Sesión 10 : Marco de Evaluación de Riesgos

Introducción a la seguridad de aplicaciones y mejores prácticas en codificación #

Mauricio Sotelo

- Ingeniero de Seguridad Nivel III
- Seguidor de las buenas prácticas, marcos de trabajo y estándares de seguridad.
- Amo las actividades al aire libre y hacer todo con música de fondo.
- https://calendly.com/mauricio_sotelo

Recomendaciones importantes

Identifícate en Zoom usando tu nombre y apellido.

Silencia tu micrófono durante el curso.

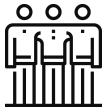
Utiliza el chat para hacer preguntas en la sección asignada para ello.

Centra tus preguntas en el tema presentado.

Mantén tu cámara encendida durante toda la sesión.

Academy Codigo de Conducta

Sé respetuoso, no hay preguntas o ideas malas.



Sé empático y paciente.

Sé cuidadoso con las palabras que eliges.

Objetivo

Al final de esta sesión podrás:

- Entender en qué consiste la evaluación de riesgos para identificar y priorizar posibles vulnerabilidades y amenazas dentro de la arquitectura de una aplicación.

Tabla de Contenidos

Conceptos.

¿ Qué ?

¿ Cómo es su Dinámica ?

Vulnerabilidad	En un sistema proporciona una oportunidad o camino para que una **amenaza** cause daño.
Amenaza	Sin una vulnerabilidad y la motivación correspondiente no representa un **riesgo** significativo.
Riesgo	Un riesgo se materializa cuando una amenaza con la **motivación** adecuada aprovecha una vulnerabilidad.

¿ En qué elemento existe la vulnerabilidad ?

¿ En qué elemento se encuentra la amenaza ?

¿ Cúal es el mayor riesgo ?

¿ Existe Vulnerabilidad, Amenaza y Riesgo ?

Modelando Amenazas

Caso Práctico: Sistema de Seguimiento de Contenedores Marítimos.

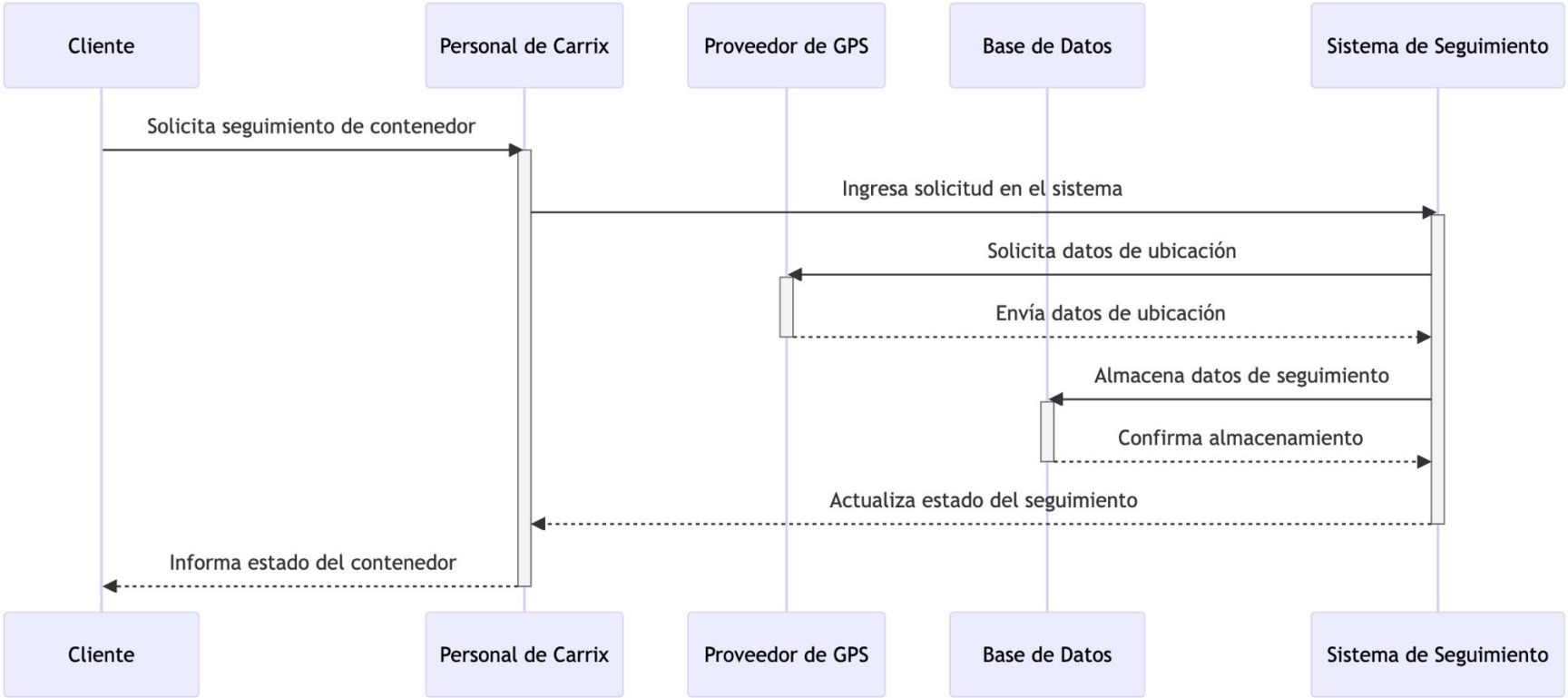
Contexto:

