Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

Mitsiu Alejandro Carreño Sarabia - E23S-18014

Contexto empresa: TechSolutions Inc.

TechSolutions Inc. es una empresa ficticia dedicada a desarrollar y vender software personalizado para pequeñas y medianas empresas (PyMEs). La empresa ofrece servicios que van desde la consultoría y análisis de requerimientos hasta el desarrollo, implementación y soporte técnico de soluciones de software.

En TechSolutions Inc., cada proceso está claramente definido y alineado con los objetivos de la empresa. Los roles están bien distribuidos, asegurando que cada persona se enfoque en tareas específicas para optimizar la eficiencia y efectividad. La implementación de diversas tecnologías permite automatizar tareas, mejorar la comunicación y facilitar la gestión de proyectos y recursos. Al integrar BPM, TechSolutions Inc. puede mejorar continuamente sus procesos, adaptándose rápidamente a cambios en el mercado y necesidades de los clientes.

Procesos Clave

1. Proceso de Ventas y Marketing
    - Generación de leads
    - Calificación de leads
    - Presentación de demos y propuestas
    - Negociación y cierre de ventas

2. Proceso de Gestión de Proyectos
    - Planificación del proyecto
    - Asignación de recursos
    - Seguimiento y control del proyecto
    - Entrega y cierre del proyecto

3. Proceso de Desarrollo de Software
    - Análisis de requerimientos
    - Diseño de software
    - Programación y pruebas
    - Implementación y despliegue

4. Proceso de Soporte Técnico

- Recepción y categorización de tickets
- Resolución de incidencias
- Mantenimiento preventivo
- Actualizaciones y mejoras

5. Proceso de Recursos Humanos
   - Reclutamiento y selección
   - Capacitación y desarrollo
   - Evaluación de desempeño
   - Gestión de nómina y beneficios

Personas y Roles

1. Proceso de Ventas y Marketing
   - Roles:
     - Gerente de Ventas: Supervisa al equipo de ventas, establece metas y estrategias.
     - Ejecutivo de Ventas: Gestiona los leads, realiza presentaciones y cierra ventas.
     - Especialista en Marketing: Genera campañas de marketing y gestiona redes sociales.

2. Proceso de Gestión de Proyectos
   - Roles:
     - Gerente de Proyectos: Planifica, coordina y supervisa los proyectos.
     - Coordinador de Proyectos: Asiste al gerente de proyectos y gestiona tareas diarias.
     - Analista de Proyectos: Realiza análisis y seguimiento de métricas del proyecto.

3. Proceso de Desarrollo de Software
   - Roles:
     - Desarrollador de Software: Programa y prueba el software.
     - Arquitecto de Software: Diseña la estructura del software.
     - Tester/QA: Realiza pruebas para asegurar la calidad del software.

4. Proceso de Soporte Técnico
   - Roles:
     - Gerente de Soporte Técnico: Coordina el equipo de soporte y prioriza incidentes.
     - Técnico de Soporte: Resuelve incidencias y realiza mantenimiento preventivo.
     - Especialista en Atención al Cliente: Gestiona la recepción de tickets y comunica con clientes.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

5. Proceso de Recursos Humanos
- Roles:
  - Gerente de Recursos Humanos: Supervisa las actividades del departamento de RRHH.
  - Especialista en Reclutamiento: Realiza procesos de selección y contratación.
  - Coordinador de Capacitación: Gestiona programas de capacitación y desarrollo.

Tecnologías Implementadas

1. Proceso de Ventas y Marketing
- CRM: Salesforce para la gestión de leads y seguimiento de clientes.
- Plataformas de Marketing: HubSpot para automatización de marketing y campañas de correo electrónico.

2. Proceso de Gestión de Proyectos
- Software de Gestión de Proyectos: Asana para planificación y seguimiento de tareas.
- Herramienta de Colaboración: Slack para comunicación y colaboración del equipo.

3. Proceso de Desarrollo de Software
- IDE: Visual Studio Code para desarrollo de software.
- Control de Versiones: Git y GitHub para gestión de código fuente.
- Plataforma de Integración Continua: Jenkins para pruebas y despliegue continuo.

