CARLOS ARIAS – LEONIS DIAZ – SAUL HERNANDEZ

"Tienda Click"

Perfil: "Tienda Click" es una empresa pequeña de comercio electrónico dedicada a la venta de productos tecnológicos y accesorios. Opera exclusivamente en línea, procesando pagos a través de su sitio web y plataformas de terceros. Su reputación depende en gran medida de la seguridad de los datos de sus clientes y la disponibilidad de sus servicios digitales.

1. Identificación de Activos Críticos

¿Qué son activos críticos?

Son recursos fundamentales para la operación y continuidad de la empresa. Su compromiso puede causar pérdidas económicas, legales o de reputación.

Activo	Prioridad	Motivo
Base de datos de clientes	Alta	Compromiso puede afectar la privacidad y causar sanciones legales.
Sistema de pagos	Alta	Su falla impide transacciones y genera pérdida de ingresos.
Sitio web	Alta	Es el canal principal de operación.
Servidor web	Media	Importante, pero puede ser reemplazado si se tienen backups.
Backups	Alta	Permiten recuperación en caso de ataque o fallo.
Cuentas Administrativas	Alta	Pueden ser punto de entrada para atacantes.
Proveedores/API	Media	Integra servicios de mensajería, inventario y pagos.

Análisis de Amenazas y Riesgos

Amenazas	Descripcion	Posible Impacto
Phishing	Intento de engañar al usuario para que entregue información confidencial (como contraseñas o datos bancarios) mediante correos o mensajes falsos que aparentan ser de fuentes confiables.	Robo de accesos, suplantación de identidad, acceso a cuentas bancarias
Malware	Programas diseñados para dañar sistemas, espiar al usuario o robar información.	Compromiso de seguridad interna o por archivos de proveedores

	Incluye virus, troyanos, spyware, etc	
Ransomware	Tipo de malware que bloquea el acceso a los sistemas o datos y exige un pago (rescate) para liberarlos. Común en ataques a pequeñas empresas.	Bloqueo de sistemas, pérdidas económicas
Artaque DDoS	Colapsan un sitio web o servidor enviando un alto volumen de tráfico falso, impidiendo el acceso a usuarios legítimos.	Caída del sitio o APIs, pérdida de confianza de clientes

En que afectaría:

Nombre	Descripcion
Base de datos de clientes	Phishing, Ransomware
Sistema de pagos	Phishing, Malware, Interceptación de datos
Sitio web	DDoS, Ransonware
Servidor web	DDoS, Ransonware
Backups	Ransomware (si están conectados en red)
Cuentas Administrativas	Phising, Malware
Proveedores/API	Phishing (falsos correos del proveedor), DDoS a servicios externos, brechas en terceros.

3. Formación del Equipo de Respuesta a Incidentes

Nombre	Rol Asignado	Funcion
Carlos Arias Gallo	Especialista técnico	Contención, análisis de malware, restauración de sistemas.
Leonis	Coordinador del equipo y comunicación	Dirige el proceso, elabora comunicados internos y externos.
Saul Hernandez	Encargado legal y auditoría	Evalúa notificación a entidades legales, documenta el proceso.

CARLOS ARIAS – LEONIS DIAZ – SAUL HERNANDEZ

Listado de Emergencias:

Contacto / Rol	Nombre / Organizacion	Medio de Contacto	Disponibilidad
Proveedor Hosting		soporte@hostsecure.com	24/7
Soporte de Pasarela de Pagos	PayFast	helppagos@payfast.com	Lunes a Sabado
Abogado externo en Ciberseguridad	Dr. Andres Duarte	Andresduarte2@gmail.com	8:00 am – 12:00 pm

