UNIVERSIDAD PRIVADA
DOMINGO SAVIO

UNIVERSIADA PRIVADA DOMINGO SAVIO

FACULTAD DE INGENIERIA

AUDITORIA INTEGRAL SISTEMA DE VENTAS

Carrera: Ingeniería en Sistemas

Materia: Auditoria de Sistemas

Docente: Ing. Yolanda Zabala Moron

Integrantes:

- Mario Barba Umalla
- José Miguel Fanola
- Wilfredo Mamani Vera
- Franz Alberto Huanca Quispe
- Luz Madelen Lazaro Flores

Santa Cruz de la Sierra – Bolivia

09/07/2025

Índice

1. INTRODUCCION 3

2. OBJETIVOS 4

2.1. Objetivo General 4

2.2. Objetivos Específicos 4

4. DIAGNOTICO 5

4.1. Investigación Preliminar 5

4.2. Selección de auditores 5

4.3. Matriz de Identificación 6

4.4. Plan de auditoria 7

5. PLAN DE TRABAJO 8

6. CONCLUSION 8

1. INTRODUCCION

La auditoría integral de sistemas de ventas en supermercados representa una evaluación crítica y sistémica de los procesos, controles y tecnologías que sustentan las operaciones comerciales del sector retail. En el contexto actual de transformación digital, donde los supermercados procesan miles de transacciones diarias a través de sistemas de punto de venta (POS) integrados, la implementación de un marco normativo robusto se vuelve fundamental para garantizar la seguridad, eficiencia y confiabilidad operacional.

La presente auditoría se fundamenta en la aplicación de la Guía Técnica 27002 que establece controles organizados en cuatro categorías principales: controles organizacionales, controles de personas, controles físicos y controles tecnológicos. Esta nueva estructura normativa, actualizada en octubre de 2022, responde a los desafíos modernos de ciberseguridad y protección de la información en el entorno comercial actual.

Los sistemas de ventas de supermercados enfrentan riesgos específicos que requieren evaluación especializada: fraude interno, interrupciones en la cadena de suministro, ciberataques, fallas en sistemas POS y pérdidas de inventario. La matriz de riesgos aplicada al sector retail identifica vulnerabilidades críticas como el acceso no autorizado a sistemas, errores en transacciones, pérdidas por hurto e incumplimiento normativo.

La auditoría integral abarca desde la evaluación técnica de la infraestructura tecnológica hasta el análisis operativo de procesos de negocio, incluyendo la verificación del cumplimiento normativo y la implementación de controles internos basados en el marco. Este enfoque multidisciplinario permite identificar brechas de seguridad, ineficiencias operativas y oportunidades de mejora en el sistema de ventas auditado.

2. OBJETIVOS

2.1. Objetivo General

Realizar una auditoría integral del sistema de ventas de un supermercado para evaluar y garantizar la seguridad, eficiencia y confiabilidad del sistema, identificando y mitigando riesgos asociados a la gestión de productos, transacciones, seguridad de la información y procesos contables, bajo los estándares 27002.

2.2. Objetivos Específicos

Algunos objetivos específicos que tenemos para la auditoria son los siguientes:

- Verificar el cumplimiento de políticas de seguridad de la información en áreas críticas como ventas, contabilidad e inventario.
- Evaluar el control de acceso lógico y físico en puntos de venta, servidores y sistemas de red.
- Analizar la seguridad del sistema de gestión de inventario en tiempo real.
- Evaluar la integración y protección de sistemas contables ante accesos no autorizados o pérdida de datos.
- Auditar la gestión de incidentes de seguridad y la continuidad operativa ante fallos del sistema.
- Evaluar la protección contra malware y vulnerabilidades técnicas en sistemas y cajas POS.
- Determinar el nivel de cumplimiento con los planes de respaldo y recuperación de información.
- Verificar el cumplimiento de los principios de desarrollo seguro en sistemas internos o tercerizados.