4. Proceso de Soporte Técnico
- Sistema de Ticketing: Zendesk para la gestión de incidencias y soporte técnico.
- Base de Conocimiento: Confluence para documentación y soluciones comunes.

5. Proceso de Recursos Humanos
- Software de Gestión de Recursos Humanos: BambooHR para gestión de nómina, beneficios y desempeño.
- Plataforma de Capacitación: LinkedIn Learning para capacitación y desarrollo de empleados.

Responder las siguientes preguntas con la finalidad de reducir los riesgos de ciberseguridad en la empresa TechSolutions Inc., para mitigar las vulnerabilidades en diversas áreas tecnológicas:

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

- ¿Qué medidas de autenticación y autorización están implementadas para proteger el acceso a los sistemas internos?

Se recomienda establecer una estratégia zero trust en la que cada conexión debe ser autorizada ya sea una conexión de un usuario, aplicación o dispositivo, en zero trust cada ente debe demostrar que tiene acceso al recurso solicitado así como demostrar su identidad, de esta manera se tiene control sobre los niveles de acceso y todos los entes que se pueden conectar.

- ¿Se realiza regularmente la evaluación de vulnerabilidades y pruebas de penetración en todos los sistemas?

Debe de realizarse una evaluación continua de vulnerabilidades, ya que es un campo en el que constantemente se realizan descubrimientos por lo que no es posible catalogar algo como seguro por siempre.

- ¿Está el sitio web protegido contra ataques comunes como XSS, CSRF y SQL Injection?

Cada uno de los sitios deberá contar con medidas de seguridad que prevengan ataques comunes (XSS, CSRF, SQL Injection), recordando que entre más sensible y especializado sea el software, se deben cubrir un mayor espectro de posibles ataques.

- ¿Utiliza HTTPS en todas las páginas web para asegurar la comunicación cifrada?

Dado que emplean plataformas comerciales (slack, Linkedin Learning, Asana, etc) dichas plataformas integran HTTPS por default, más todo desarrollo in-house debe seguir estas prácticas

- ¿Existe una política de actualización y parcheo para todos los servidores y aplicaciones web?

Dado el escenario que se describe no se menciona ningún tipo de política al respecto, pero marcos de referencia como OWASP SAMM que permiten definir estratégias respecto a actualizaciones del software empleado.

- ¿Están las aplicaciones móviles diseñadas con medidas de seguridad para proteger los datos sensibles almacenados en el dispositivo?

En el escenario no se menciona si el software empleado se accede a través de dispositivos móviles o de escritorio, pero se puede analizar respecto a las aplicaciones que sí cuentan con versión móvil (asana, linkedin) dado que estas aplicaciones son comerciales y desarrolladas por terceros es esperable que implementen medidas de seguridad, más todo desarrollo in-house deberá cubrir medidas de seguridad básicas.

- ¿Se realizan auditorías de seguridad en el código de las aplicaciones móviles antes de su despliegue?

Para los desarrollos in-house se deben establecer protocolos y metodologías para analizar el código generado respecto a integridad de datos, resguardo de datos, así como protecciones a ataques cibernéticos comunes

- ¿Están las aplicaciones móviles configuradas para solicitar permisos mínimos necesarios?

Las buenas prácticas establecen que así debe ser, las aplicaciones deben solicitar únicamente los permisos que requieran para su correcto funcionamiento.

- ¿Están los dispositivos IoT configurados con contraseñas fuertes y únicas?

En la descripción no se menciona ningún dispositivo IoT, pero en el mundo moderno es común contar con ellos, los cuales deben ser configurados apropiadamente respecto al uso y utilidad que tengan por finalidad, así como definir una contraseña distinta a la de fábrica, con alta entropía.

- ¿Se aplica cifrado de datos para la comunicación entre dispositivos IoT y la red interna?