Una empresa de logística marítima desea implementar un nuevo sistema de seguimiento de contenedores para mejorar la eficiencia operativa y la seguridad. El sistema permitirá a los clientes y al personal de la empresa rastrear la ubicación y el estado de los contenedores en tiempo real.

Aplicación de los principios CID

ISO: 27001

Diagrama de Secuencia

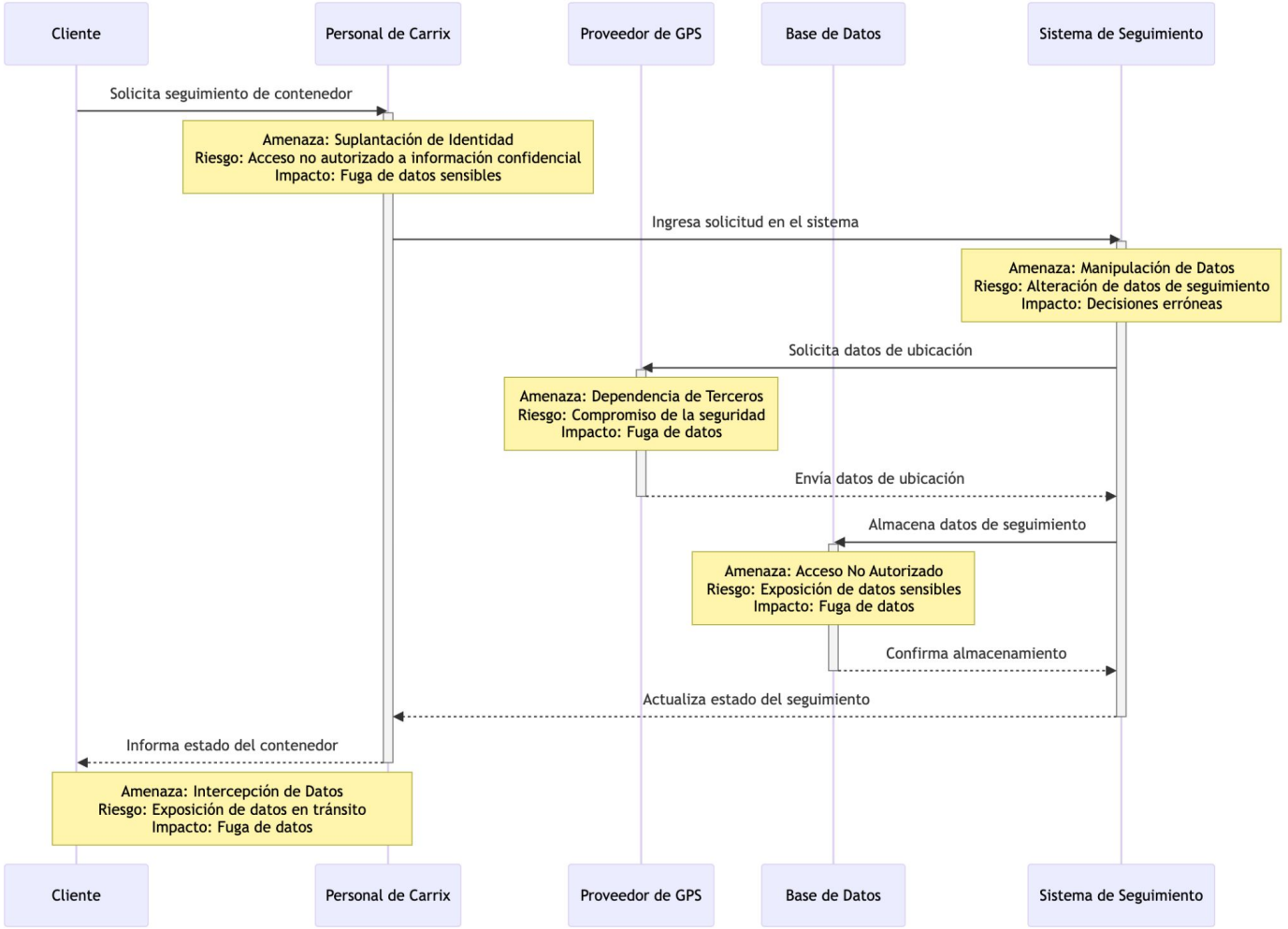


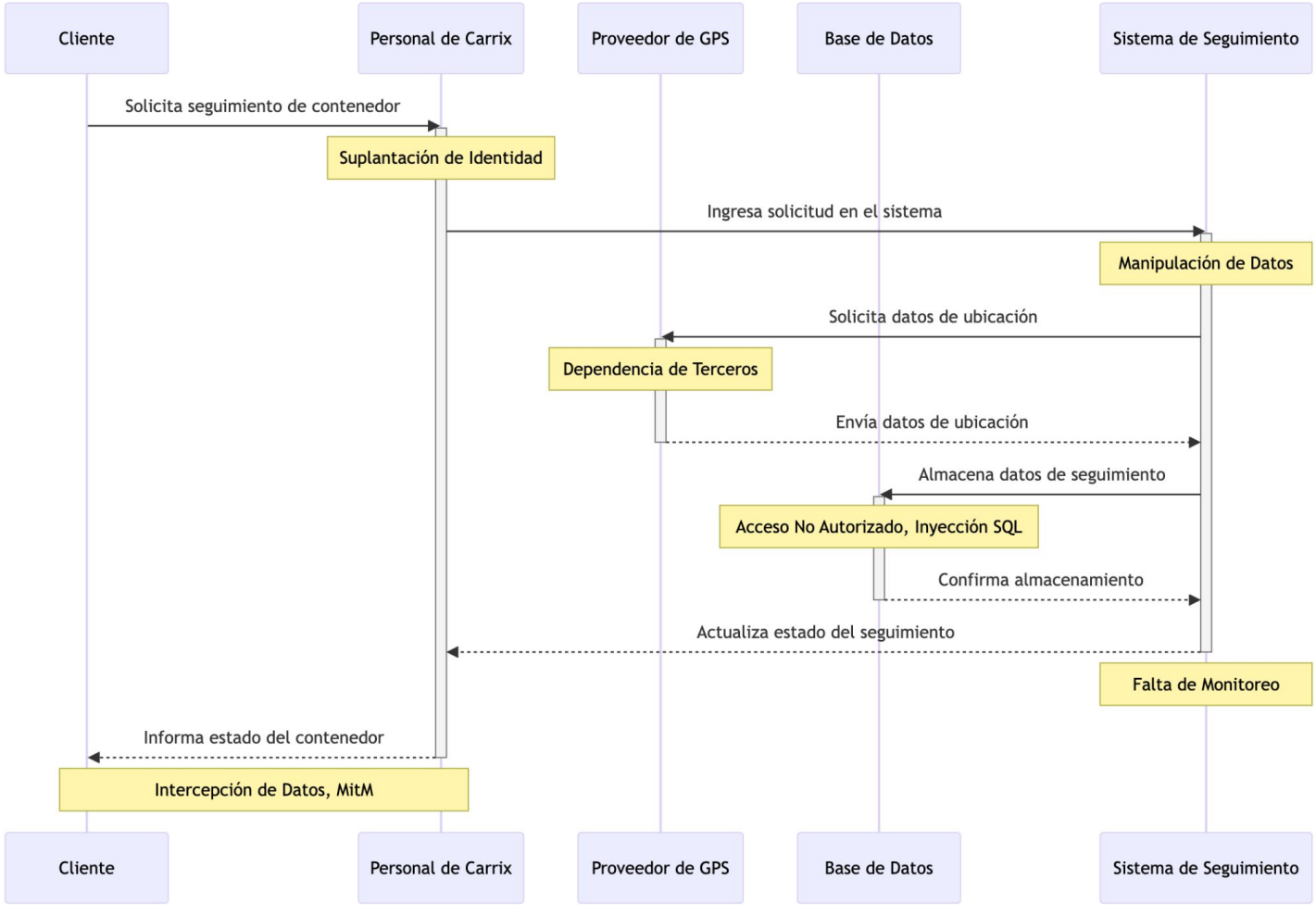
Enfoque centrado en el sistema

El objetivo es proteger todo el sistema, lo que incluye:

01	**Procesos**	• ¿ Cómo se recopilan y procesan los datos de seguimiento ? • ¿ Cómo se autentican los usuarios ? • ¿ Cómo se generan las alertas ?...
02	**Almacén de Datos**	• ¿ Dónde y cómo se almacenan los datos de seguimiento, , los detalles del cliente y la información del contenedor ?
03	**Flujo de Datos**	• ¿ Cómo se mueven los datos entre diferentes componentes del sistema ?
