% (Bajo)	Bajo

Disponibilidad	Pérdida de datos	Falta de copias de seguridad actualizadas lleva a la pérdida irrecuperable de datos tras un fallo del sistema o ataque.	Pérdida total o parcial de datos, necesidad de reconstrucción de información. (Medio)	55% (Medio)	Medio

Activo 3: Reputación					
CIA	Riesgo	Descripción	Impacto	Probabilidad	Nivel de riesgo
Confidencialidad	Robo de información de clientes	Robo de información.	Credibilidad para Fundación Sanders. (Medio)	45% (Medio)	Medio

VIII. Priorización de riesgos y definición de tratamiento para los riesgos (evitar, transferir, mitigar, aceptar)

Ordenamiento de los riesgos según su nivel de criticidad:

1. Falsificación de roles.
2. Intrusión.
3. Robo de datos personales.
4. Injection NoSQL.
5. Ransomware.

Alto:

1. **Falsificación de roles:** Mitigar; implementando autenticación multifactor para usuarios con colores críticos.
2. **Intrusión:** Evitar, usar contraseñas fuertes y únicas.
3. **Ransomware:** Evitar, normalmente se debe a un archivo malicioso por ende evitar el contacto con estos.
4. **Robo de datos personales:** Aceptar, no puede haber un sistema completamente seguro por lo que se acepta que existe la posibilidad para un robo de datos personales por lo que se guardan únicamente datos completamente necesarios.

5. **Injection NoSQL:** Mitigar, implementar medidas para hacer una inyección NoSQL

Medio:

1. **XSS:** Mitigar, que no se pueda realizar XSS.
2. **Caída de servicio:** Mitigar, con buena configuración y defensa contra DDoS.
3. **Pérdida de datos:** Mitigar, guardar copias de seguridad.
4. **Robo de información de clientes:** Transferir, se requiere de un equipo legal, siendo que se refiere al activo de reputación.

Bajo:

1. **Bloqueo:** Aceptar, no presenta ningún riesgo mayor y es fácil de resolver en caso de que ocurra.

IX. Selección de medidas de mitigación por cada riesgo y describir consideraciones para su implementación. Considerar al menos los siguientes controles:

1. Seguridad de datos en tránsito: https para backend y frontend.
    - **Medida de mitigación:** Implementar el uso de HTTPS para asegurar que todas las comunicaciones entre el frontend, backend y API.
    - **Consideraciones para implementación:**
        - Certificado SSL válido requerido.
        - Transición de http a https.
        - Verificar configuraciones SSL / TLS.

2. Seguridad de datos en reposo: *hasheo* de secretos.
    - **Medida de mitigación:** Los datos sensibles como las contraseñas de los usuarios deben encriptarse por medio de algoritmos hash.
    - **Consideraciones para implementación:**
        - Asegurar que todos los secretos se almacenen utilizando un hash seguro.
        - Configurar el proceso de revisión.
        - Implementación de sistema de gestión de secretos.

3. Controles de autenticación: login y generación de tokens JWT.
    - **Medida de mitigación:** Implementar un sistema de autenticación basado en tokens JWT, que garantice la seguridad de los usuarios y las sesiones.
    - **Consideraciones para implementación:**
        - Los tokens JWT deben estar firmados y encriptados para prevenir la falsificación o manipulación de los mismos.

- Utilizar algoritmos seguros para la firma de los JWT como RS256.
- Establecer tiempos de expiración cortos para los tokens JWT.

4. Controles de autorización: roles de usuario y validación de de tokens JWT.
    - **Medida de mitigación:** Establecer un sistema de control de acceso basado en roles, donde los usuarios tengan permisos específicos según su rol en el sistema.
    - **Consideraciones para implementación:**
        - Asignar los permisos mínimos necesarios a cada rol.
        - Asegurar que cada solicitud realizada por el usuario sea validada mediante el token JWT.

5. Prevención de vulnerabilidades comunes (XSS y SQL / NOSQL injection).
    - **Medida de mitigación:**
        - **Prevención de XSS:**
            - Validar y sanitizar todas las entradas del usuario en el frontend y backend.
            - Escapar cualquier dato dinámico antes de ser inyectado en HTML.
        - **Prevención de SQL/NoSQL Injection:**
            - Implementar una capa adicional de validación de entradas en el backend para asegurarse de que los datos introducidos por el usuario sigan un formato seguro y esperado.
    - **Consideraciones para implementación:**
        - Mantener actualizados los componentes de seguridad (ORM, frameworks, librerías) que se utilizan en la aplicación.

XII. Conclusiones

En este análisis de riesgos creado para el sistema de la Fundación Sanders se ha identificado una serie de posibles amenazas para los principales activos: CRM, base de datos y la reputación de la organización. Los riesgos más peligrosos o con mayor impacto incluyen la falsificación de roles, intrusiones, ransomware, y robo de datos personales, todos los cuales si llegan a ocurrir tendrían un alto impacto y se necesitan medidas de mitigación urgentes.

Las recomendaciones para mitigar o evitar estos riesgos incluyen la implementación de autenticación multifactor, el uso de contraseñas robustas y únicas, y la adopción de medidas preventivas contra inyecciones NoSQL y ataques de ransomware. Además, se ha priorizado la seguridad de los datos tanto en tránsito como en

reposo, con controles específicos como el uso de HTTPS, hasheo, y la correcta gestión de tokens JWT para la autenticación y autorización.

En resumen, es completamente necesario que el sistema cuente con estrategias de mitigación para los riesgos identificados y que la fundación Sanders realice una revisión continua de sus prácticas de seguridad una vez entregado el sistema. Con esto se logrará la protección de sus datos sensibles, la integridad del sistema y la confianza de los donantes, elementos que son esenciales para lograr sacarle el máximo provecho al sistema.