Actualmente la mayoría de los dispositivos emplean cifrado por default, más en ciertos mercados no es una obligación, por lo que se recomienda investigar antes de realizar la compra que el dispositivo a adquirir cuente con cifrado por default y empleando protocolos seguros.

- ¿Existe una política de actualización de firmware y software para dispositivos IoT?

En la descripción no se menciona, más deberá haber una política y un rol asociado a la continua actualización de software y firmware, esta política se deberá extender más allá de los dispositivos IoT.

- ¿Cómo se gestionan las credenciales y accesos a los servicios en la nube (AWS, Azure, GCP)?

La estratégia zero trust propone que las credenciales deben ser obligatorias, lo más restrictivo posible y lo más granulares posible, con ello solo se ofrecen accesos a quien lo requiere solo con los privilegios que necesita, y si ese actor/dispositivo/app se ve comprometida no pueda escalar privilegios.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

- ¿Se aplican políticas de seguridad como la segmentación de redes y el uso de roles con permisos mínimos en la nube?

La descripción no lo menciona más se deberá implementar segmentación de redes y una política zero trust de permisos mínimos (no solo en la nube) para mitigar el riesgo de escalada de permisos y movimiento horizontal en caso de un ataque cibernético.

- ¿Están los datos en la nube cifrados tanto en tránsito como en reposo?

Los proveedores de servicio como AWS, Azure, GCP cuentan con cifrado usualmente por default, más es necesario investigar el proveedor específico para activarlo en caso de que sea opcional.

- ¿Se utilizan tokens de autenticación seguros (como JWT) para el acceso a las API's?

No se menciona en la descripción provista mas se recomienda aplicar mecanismos de autenticación y autorización como JWT para mitigar el riesgo de exponer información.

- ¿Están las API's protegidas contra ataques de denegación de servicio (DoS) y otras amenazas comunes?

La respuesta está vinculada a la configuración de red, proxy y del proveedor de servicio de red, actualmente la mayoría de los proveedores cuentan con protección DoS estándar.

- ¿Se realiza un registro y monitoreo exhaustivo de las actividades de las API's para detectar comportamientos anómalos?

Depende de la arquitectura que usen, varios servicios ofrecen registro por default (apache HTTP, nginx, AWS cloudwatch,) lo que permite realizar seguimiento y monitoreo del uso de la plataforma.

- ¿Se protegen los datos de entrenamiento y modelos de machine learning contra accesos no autorizados?

Es esperable que si la empresa descrita realiza tareas de entrenamiento en el área de machine learning se aseguren de proteger tanto la información de entrenamiento y validación así como los modelos entrenados, esto tanto por cuestiones legales de protección de datos como cuestiones de protección de propiedad intelectual.

- ¿Existe un proceso para verificar la integridad de los datos utilizados en el entrenamiento de modelos de machine learning?

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

Se deben establecer protocolos específicos que determinen cómo se recaba u obtiene la información, contar con el permiso explícito de usar los datos para entrenar un modelo y aislar el almacenamiento de dichos datos para evitar exponerlos innecesariamente.

- ¿Cómo se gestionan las dependencias y bibliotecas de terceros utilizadas en los proyectos de machine learning para evitar vulnerabilidades conocidas?

El modelo OWASP SAMM ofrece una serie de pautas para mitigar los riesgos asociados a dependencias, que van desde la enumeración misma de dependencias, hasta tratar las vulnerabilidades de terceros como propias.

- ¿Se implementan medidas para evitar el acceso no autorizado a los modelos de lenguaje grande (LLM) y sus datos?

Bajo una estrategia zero trust, se dictamina que todo acceso debe ser autorizado y autenticado con ello se fortalece la seguridad del sistema a la vez que se dificulta el acceso a terceros maliciosos.

- ¿Se realiza una evaluación de riesgos de seguridad antes de la implementación de LLMs en producción?

Se deben establecer riesgos así como planes de contingencia y mitigación para que el equipo esté preparado y sepa reaccionar ante eventualidades.

- ¿Se establecen controles para evitar el uso indebido de LLMs, como la generación de contenido malicioso?

