UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA PARACENTRAL

INGENIERÍA DE SISTEMAS INFORMÁTICOS

ANALISIS DE RIESGOS INFORMATICOS

Presentado por:	**Carnet**
Br. Edgar Giovanni Gómez Cerón	GC21028
Br. Javier Eduardo Hernández Sánchez	HS21002

Docente:

Ing. Eliseo Eulises Romero Ayala

San Vicente, 29 de septiembre de 2025

Empresa: Almacenes SIMAN SA de CV

Contenido

Área de ciberseguridad

Misión

Proteger la información y los activos digitales garantizando la confidencialidad, integridad y disponibilidad, mediante soluciones innovadoras de ciberseguridad y asesoría especializada.

Visión

Ser líderes regionales en ciberseguridad, anticipando amenazas y promoviendo una cultura digital segura que impulse la transformación sostenible.

Objetivos estratégicos

Fortalecer la protección de la información y activos críticos.

Implementar y mantener controles de seguridad basados en normas internacionales (ISO 27001/27002).

Garantizar la confidencialidad, integridad y disponibilidad de los datos de clientes y de la organización.

Prevenir, detectar y responder a incidentes de seguridad.

Establecer un Centro de Operaciones de Seguridad (SOC) interno con monitoreo 24/7.

Reducir el tiempo de detección y respuesta ante incidentes críticos en al menos un 30% anual.

Fomentar una cultura de ciberseguridad en la organización y en los clientes.

Diseñar programas de capacitación continua para colaboradores y clientes.

Realizar simulaciones de ataques (phishing, ransomware) para medir la preparación del personal.

Asegurar el cumplimiento normativo y regulatorio.

Mantener la conformidad con la ISO 27001, GDPR, PCI-DSS u otras normativas aplicables.

Implementar auditorías internas y externas periódicas para garantizar la efectividad de los controles.

Impulsar la innovación en ciberseguridad.

Integrar inteligencia artificial y automatización en procesos de seguridad (ej. detección de anomalías).

Evaluar e implementar tecnologías emergentes (Zero Trust, DevSecOps, seguridad en la nube).

Gestionar y mitigar riesgos tecnológicos.

Elaborar y actualizar periódicamente un mapa de riesgos cibernéticos.

Definir planes de continuidad del negocio y recuperación ante desastres (BCP/DRP) probados al menos 1 vez al año.

Contexto de la organización

Descripción de la organización

Almacenes SIMAN es uno de los almacenes más grande de El Salvador, dedicados a la comercialización de productos de masivos en el país, cuenta con una plataforma digital de comercio electrónico, en los últimos años la organización ha invertido fuertemente en transformación digital, incorporando plataformas de e-commerce y aplicaciones móviles, donde se procesan datos sensibles de clientes como información personal, métodos de pago, sistemas de punto de venta (POS) en cada sucursal, conectados con la red central para control de inventarios y facturación, infraestructura tecnológica que incluye centros de datos, servidores, redes internas y sistemas de logística automatizada.

Este modelo de operación expone a Almacenes SIMAN a un entorno con múltiples riesgos tecnológicos y de ciberseguridad, como:

Robo o fuga de datos de clientes y transacciones financieras.

Ataques a los sistemas de comercio electrónico y POS.

Interrupciones operativas por incidentes de malware, ransomware o fallos de red.

Riesgos de cumplimiento normativo en la protección de datos personales y regulaciones del comercio digital.

Por ello, la organización ha identificado que el área de ciberseguridad es crítica para garantizar la confidencialidad, integridad y disponibilidad de la información, proteger sus operaciones comerciales y reputación corporativa, mantener la continuidad del negocio frente a incidentes de seguridad, asegurar el cumplimiento de normativas internacionales y locales en protección de datos y seguridad de la información.

Factores externos

Crecimiento y expansión: Almacenes SIMAN está haciendo inversiones grandes para abrir nuevas salas de venta este año y remodelar otras existentes.

Competencia y liderazgo de mercado: Tiene una cuota de mercado muy significativa, lo que lo convierte en objetivo visible para competidores y también para ataques (por ejemplo, fraudes, amenazas de reputación).