04	**Entidades Externas**	• Proveedores de servicios de GPS, bases de datos de clientes, sistemas de facturación, etc.
05	**Limites de Confianza**	• Qué partes del sistema son de confianza y cuáles no lo son.

		Amenazas Identificadas	Riesgos Identificados	Descripción
1	Procesos	✓	✓	• **Suplantación de Identidad (Spoofing):** Riesgo de que un atacante pueda hacerse pasar por un usuario legítimo. • **Manipulación de Datos:** Riesgo de alteración de los datos de seguimiento.
2	Almacén de Datos	✓	✓	• **Acceso No Autorizado:** Riesgo de que alguien pueda acceder a los datos sensibles almacenados. • **Inyección SQL:** Ataque para manipular la base de datos.
3	Flujo de Datos	✓	✓	• **Intercepción de Datos (Sniffing):** Riesgo de que los datos en tránsito puedan ser interceptados. • **Ataque de Hombre en el Medio (MitM):** Riesgo de intercepción y alteración de los datos durante su transmisión.
4	Entidades Externas	✓	✓	• **Dependencia de Terceros:** Riesgo asociado con la seguridad de los proveedores de servicios externos, como los de GPS. • **Fuga de Datos:** Riesgo de que los datos compartidos con entidades externas sean comprometidos.
5	Límites de Confianza	✓	✓	• **Acceso Interno No Autorizado:** Riesgo de que empleados o sistemas internos accedan a información que no deberían. • **Exfiltración de Datos:** Riesgo de que los datos se muevan desde un entorno de confianza a uno no confiable.
6	Recursos Lógicos	✓	✓	• **Vulnerabilidades en el Código Fuente:** Como inyección SQL, Cross-Site Scripting (XSS), etc. • **APIs No Seguras:** Riesgo de exposición de datos a través de APIs no seguras.





Descanso

5 minutos.

Evaluación y Tratamiento de Riesgos

ISO: 27005

Gestión de Riesgos de Seguridad de la Información.