Se deben establecer estrategias para limitar los vectores de interacción con LLMs esto permitirá el uso seguro y controlado del LLM ofreciendo un servicio de calidad.

- ¿Se dispone de un plan de respuesta a incidentes de ciberseguridad que incluya acciones específicas para cada área tecnológica?

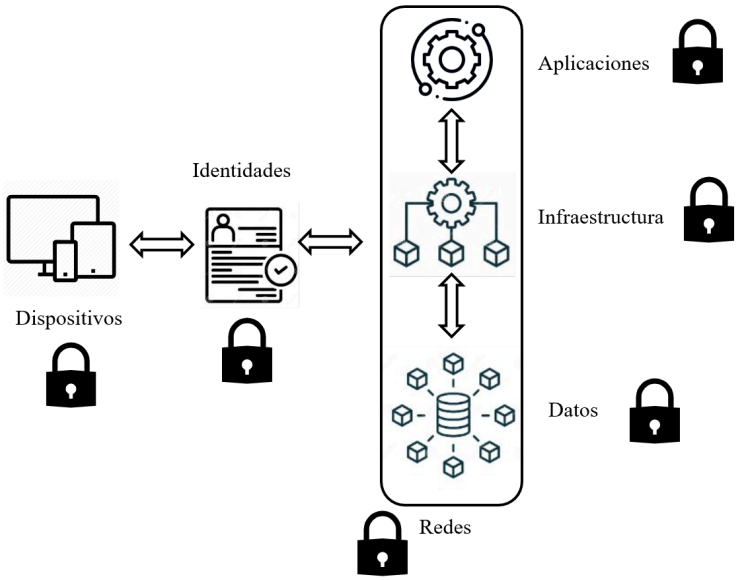
Se debe disponer de dichos planes adecuados a la capacidad técnica, tecnológica, de infraestructura y de personal estableciendo cuales son sus vulnerabilidades así como las acciones necesarias para recuperarse.

- ¿Se llevan a cabo capacitaciones regulares en ciberseguridad para todo el personal de la empresa?

Se deben realizar capacitaciones generales, pero bajo la estratégia zero trust, no se debe permitir más acceso del necesario y considero que se debe priorizar capacitaciones más técnicas y profundas a los responsables de reaccionar a riesgos de ciberseguridad.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

Considerando los puntos anteriores mencionados y realizando una reflexión de los componentes involucrados en la arquitectura Zero Trust, responder las siguientes preguntas.



- ¿Qué principios fundamentales sustentan el enfoque de seguridad de Zero Trust?

La estrategia zero trust se basa en 3 principios, “siempre verificar” mediante el cuál se solicita que cada conexión demuestre su acceso e identidad para poder continuar, “menor privilegio” en el que solo se dan los accesos necesarios a cada dispositivo y “asumir incumplimiento” que permite a la organización realizar estratégias para el peor escenario preparándose en caso de que realmente pase.

- ¿Cómo se diferencia Zero Trust de los modelos de seguridad tradicionales basados en perímetros?

Zero trust es un modelo mejor adaptado al mundo moderno donde los sistemas están distribuidos (trabajo desde casa, servidores remotos) y existe una amplia gama de dispositivos conectados (celulares, tablets, IoT), donde definir un “perímetro” es difícil porque ya no existen estas restricciones físicas, geográficas y monolíticas de una oficina con una red y dispositivos establecidos

- ¿Qué rol juega la autenticación multifactor (MFA) en una arquitectura Zero Trust?

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

Permite reforzar el principio de “siempre verificar” mediante el cuál no solo te auténticas con algo que sabes (usuario/contraseña) sino también con algo que tienes (token)

- ¿Qué pasos debe seguir una organización para implementar una estrategia de Zero Trust de manera efectiva?

Para implementar zero trust es necesario comenzar por entender que para su correcta implementación es necesario realizar cambios tanto técnicos como procedimentales en la forma de trabajo de los empleados; de manera general se debe definir los posibles vectores de ataque, implementar controles y segregación en las redes, implementar políticas y arquitecturas adecuadas para zero trust y realizar monitoreo de red.

