Parte 2

PLAN DE SEGURIDAD GRUPO 3

1. Identificación:
   - No realizan copias de información
   - Todos los usuarios pueden ver la información sensible

2. Toma las precauciones adecuadas:

   - Realizar copias de información
   - Los usuarios tendrán acceso sólo a los recursos que necesitan en el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue.
   - Certificar y autenticar la identidad de tu negocio con la tecnología SSL. Protege desde la información de las tarjetas de crédito hasta el proceso de pago brindado por terceros.
   - No guardar datos necesarios para completar otra transacción como la fecha de expiración o el código de verificación.

AUDITORIA

1. Realizar una auditoría del plan de seguridad de uno de los grupos en base a los escenarios planteados.
2. Buscar vulnerabilidades y fallas que faltaron solventar. Cuando se encuentre una falla, hay que explicar por qué es una vulnerabilidad y cómo podríamos atacar. A su vez, se debe explicar cómo solucionar dicha vulnerabilidad.

- Realizar capacitaciones a los empleados sobre los nuevos accesos restringidos, el uso de usuarios y contraseñas apropiadas. Establecer a qué tipo de información podrán acceder.
- Analizar las políticas respecto a las copias de seguridad, que sistemas se van a utilizar, frecuencia, si va a ser sincrónica y/o asincrónica.
- Falta de equipos UPS en caso de corte de luz