Laboratorio # 4

Laboratorio 4: Ciberseguridad en el sector comercio electrónico

Nombre de la Empresa: Distribuciones camilo   
Perfil: Empresa pequeña que vende productos orgánicos por internet.  
Objetivo del laboratorio: Fortalecer la seguridad de la información, responder ante incidentes y diseñar un plan de recuperación.

**1. Identificación de Activos Críticos**

Activos Críticos Identificados:

Plataforma de comercio electrónico (sitio web)

Base de datos de usuarios y pedidos

Sistema de facturación

Servicios de correo para atención al cliente

Aplicación móvil (Android/iOS)

Clasificación por Criticidad:

| Activo | Nivel de Criticidad |
| --- | --- |
| Base de datos de usuarios | Alta |
| Sitio web de ventas | Alta |
| Aplicación móvil | Media |
| Sistema de facturación | Alta |
| Correos de atención al cliente | Media |

**2. Análisis de Amenazas y Riesgos**

Amenazas Identificadas:

Phishing dirigido a clientes y empleados

Ransomware en el servidor

DDoS al sitio web

Acceso no autorizado a la base de datos

Evaluación de Riesgos:

| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| --- | --- | --- | --- | --- |
| Base de datos | Acceso no autorizado | Alta | Alta | Crítico |
| Plataforma de pagos | Phishing | Alta | Alta | Crítico |
| Servidor web | DDoS | Media | Media | Alto |
| Correos corporativos | Phishing | Alta | Media | Alto |

**3. Formación del Equipo de Respuesta a Incidentes (ERI)**

Miembros del Equipo:

Coordinador de Incidentes: Camilo Gutierrez

Técnico de Sistemas: Stiven Orozco

Responsable Legal: Camilo Brito

Comunicación Interna: Mario Sosa

Lista de Contactos de Emergencia:

CERT Colombia: cert@colCERT.co

Soporte de Hosting: Camilogutierrez@hosting.com

Gerencia: gerencia@ecomercado.co

**4. Desarrollo de Procedimientos de Detección**

Procedimientos Básicos:

Activar monitoreo de logs en el servidor (fail2ban + logwatch)

Configurar alertas automáticas para accesos sospechosos

Auditoría de usuarios mensualmente

Uso de antivirus actualizado con escaneo semanal

**5. Elaboración del Plan de Contención**

Pasos del Plan:

Aislar el servidor afectado de la red

Detener servicios críticos temporalmente

Activar backup en servidor alternativo

Notificar al ERI y al proveedor de seguridad

Mantener informados a los clientes por correo oficial

🔁 6. Plan de Recuperación y Continuidad del Negocio

Recuperación:

Restaurar backups automáticos diarios

Verificar integridad con hash MD5

Pruebas funcionales post-recuperación

Continuidad del Negocio:

Sitio web alternativo en servidor espejo

Soporte telefónico mientras se recupera el sitio

Comunicación proactiva con clientes y proveedores

🧠 7. Conclusiones y Preguntas

Lecciones Aprendidas:

La prevención es más barata que la recuperación

El monitoreo continuo es esencial

Los roles bien definidos aceleran la respuesta

📝 8. Evaluación del Taller

Retroalimentación:

Taller práctico y aplicable

Se sugiere incluir simulaciones con herramientas reales

Excelente guía para negocios pequeños

✔️ Checklist Final

Identificación de activos críticos

Evaluación de riesgos

Formación del ERI

Procedimientos de detección definidos

Plan de contención elaborado

Plan de recuperación redactado

Conclusiones y evaluación completadas

Documento subido al GitHub como PDF