- ¿Cómo puede la microsegmentación de red contribuir a la implementación de un modelo Zero Trust?

La microsegmentación sigue el principio de “asumir incumplimiento” al dificultar el movimiento lateral dentro de una red, aunque un actor malicioso logre acceder a una red, la cantidad de dispositivos a los que puede saltar dentro de la red está limitado por lo que se contiene el riesgo de infectar otros dispositivos.

Riesgos en tecnología web.

- ¿Cómo se puede prevenir la inyección SQL en una aplicación web?

La manera de prevenir SQL injection es filtrando y escapando apropiadamente cada input especialmente aquellos que provengan de usuarios.

- ¿Cuáles son las diferencias entre un ataque XSS almacenado y un XSS reflejado, y cómo se pueden mitigar ambos?

El ataque XSS almacenado es aquel en el que el input contaminado es guardado en el sistema y después leído y regresado a otro usuario, en cambio el XSS reflejado es aquel que el sistema inmediatamente interpreta el input contaminado y regresa al usuario información que no debe. Similar al SQL injection, se puede prevenir realizando filtros pertinentes a la entrada del usuario así como aplicar HTML encoding.

- ¿Qué medidas se pueden tomar para proteger una aplicación web contra ataques CSRF?

Varios frameworks contienen medidas anti CSRF, pero en caso de no contar con ellas es posible reforzar los mecanismos de autenticación y autorización con tokens dinámicos, o patrones de sincronización de tokens.

- ¿Qué es la deserialización insegura y qué prácticas pueden ayudar a evitarla en el desarrollo de aplicaciones web?

La deserialización es el proceso de interpretar una serie de bytes "flat" a una estructura compleja (por ejemplo un objeto) el proceso de deserializar involucra interpretar un stream de bytes desconocidos y si están en control del usuario es donde el riesgo existe. Para mitigarlo se recomienda evitar la deserialización de cualquier input que pueda modificar el usuario o en su defecto implementar controles que verifiquen la integridad de los datos serializados (firma digital)

- ¿Cómo puede una empresa asegurar que sus dependencias de software no introduzcan vulnerabilidades en su aplicación web?

Como se mencionó anteriormente el modelo OWASP SAMM ofrece una serie de pautas para mitigar los riesgos asociados a dependencias, en términos generales es necesario evaluar periódicamente la seguridad de las dependencias empleadas, e incluso se pueden considerar las vulnerabilidades de terceros como propias.

Riesgos en tecnología móvil

- ¿Qué medidas de seguridad se pueden implementar para prevenir la ejecución de comandos del sistema a través de entradas no validadas en aplicaciones móviles?

Se debe realizar una validación de todos los inputs que puede generar el usuario, realizar un manejo de excepciones adecuado y bloquear las tareas que tengan errores para prevenir vulnerabilidades en todas las capas del sistema.

- ¿Qué mejores prácticas aseguran que los datos sensibles estén cifrados en almacenamiento y transmisión en una aplicación móvil?

Como la pregunta lo indica, emplear técnicas de cifrado seguras (SHA256 por ejemplo) así como aplicar el cifrado de extremo a extremo además empleando protocolos de cifrado como HTTPS permiten que la información enviada sea segura y confidencial.

- ¿Cómo se puede mejorar la implementación de mecanismos de autenticación y gestión de sesiones en aplicaciones móviles para evitar vulnerabilidades comunes?

Una de las mejores estratégias es implementar mecanismos de autenticación modernos y conocidos, no es recomendable intentar desplegar un sistema de autenticación y gestión propio ya que puede contener vulnerabilidades importantes, además es necesario periódicamente evaluar dichas dependencias y actualizarlas de manera acorde.

- ¿Qué pasos deben seguir los desarrolladores para asegurar que las bibliotecas y paquetes utilizados en una aplicación móvil estén actualizados y libres de vulnerabilidades conocidas?