Regulatorio y social: Al trabajar con proveedores locales, marcas privadas, está sujeto a regulaciones de protección de datos, estándares de calidad.

Tendencias tecnológicas: Tiene presencia digital (app, tienda en línea), modernización de salas, eficiencia energética, automatización en compras de productos, remodelaciones con tecnologías sostenibles.

Factores internos

Infraestructura física: Tiene muchas salas de venta, cadena de suministros con sus proveedores lo cual lleva a una logística extensa.

Operaciones digitales: Tienen plataforma de ecommerce, aplicaciones, sistemas de punto de venta (POS), sistemas de compras, logística, etc. Esto implica muchos activos de tecnologías de información que deben protegerse.

Cultura empresarial: Enfocada en calidad, servicio al cliente, responsabilidad social.

Partes interesadas

Clientes: Consumidores de productos de supermercado, usuarios de la tienda en línea, clientes de marcas privadas.

Empleados: Personal de tiendas, administración, logística, y producción.

Proveedores: Empresas nacionales y extranjeras que fabrican productos, proveedoras de marcas privadas.

Socios tecnológicos: Proveedores de sistemas informáticos, plataformas de ecommerce, empresas de seguridad, servicios de infraestructura (redes, energía, etc.).

Reguladores: Entidades que supervisan alimentación, salud, protección al consumidor, protección de datos, normas de comercio.

Comunidad y medios: La marca tiene alto reconocimiento público; temas de reputación son importantes.

Riesgos IT para Almacenes SIMAN

- **Computadoras y laptops de empleados**

Riesgo: Robo de información sensible por malware, keyloggers o pérdida de equipos.

Impacto: Alto (pueden filtrar credenciales o datos financieros).

Probabilidad: Media.

Controles recomendados: Antivirus EDR, cifrado de disco y políticas de uso.

- **Reportes de ventas, proyecciones y hojas Excel**

Riesgo: Alteración de datos estratégicos que afecten decisiones.

Impacto: Alto porque puede afectar planeación y finanzas.

Probabilidad: Alta, se manipulan manualmente.

Controles recomendados: Control de versiones, permisos de acceso, almacenamiento en repositorio seguro (ej. SharePoint).

- **Base de datos**

Riesgo: Manipulación de precios en el sistema para fraude o competencia desleal.

Impacto: Muy alto, afecta ventas, ingresos y reputación.

Probabilidad: Media.

Controles recomendados: Segregación de funciones, monitoreo de cambios, auditorías periódicas, cifrado.

- **Facturas de ventas y compras**

Riesgo: Facturación falsa o alteración de comprobantes.

Impacto: Alto, fraude económico y problemas fiscales.

Probabilidad: Media.

Controles recomendados: Validación digital, firma electrónica, control de acceso a sistemas de facturación.

- **Correo corporativo**

Riesgo: Phishing y robo de credenciales que comprometa otros

Impacto: Muy alto.

Probabilidad: Alta, es el principal vector de ataque.

Controles recomendados: Filtros antispam, concienciación del usuario, MFA, simulaciones de phishing.

- **Plataforma de e-commerce y POS (integrado a la red central)**

Riesgo: Ataques de ransomware, DDoS o robo de datos de tarjetas.

Impacto: Crítico (interrumpe ventas y afecta clientes masivamente).

Probabilidad: Alta, es un objetivo común en retail.

Controles recomendados: PCI-DSS, WAF, monitoreo SOC 24/7, segmentación de red, backups en caliente

Plan de acción para mitigar riesgos de seguridad informática

- **Capacitación del personal en seguridad informática.**

Mitigar

Capacitación continua en ciberseguridad.

Simulacros de ataques de phishing.

Conciencia en manejo de información sensible.

Guías prácticas de uso.

Transferir

Externalizar parte de la capacitación.

Seguros de responsabilidad digital para errores humanos.

Eliminar

Procesos manuales inseguros.

Dependencia de la memoria del empleado.

Uso de capacitación puntual única.

- **Computadoras y laptops de empleado (ventas, compras).**

Mitigar

Implementar EDR/antivirus centralizado con monitoreo.

