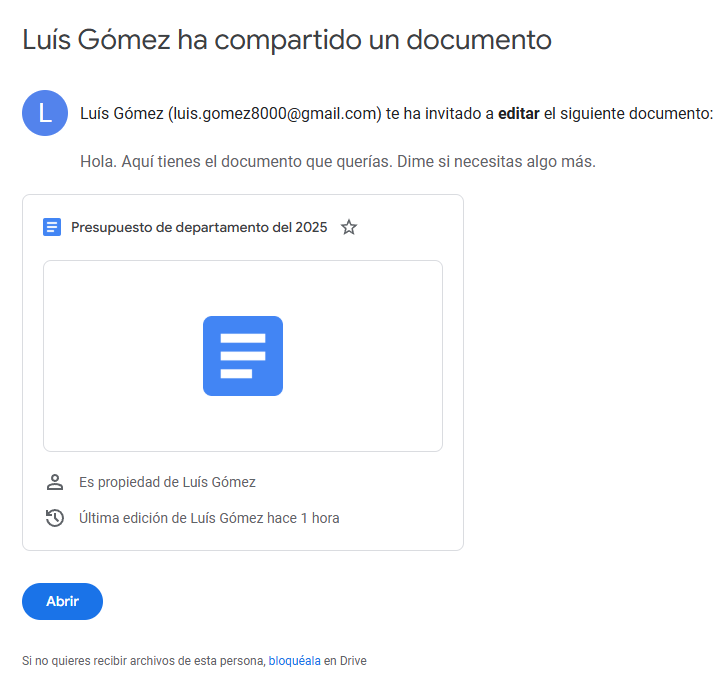
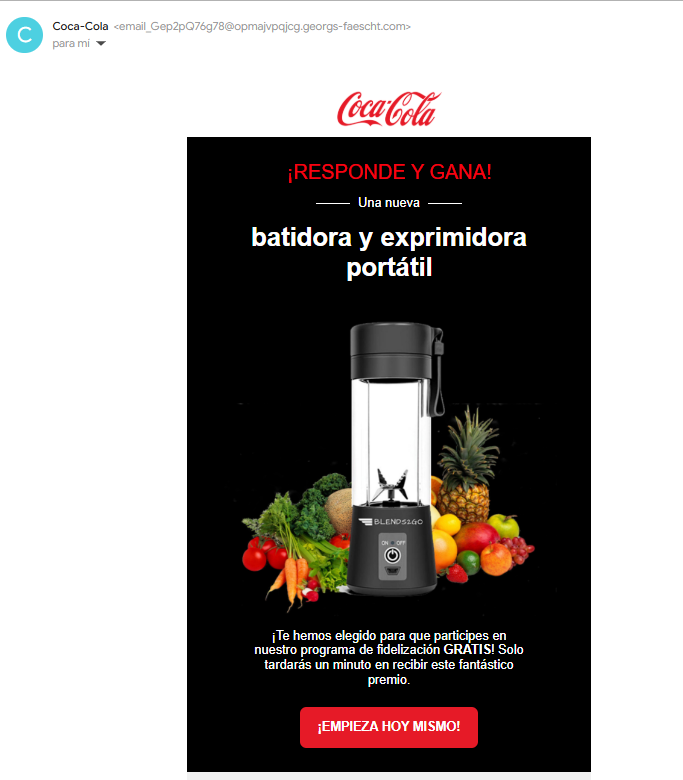
LABORATORIO 11)



Solución

1. Parámetros

* Correo malicioso = [Luis.gomez8000@gmail.com](mailto:Luis.gomez8000@gmail.com)
* Asuntos urgentes = no se tiene una certeza de que esa acción de edición sea esperada



1. Parámetros

* Dirección de correo electrónico= dice ser de Coca-Cola y no tiene ninguna relación ese correo con el correo oficial de la empresa de Coca-Cola🀄
* Enlaces sospechosos que redirigen página falsa=el enlace que se observa es falso se puede detectar porque es una de las tácticas mas usada para un ataque promocionar algo que sabes que no te ganaste diciendo que te lo ganaste gratis sin participar.
* Asunto urgente=que el remitente como pudo sacar la información de Gmail del receptor para enviarle ese link.
* HOJA DE RUTA PARA HACER MAS SEGURA UNA RED SOCIAL
* **Objetivo**: Identificar riesgos y establecer las bases de seguridad.
* **Auditoría de seguridad inicial**
  + Identificar vectores de ataque comunes: XSS, CSRF, inyecciones, etc.
  + Evaluar arquitectura y puntos débiles (frontend, backend, API).
* **Definición de políticas de seguridad**
  + Políticas de contraseñas seguras.
  + Gestión de sesiones.
  + Control de acceso por roles.
* **Evaluación de cumplimiento normativo**
  + GDPR, CCPA, LOPD, etc.
  + Términos de uso y políticas de privacidad claras.
* **Fase 2: Fortalecimiento de Autenticación y Autorización**

**Objetivo**: Asegurar la identidad de los usuarios y proteger los accesos.

* **Autenticación robusta**
  + Implementar autenticación multifactor (2FA).
  + Limitar intentos de inicio de sesión.
  + Uso de tokens seguros (JWT, OAuth).
* **Gestión de sesiones**
  + Expiración y renovación segura de tokens.
  + Invalidación de sesión tras cambio de credenciales.
* **Autorización granular**
  + Control de acceso basado en roles (RBAC).
  + Evitar exposición de endpoints no autorizados.
* **Fase 3: Protección de Datos del Usuario**

**Objetivo**: Asegurar la privacidad y confidencialidad de la información.

* **Cifrado**
  + Cifrado de datos en tránsito (HTTPS).
  + Cifrado de datos en reposo (AES, bcrypt para contraseñas).
* **Minimización de datos**
  + No recolectar más datos de los necesarios.
* **Anonimización y pseudonimización** de datos sensibles en análisis o backups.
* **Fase 4: Defensa ante Ataques Comunes**

**Objetivo**: Blindar la aplicación ante vulnerabilidades típicas.

* **Validación y sanitización de entradas**
  + Prevenir XSS, SQLi, SSRF, etc.
* **Protección contra CSRF**
  + Uso de tokens antifalsificación.
* **Subida de archivos**
  + Validar extensiones, tamaño, y escanear con antivirus.
* **Tasa de peticiones**
  + Implementar rate-limiting y CAPTCHA en formularios críticos.
* **Fase 5: Monitoreo y Respuesta**

**Objetivo**: Detectar incidentes y responder rápidamente.

* **Logging centralizado**
  + Registrar eventos clave: inicios de sesión, cambios de datos, errores, etc.
* **Sistemas de detección de intrusos (IDS)**
  + Detección de patrones anómalos.
* **Alertas en tiempo real**
  + Para actividades sospechosas o accesos inusuales.
* **Planes de respuesta a incidentes**
  + Procedimientos para brechas de seguridad.
* **Fase 6: Mantenimiento Continuo y Mejora**

**Objetivo**: Mantener la seguridad a lo largo del tiempo.

* **Actualización periódica**
  + Parcheo de dependencias, frameworks, sistemas operativos.
* **Pentesting regular**
  + Simular ataques para descubrir nuevas vulnerabilidades.
* **Capacitación al equipo**
  + Conciencia sobre ingeniería social, phishing, y mejores prácticas de codificación segura.