Como se mencionó anteriormente el modelo OWASP SAMM ofrece una serie de pautas para mitigar los riesgos asociados a dependencias, en términos generales es necesario evaluar periódicamente la seguridad de las dependencias empleadas, e incluso se pueden considerar las vulnerabilidades de terceros como propias.

- ¿Cuáles son los métodos más efectivos para asegurar la sanitización y validación de entradas del usuario en una aplicación móvil para prevenir ataques como XSS y CSRF?

De manera muy similar a un ataque web, para prevenir ataques XSS o CSRF es necesario implementar controles de filtro y validación apropiados como un validador de tipo, enum, expresiones regulares, etc.

Riesgos en tecnología para API`s.

- ¿Qué métodos de autenticación se están utilizando en nuestra API para garantizar que solo los usuarios y servicios autorizados puedan acceder a ella? ¿Estamos implementando tokens de acceso o certificados para este propósito?

Se implementó Json Web Tokens los cuales están firmados con un secret almacenado en el servidor y para cada petición se valida con la firma, así como se revisa si ha o no expirado.

- ¿Cómo estamos asegurando que los usuarios y servicios solo tengan acceso a los recursos y operaciones que realmente necesitan? ¿Estamos utilizando un control de acceso basado en roles (RBAC)?

Si, se generan middlewares por rol o por feature lo que permite filtrar las peticiones solo a los roles que sean apropiados para la conexión solicitada.

- ¿Qué medidas hemos implementado para proteger nuestra API contra ataques de falsificación de solicitudes entre sitios (CSRF)? ¿Estamos utilizando tokens anti-CSRF y asegurándonos de que todas las solicitudes requieran autenticación?

En efecto, se han activado las opciones anti-CSRF del framework empleado y como se comentó anteriormente se han habilitado middlewares que validan la autenticación.

- ¿Qué procesos de validación y sanitización de datos hemos implementado para todas las entradas de usuario y datos recibidos a través de la API? ¿Cómo prevenimos ataques de inyección de SQL y scripting entre sitios (XSS)?

Por el lado de la inyección SQL se ha estandarizado el uso de cadenas escapadas provistas por el mismo driver de conexión a la base de datos, para la validación XSS se ha implementado la librería AJV validator que nos permite definir las estructuras y tipos de datos esperados.

- ¿Tenemos un sistema robusto de registro y monitoreo en funcionamiento para detectar y responder rápidamente a posibles amenazas o comportamientos anómalos? ¿Cómo registramos los eventos de seguridad para permitir un análisis forense en caso de incidentes?

Se han implementado sistemas de bitácoras tanto a nivel servidor (docker) como a nivel proxy (nginx) por lo que es posible rastrear peticiones o guardar los registros para una evaluación más profunda, además se integraron sistemas de reporte de errores (sentry) que nos permiten detectar actividad sospechosa en tiempo real.

Riesgos en tecnología para Machine Learning (ML).

- ¿Qué métodos de autenticación se están utilizando en nuestra API para garantizar que solo los usuarios y servicios autorizados puedan acceder a ella? ¿Estamos implementando tokens de acceso o certificados para este propósito?

Como se mencionó anteriormente se implementó Json Web Tokens los cuales están firmados con un secret almacenado en el servidor y para cada petición se valida con la firma, así como se revisa si ha o no expirado.

- ¿Cómo estamos asegurando que los usuarios y servicios solo tengan acceso a los recursos y operaciones que realmente necesitan? ¿Estamos utilizando un control de acceso basado en roles (RBAC)?

Como se mencionó anteriormente, se generan middlewares por rol o por feature lo que permite filtrar las peticiones solo a los roles que sean apropiados para la conexión solicitada.

- ¿Qué medidas hemos implementado para proteger nuestra API contra ataques de falsificación de solicitudes entre sitios (CSRF)? ¿Estamos utilizando tokens anti-CSRF y asegurándonos de que todas las solicitudes requieran autenticación?

Como se mencionó anteriormente, se han activado las opciones anti-CSRF del framework empleado y como se comentó anteriormente se han habilitado middlewares que validan la autenticación.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

- ¿Qué procesos de validación y sanitización de datos hemos implementado para todas las entradas de usuario y datos recibidos a través de la API? ¿Cómo prevenimos ataques de inyección de SQL y scripting entre sitios (XSS)?