4. Desarrollo de Procedimientos de Detección

Activo	¿Qué se monitorea?	Herramienta	Uso
Base de datos de clientes	Accesos inusuales, cambios inesperados	MySQL Logs / phpMyAdmin / Logwatch	Revisa accesos y operaciones en la base de datos
Cuentas Adminstrativas	Intentos de login sospechosos, cambios de permisos	Fail2Ban / Authlog Viewer	Bloquea IPs maliciosas y alerta sobre intentos de acceso fallidos
Sitio web	Disponibilidad, caídas, lentitud	UptimeRobot	Verifica que el sitio web esté disponible
Backups	Integridad, frecuencia y éxito del backup	Duplicati / Cron Logs	Verifica si los backups se están realizando correctamente
Proveedores y servicios externos (API, pasarela de pago)	Tiempo de respuesta, errores	Pingdom / Postman Monitors	Detecta fallas en conexión o lentitud con servicios de terceros

CARLOS ARIAS – LEONIS DIAZ – SAUL HERNANDEZ

5. Elaboración del Plan de Contención

Un ataque de *ransomware* ha cifrado la base de datos de clientes y el sitio web muestra una pantalla de “rescate”.

Plan de Contención Rápida

Paso	Accion	Responsable
Detección	Revisión de alertas de UptimeRobot y bloqueo de acceso web	Carlos
Aislamiento	Desconectar base de datos del servidor y desactivar pasarela de pago	Carlos
Comunicación interna	Informar inmediatamente a Leonis y Saul	Carlos
Preservación de evidencias	Guardar logs, capturas de pantalla y mensajes del atacante	Saul
Activacion de Respaldo	Restaurar último backup funcional verificado	Saul
Notificacion a Proveedores	Contactar hosting y pasarela de pago	Leonis
Comunicación a clientes	Enviar comunicado por email y redes sociales	Leonis

CARLOS ARIAS – LEONIS DIAZ – SAUL HERNANDEZ

6. Plan de Recuperación y Continuidad del Negocio

La base de datos fue cifrada por un ransomware y el sitio web estuvo inactivo por 6 horas. Tienes respaldo en la nube de hace 24 horas.

Fase	Acción específica	Herramienta / Medio	Responsable
Verificación	Confirmar qué datos están comprometidos	phpMyAdmin, logs	Carlos
Restauración de datos	Usar backups seguros para recuperar la información	Duplicati / Copia local y en Drive	Saul
Revisión del sistema	Asegurar que no queden rastros del ataque	Antivirus, escaneo manual	Carlos
Comunicación	Informar a clientes sobre el restablecimiento	Email, redes sociales	Leonis
Reanudación parcial	Activar sitio web con acceso limitado	Hosting / Cloudflare	Carlos
Prueba de funcionamiento	Confirmar que todo opera correctamente	Acceso test, verificación manual	Equipo
Reporte final	Documentar lo ocurrido y medidas tomadas	Informe escrito	Saul

CARLOS ARIAS – LEONIS DIAZ – SAUL HERNANDEZ

7. Conclusiones principales del taller:

1. **Identificación de Activos Críticos:**
    - Se reconocieron los activos esenciales como base de datos de clientes, sitio web, y proveedores.
    - Se priorizó la protección de la información sensible.
2. **Reconocimiento de Amenazas:**
    - Se analizaron amenazas comunes como phishing, malware y DDoS.
    - Se relacionaron estas amenazas con los activos vulnerables de la empresa.
3. **Formación del Equipo de Respuesta a Incidentes:**
    - Se asignaron roles claros: comunicación, técnico, y legal.
    - Se definieron contactos de emergencia y responsabilidades.
4. **Plan de Contención de Incidentes:**
    - Se elaboró un protocolo para actuar rápidamente ante ataques como ransomware.
    - Se documentó un procedimiento paso a paso para minimizar daños.
5. **Monitoreo y Herramientas:**
    - Se establecieron herramientas como UptimeRobot, Duplicati y Cloudflare.
    - Se definió una rutina y responsables para el seguimiento.
6. **Recuperación y Continuidad del Negocio:**
    - Se construyó un plan para restaurar sistemas y continuar operando.
    - Se destacaron acciones inmediatas, comunicación con clientes y uso de respaldos.