Forzar cifrado completo de disco (BitLocker, FileVault).

Aplicar MFA en sistemas sensibles.

Políticas de uso: prohibir descargas no autorizadas, bloqueo de USB.

Transferir

Contratar ciberseguro corporativo que cubra fuga de datos.

Eliminar

Sustituir laptops con VDI (escritorios virtuales), donde no quede información local.

- **Impresoras de facturas y recibos.**

Mitigar

Implementar impresión segura con PIN/tarjeta.

Registro y auditoría de uso de impresión.

Capacitación sobre destrucción segura de documentos (trituradoras certificadas).

Transferir

Contratar servicio externo de destrucción de papel con certificación ISO 27001.

Eliminar

Migrar facturación 100% digital (XML/PDF firmados).

- **Reportes de ventas, proyecciones y hojas Excel.**

Mitigar

Centralizar en SharePoint/OneDrive con control de versiones.

Definir roles y permisos de acceso (lectura/escritura).

Capacitación en buenas prácticas de manipulación de datos.

Transferir

Respaldos gestionados en nube certificada (ISO 27001, SOC 2).

Eliminar

Migrar cálculos a BI corporativo (ej. Power BI con acceso controlado), evitando archivos manuales.

- **Base de datos.**

Mitigar

Segregación de funciones: separar usuarios de consulta, edición y auditoría.

Registro y monitoreo en tiempo real de cambios.

Cifrado en reposo y en tránsito.

Transferir

Auditorías externas de seguridad de base de datos.

Eliminar

Automatizar precios desde sistema central, sin edición manual.

- **Facturas de ventas y compras**

Mitigar

Validación contra SAT o sistema tributario oficial.

Firma electrónica avanzada en cada comprobante.

Restricción de accesos al sistema de facturación.

Transferir

Servicio de facturación electrónica con PAC certificado.

Eliminar

Prohibir el uso de facturas en papel (todo digital)

- **Correo corporativo**

Mitigar

Filtro antispam avanzado con sandboxing.

Capacitación continua en phishing con simulaciones.

MFA en acceso al correo.

Transferir

Ciberseguro que cubra phishing y ransomware.

Eliminar

Bloquear reenvío automático hacia correos externos.

- **Plataforma de e-commerce y POS**

Mitigar

Cumplimiento de PCI-DSS para pagos con tarjeta.

Implementar WAF y DDoS protection.

Segmentación de red (POS aislado del resto de la red).

Backups en caliente y pruebas de recuperación.

Transferir

Contratar SOC 24/7 y monitoreo gestionado (MSSP).

Eliminar

Retirar almacenamiento local de datos de tarjeta (usar tokenización del proveedor de pagos)

1 . Fecha de actualización	29/9/2025

No	2. Proceso	3.Propietario (ROLES)	4.Responsable (ROLES)	5. Nombre del activo (Caracterizacion del activo)	6. Descripcion / funcionalidad (Caracterizacion del activo)	7.Tipo (Caracterizacion del activo)
1	Ventas	Supervisor de ventas	Gerente	Sistema de punto de ventas	Es el software esencial para registrar ventas, aplicar descuentos, emitir facturas y controlar inventario en tiempo real.	Aplicaciones informáticos
2	Ventas	Gerente de ventas	Administrador de TI	Equipos informaticos y terminales de cobro	Soportan el proceso de ventas y agilizan la facturación.	Equipos informátic
3	Ventas	Gerente de ventas	Administrador de TI	Red corporativa	Permiten que las transacciones sean seguras, que se valide la información con bancos y que el sistema central registre todo.	Las redes de comunicaciones
4	Ventas	Gerente de ventas	Administrador de TI	Personal de ventas y cajeros	Interactúan directamente con los clientes y operan el POS, asegurando la experiencia de compra.	Personas
5	Ventas	Gerente de ventas	Administrador DBA	Base de datos	Contiene información de compras, historial de clientes, devoluciones, garantías y promociones aplicadas	Datos