Como se mencionó anteriormente, por el lado de la inyección SQL se ha estandarizado el uso de cadenas escapadas provistas por el mismo driver de conexión a la base de datos, para la validación XSS se ha implementado la librería AJV validator que nos permite definir las estructuras y tipos de datos esperados.

- ¿Tenemos un sistema robusto de registro y monitoreo en funcionamiento para detectar y responder rápidamente a posibles amenazas o comportamientos anómalos? ¿Cómo registramos los eventos de seguridad para permitir un análisis forense en caso de incidentes?

Como se mencionó anteriormente, se han implementado sistemas de bitácoras tanto a nivel servidor (docker) como a nivel proxy (nginx) por lo que es posible rastrear peticiones o guardar los registros para una evaluación más profunda, además se integraron sistemas de reporte de errores (sentry) que nos permiten detectar actividad sospechosa en tiempo real.

Riesgos en tecnología para Large Language Models (LLM).

- ¿Qué medidas de seguridad están implementadas para detectar y prevenir la manipulación de prompts que busquen acceso no autorizado, filtraciones de datos o comprometer la toma de decisiones?

Se han implementado estrategías de validación de inputs y segregación de contenidos, además de técnicas tradicionales como sistemas de autenticación y autorización.

- ¿Cómo se asegura que los resultados generados por el LLM sean validados correctamente para evitar vulnerabilidades de seguridad, como la ejecución de código malicioso?

Se sanitiza y valida todos el contenido generado por el LLM para prevenir filtraciones de información.

- ¿Qué estrategias existen para proteger la integridad de los datos de entrenamiento y prevenir que una reducción gradual comprometa la seguridad, precisión o comportamiento ético del LLM?

Se somete a un proceso riguroso de verificación y validación de las fuentes de información, se aplica tratamiento y rotación de los datos empleados para el entrenamiento.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

- ¿Qué mecanismos de control de carga se han implementado para evitar que una sobrecarga de peticiones mediante prompts afecte los recursos computacionales y provoque interrupciones en el servicio o aumente los costos operativos?

Se han implementado protección DoS por el proveedor de servicios de red que ofrecen protección DoS así como técnicas de limitación de peticiones por usuario e implementación de colas de espera.

- ¿Qué protocolos se siguen para evitar la divulgación de datos confidenciales en los resultados generados por el LLM, y cómo se manejan las consecuencias legales o la pérdida de credibilidad en caso de que ocurra una filtración?

Se han aplicado una serie de protocolos que salvaguardan la integridad y confidencialidad de los datos, así como una constante evaluación de vulnerabilidades en librerías y paquetes empleados. Respecto al manejo de filtraciones, se aplica una serie de validaciones y aseguramiento de la cadena de suministros para evitar posibles filtraciones.

Referencias

- Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], 10.6028/NIST.SP.800-207

- Cusick, James. (2018). The General Data Protection Regulation (GDPR): What Organizations Need to Know. CT Corporation Resource Center.

- Seaman, Jim. (2023). Zero Trust Security Strategies and Guideline. 10.1007/978-3-031-09691-4_9.

- Garbis, Jason & Chapman, Jerry. (2021). Zero Trust Security: An Enterprise Guide. 10.1007/978-1-4842-6702-8.

- Sarkar, Sirshak & Choudhary, Gaurav & Shandilya, Shishir K & Hussain, Azath & Kim, Hwankuk. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability. 14. 11213. 10.3390/su141811213.

- Alawneh, Muntaha & Abbadi, Imad. (2023). Approaches for Zero Trust Adoption Based upon Organization Security Level. 10.1007/978-981-99-0272-9_36.

Cuestionario relacionado con administración de riesgos en tecnologías de información y comunicaciones para Big Data & Data.

- Cheng, Ruizhi & Chen, Songqing & Han, Bo. (2023). Towards Zero-trust Security for the Metaverse.