Perfil: empresa pequeña dedicada al comercio electrónico que almacena datos de los usuarios como tarjetas de crédito o debito y cuentas de usuario

Identificación de activos críticos

Los activos críticos son aquellos recursos o sistemas cuya pérdida o compromiso puede afectar gravemente la operatividad del negocio o la confianza del cliente.
los activos críticos que se pueden identificar son:
base de datos de los clientes, sistema de pagos, servidor web; siendo todos esto de un alto nivel de criticidad.
sistema de correos y pagina de administración con una criticidad de nivel medio

Análisis de amenazas y riesgos

Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Base de datos de clientes	Phishing	Alta	Alto	Alto
Servidor web	DDoS	Media	Alto	Alto
Sistema de pagos	Malware	Alta	Muy alto	Alto
Sistema de correos	Suplantación	Media	Medio	Medio
Página de administración	Ransomware	Alta	Alto	Alto

En este punto se prioriza la protección de la base de datos, servidor web y sistema de pagos debido a su alto riesgo y criticidad.

Formación del Equipo de Respuesta a Incidentes

Roles definidos:
Responsable de Comunicaciones: Roberto Fernández – Comunica a clientes y autoridades
Técnico de Sistemas: Jhonnier Rodríguez – Encargado de análisis técnico y contención.
Lista de contactos de emergencia:
Proveedor de hosting: soporte@hostingempresa.com

Consultor en ciberseguridad: consultor@seguridaddigital.com
Autoridades: Policía Cibernética

Elaboración del Plan de Contención

Plan para las primeras 24 horas:

- Detectar y aislar el sistema afectado.
- Desconectar temporalmente la red si es necesario.
- Ejecutar scripts de diagnóstico para determinar el tipo de ataque.
- Notificar al equipo de respuesta inmediatamente.
- Iniciar bitácora del incidente para registrar acciones.
- Informar a los usuarios si hubo fuga de datos.

Plan de Recuperación y Continuidad del Negocio

- Restauración desde copias de seguridad (almacenadas en la nube y localmente).
- Verificación de integridad de los datos recuperados.
- Notificación transparente a los clientes explicando el incidente.
- Prueba de funcionamiento del sistema antes de volver a estar en línea.
- Evaluación post mortem del incidente para mejorar los controles.