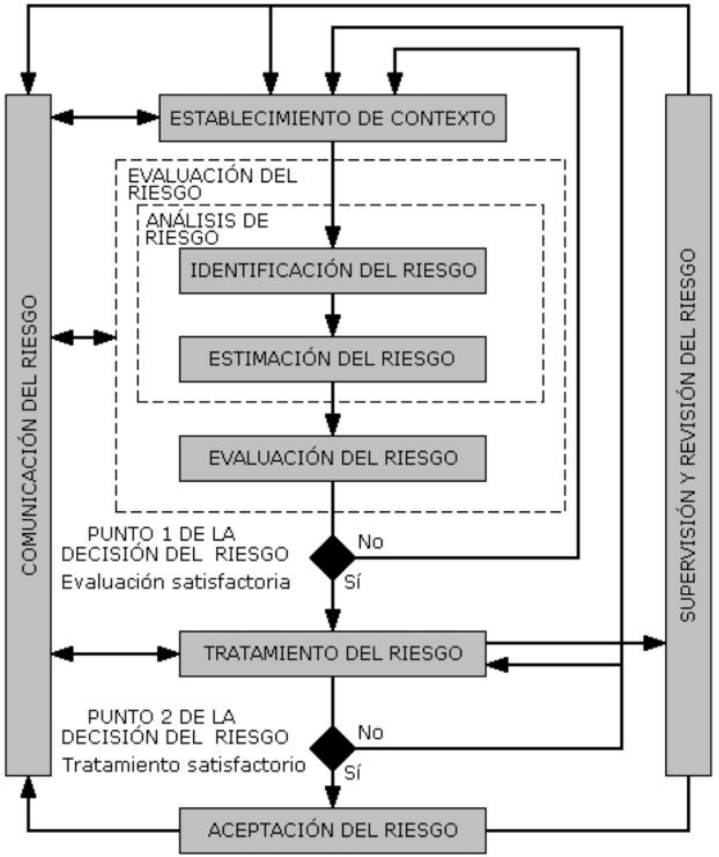
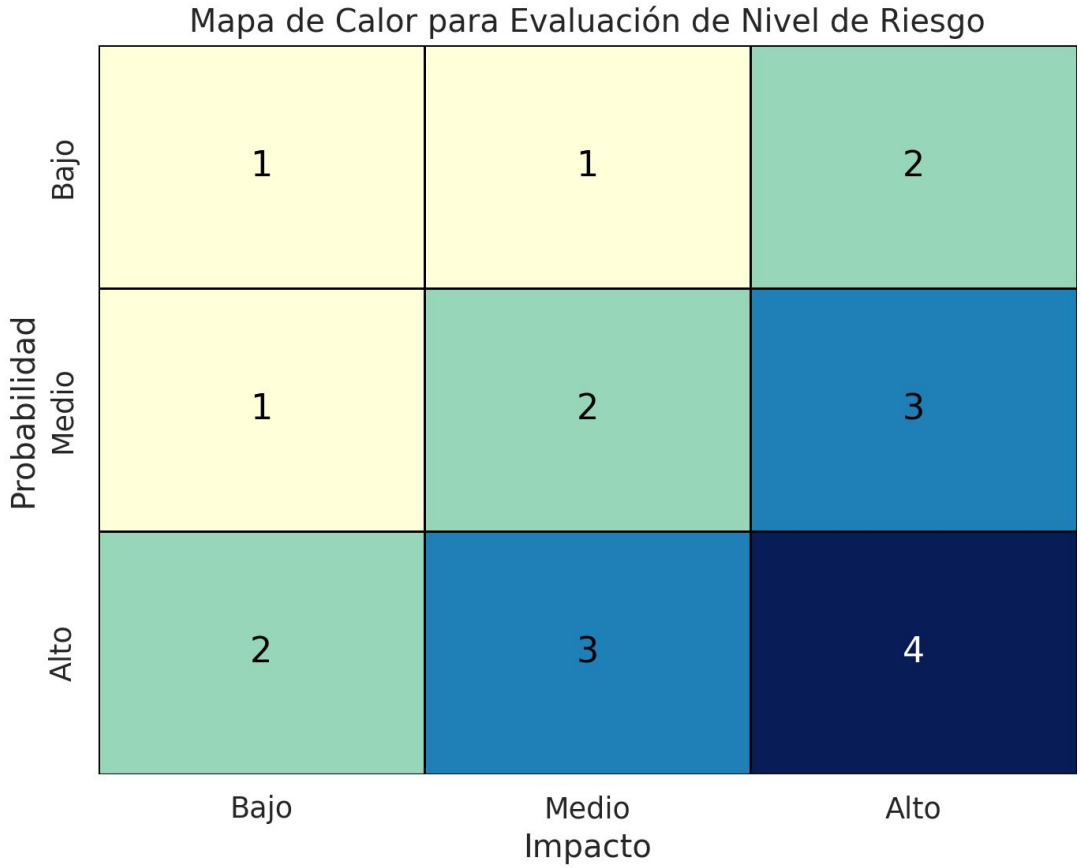


Ilustración 1: Proceso de para la Gestión del Riesgo ISO/IEC 27005:2018. Fuente: [9]

