Recomendaciones

Fecha	Autores
28/09/2024	Sandra González y Gonzalo Celaya

1. *Autenticación y Control de Acceso*

- **MFA:** Implementar autenticación multifactor para todos los usuarios, reduciendo accesos no autorizados.
- **RBAC:** Establecer acceso basado en roles para limitar la información sensible a los usuarios según sus funciones.
- **Monitoreo:** Usar herramientas para registrar actividades de usuarios y detectar comportamientos raros.

2. *Protección de Datos Sensibles*

- **Cifrado:** Asegurar cifrado de datos críticos en tránsito y en reposo.
- **Gestión de Claves:** Implementar rotación regular y almacenamiento seguro de claves.
- **Seguridad GPS:** Cifrar datos de ubicación para proteger información.

3. *Seguridad de API y Servicios Web*

- **Protección de API:** Reforzar la seguridad de las API con autenticación y cifrado.
- **Validación de Entradas:** Validar formularios en línea para prevenir ataques.
- **Gestión de Parches:** Mantener sistemas actualizados.

4. *Supervisión y Monitoreo Continuo*

- **SIEM:** Implementar sistemas para supervisar eventos de seguridad en tiempo real.
- **Monitoreo de Sistemas:** Vigilar sistemas críticos para detectar accesos no autorizados.

5. *Resiliencia Operativa*

- **Mitigación DDoS:** Usar servicios para proteger contra ataques DDoS.
- **Planes de Recuperación:** Desarrollar un Plan de Recuperación ante Desastres con copias de seguridad.
- **Redundancia:** Implementar balanceo de carga para asegurar disponibilidad.

6. *Capacitación del Personal*

- **Programas de Capacitación:** Entrenar a empleados sobre ciberseguridad y manejo de datos.
- **Simulaciones:** Realizar ejercicios para mejorar la respuesta ante incidentes.

7. *Auditorías de Seguridad*

- **Auditorías Periódicas:** Evaluar efectividad de medidas de seguridad e identificar vulnerabilidades.
- **Evaluación Continua de Riesgos:** Actualizar análisis de riesgos ante nuevas amenazas.