Ventas | Compras

	Valor: . Confidencialida MA	A	M	B	MB	9. Integridad MA	A	M	B	MB	. Disponibilida MA	A	M	B	MB	11. Valor MA	A	M	B	MB	12. Atributos A1	A2	A3	A4	A5	A6	A7	13. Ubicación	. Electronic	15. Fisica	16. Vulnerabilidades	17. Amenazas	18. Controles Existentes	19. Controles a implementar
		1				1					1						1					1						Oficina de ventas		x	Se quede innaccesible	Se caiga la red	Control de acceso de usuarios	
os		1					1					1					1					1						Oficina de ventas		X	Acceso no autorizado por personal	Robos en la empresa	Cuentas de usuario y antivirus del sistemas operativos	Protección física adicional
			1				1				1						1				1							Departamentos de ventas		X	Acceso no autorizado por personal	Puertos abiertos y malas practicas de seguridad	Medianamente mantenimiento a las	Cerrar puertos y agregar seguridad a la red
		1					1							1				1			1							Oficina de ventas		X	pishing e ingenieria socia	Robo de información	Registros de usuarios	Imprimir codigo del reporte y usuario
	1					1					1					1					1							Servidor en la nube		X	Alteración de datos, acc	ciberataque, robo o perdida de inf	Acceso basado en roles, back	Cifrado de base de datos

1 . Fecha de actualización	29/9/2025

No	2. Proceso	3.Propietario (ROLES)	4.Responsable (ROLES)	5. Nombre del activo (Caracterizacion del activo)	6. Descripcion / funcionalidad (Caracterizacion del activo)	7.Tipo (Caracterizacion del activo)
1	Compras	Encargado de compras	Supervisor	Sistema de gestión de compra	Permite registrar, gestionar y aprobar órdenes de compra, controlando proveedores, precios y abastecimiento.	Aplicaciones informaticas
2	Compras	Encargado de compras	Analista de compras	Base de datos	Contiene información crítica como contratos, listas de precios, historial de compras y condiciones	Datos
3	Compras	Encargado de compras	Usuario compras	Equipos informaticos	Usados por el personal de compras para acceder al ERP y demás aplicaciones corporativas.	Equipos informáticos
4	Compras	Encargado de compras	Supervisor	Personal del area de compra	Los compradores y analistas que negocian, validan información y ejecutan las operaciones.	Personas
5	Compras	Encargado de compras	Supervisor	Red corporativa	Necesarios para conectar el sistema de compras con proveedores externos y con otros departamentos internos (finanzas, logística, almacén).	Las redes de comunicacion

Ventas | Compras

Valor																																	
. Confidencialida					9. Integridad					0. Disponibilida					11. Valor					12. Atributos							3. Ubicació	4. Electronic	15. Fisica	6. Vulnerabilidade	17. Amenazas	. Controles Existent	19. Controles a implementar
MA	A	M	B	MB	MA	A	M	B	MB	MA	A	M	B	MB	MA	A	M	B	MB	A1	A2	A3	A4	A5	A6	A7							
	1				1							1				1				1		1		1			Oficina de compras	x		Acceso no autorizado o perdida por fallos del sistema	Robos de información, modificación maliciosa	Acceso con usuario y contraseña, permisos por rol	cifrados y respaldos automaticos
1					1							1			1					1		1	1			1	Servidores en la nube	x		Fuga de información, corrupción de datos	Acceso indebido, ransomware	Restricciones de acceso, respaldos	Cifrado en tránsito/reposo, DLP
		1				1				1						1					1			1		1	Oficina compras	x	x	Fallos de hardware, falta de parches	Pérdida de datos, virus	Antivirus, firewall local	Control de inventario, reemplazo preventivo
	1					1					1					1				1		1			1		Area de compra	x		Pishing, suplementación	Fraude, fuga de información	Filtros antispam, capacitación	DMARC, DKIM, sensibilización periódica
1					1						1				1					1			1		1		Departamento de compras	x		Acceso indebido, manipulación	Puertos abiertos, mala infraestructura de red	Mantenimiento a la red una vez al mes	Cerrar puertos que esten abiertos, una infraestructu red mas limpia

Compras