Convención de una matriz cualitativa de 3x3

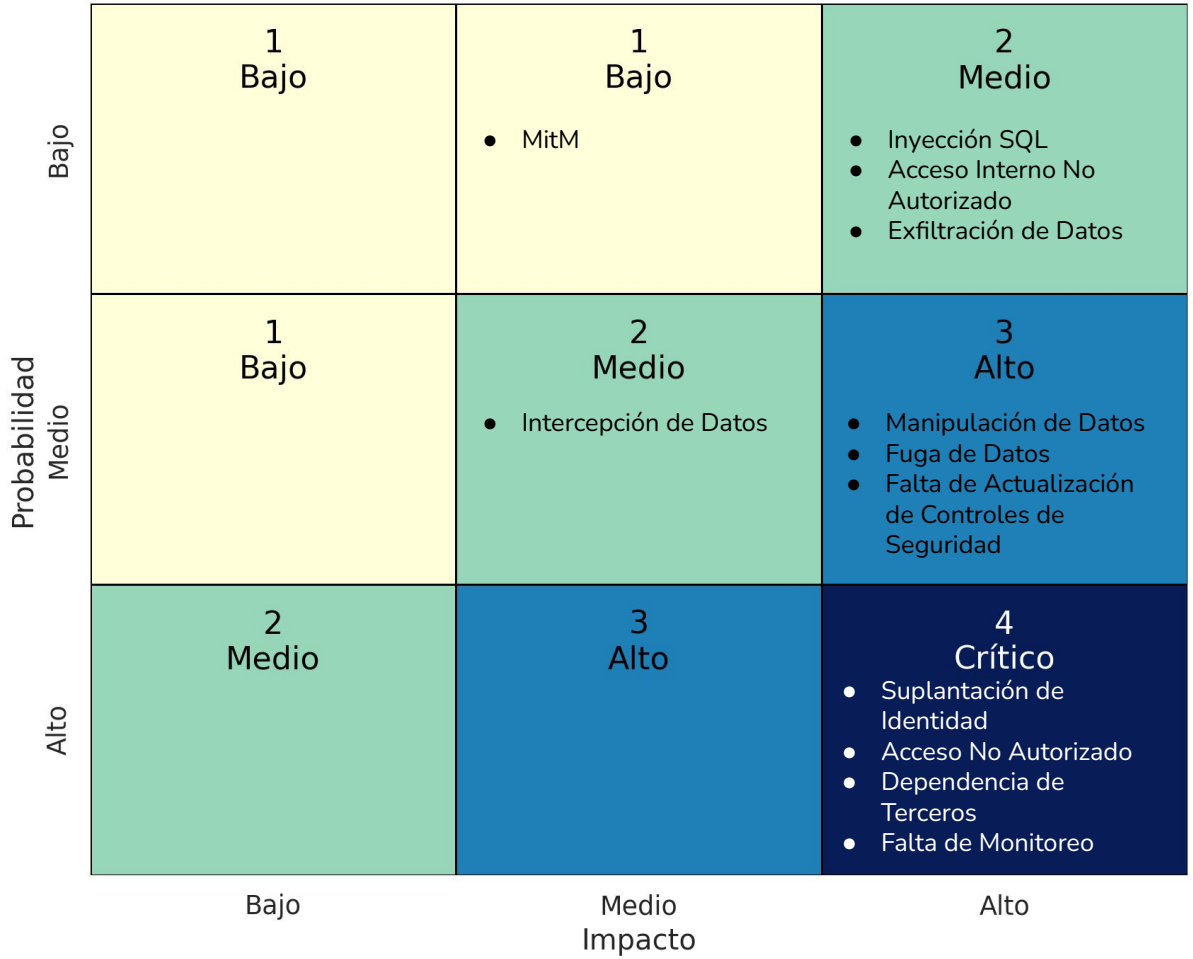
Niveles de Riesgo

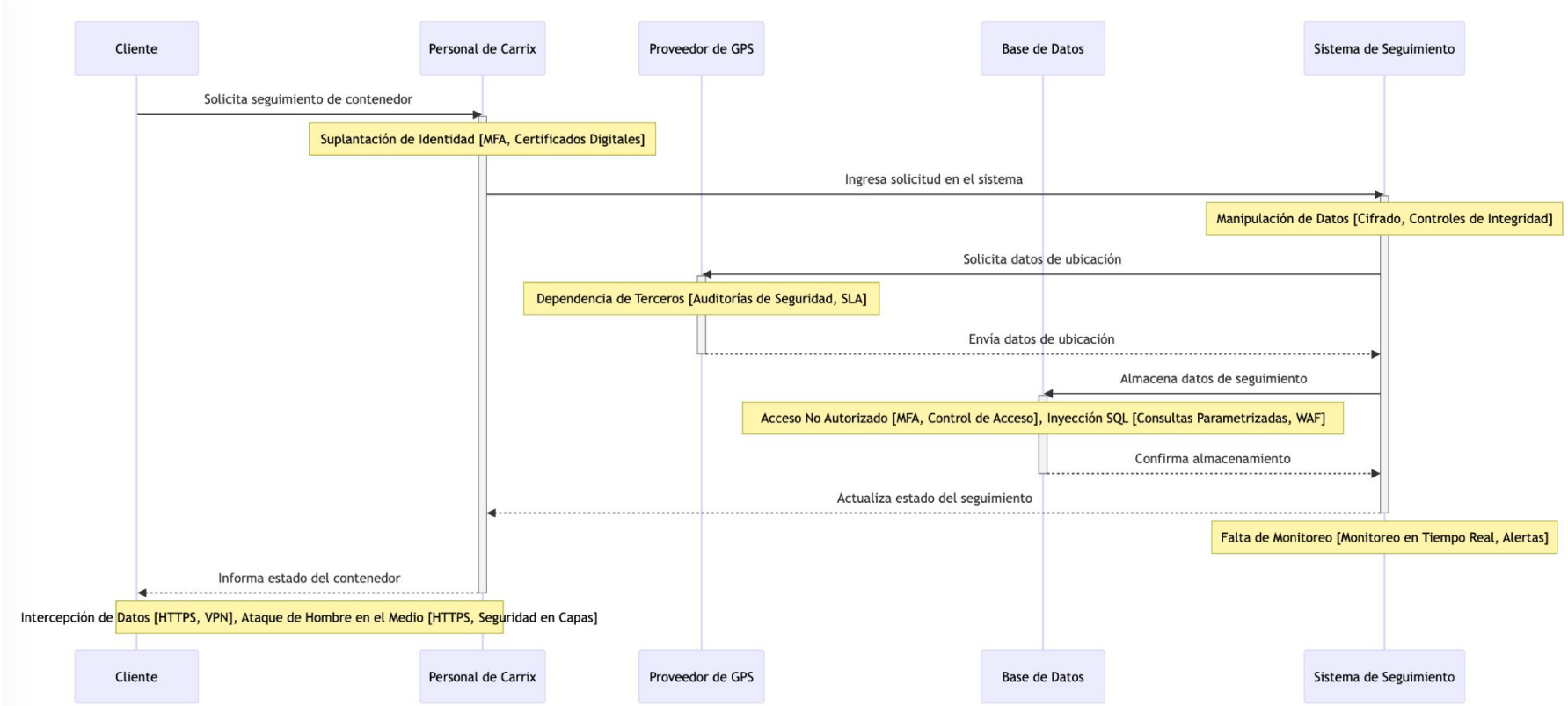
1: Bajo
2: Medio
3: Alto
4: Crítico



Amenaza	Probabilidad	Impacto	Nivel de Riesgo
Suplantación de Identidad	Alto	Alto	Crítico
Manipulación de Datos	Medio	Alto	Alto
Acceso No Autorizado	Alto	Alto	Crítico
Inyección SQL	Bajo	Alto	Medio
Intercepción de Datos	Medio	Medio	Medio
Ataque de Hombre en el Medio (MitM)	Bajo	Medio	Bajo
Dependencia de Terceros	Alto	Alto	Crítico
Fuga de Datos	Medio	Alto	Alto
Acceso Interno No Autorizado	Bajo	Alto	Medio
Falta de Monitoreo	Alto	Alto	Crítico
Falta de Actualización de Controles de Seguridad	Medio	Alto	Alto

Mapa de Calor para Evaluación de Nivel de Riesgo (Sin Amenazas)





Encuesta

Gracias.