3. PLANEACION

La fase de planeación implicó definir el alcance, los recursos necesarios y los responsables del proceso de auditoría. Se estableció como prioridad cubrir los procesos críticos relacionados con la operación del sistema de ventas: administración de productos, caja y métodos de pago, inventario, integración contable, continuidad del negocio, y seguridad física y lógica.

El equipo auditor elaboró un cronograma con actividades distribuidas en tres semanas. Se asignaron tareas de relevamiento de información, entrevistas con el personal clave, revisión de documentación técnica y políticas internas, pruebas técnicas de seguridad, y elaboración del diagnóstico.

La auditoría se llevó a cabo bajo los principios de confidencialidad, integridad e imparcialidad, asegurando la validez de los resultados obtenidos.

4. DIAGNOTICO

4.1. Investigación Preliminar

En esta fase se recopiló información sobre la infraestructura tecnológica del supermercado. Se revisaron manuales operativos, diagramas de red, contratos de servicios con proveedores, y se realizaron entrevistas con los encargados de sistemas, ventas y contabilidad.

Se detectó que el sistema de ventas está compuesto por:

- Un software de gestión de productos y precios.
- Módulos POS distribuidos en diferentes cajas.
- Sistema de inventario en tiempo real.
- Integración con contabilidad a través de servicios web.
- Infraestructura de red cableada y Wifi, conectada a un servidor local con respaldo en la nube.

4.2. Selección de auditores

El equipo auditor estuvo conformado por cinco integrantes con conocimientos en auditoría de sistemas, seguridad de la información y gestión de tecnologías. La selección se realizó en función de las competencias individuales, conocimientos normativos y experiencia práctica en entornos de sistemas empresariales.

Los auditores participaron activamente en todas las fases del proceso, desde la planeación hasta la emisión del informe final.

Los miembros del equipo auditor fueron:

- **Mario Barba Umalla** Especialista en infraestructura y redes.
- **José Miguel Fanola** Enlace con el área contable y sistemas financieros.
- **Luz Madelen Lazaro** Coordinadora de entrevistas y análisis documental.
- **Wilfredo Mamani Vera** responsable del análisis técnico de vulnerabilidades.
- **Franz Alberto Huanca** Quispe Coordinador general del equipo y responsable de la planificación.

Cada auditor asumió tareas específicas según su área de enfoque, garantizando un análisis integral y equilibrado de todos los procesos auditados. La labor del equipo se llevó a cabo con imparcialidad, respeto a la confidencialidad de la información, y alineamiento con la norma 27002.

4.3. Matriz de Identificación

Se desarrolló una matriz de identificación alineada a los dominios de la norma ISO/IEC 27002:2022. Esta matriz facilitó la evaluación específica de cada área crítica del sistema de ventas del supermercado, considerando los siguientes aspectos:

- **Ítems evaluados**: 9-15
- **Controles ISO/IEC 27002 aplicables**
- **Áreas responsables**: sistemas, contabilidad, desarrollo, gerencia y seguridad
- **Técnicas utilizadas**: entrevistas, cuestionarios y listas de verificación y observación

Item	Nro. Dominio	Dominio(ISO/IEC72002)	Area(s) Auditar	Entrevista			Cuestionario			Lista de Verificación			Observación		
				A	B	C	A	B	C	A	B	C	A	B	C
Auditoria de La seguridad Fisica y Lógica	5	Política de Seguridad de la Información	Gerencia de ventas y contabilidad de inventario	*	*	*									
Gestión de Productos	5.1	Seguridad de acceso y control al sistema	Gerencia de ventas y contabilidad de inventario	*	*										
Puntos de Venta (POS)	11	Seguridad Física y del Entorno	Punto de venta			*					*				
Inventario en Tiempo Real	5,1	Seguridad de acceso y control	Contabilidad de inventario	*	*										
Caja y Método de Pago	9	Control de Acceso	Punto de venta			*									
Roles y Control de Acceso al Sistema de Ventas	9	Control de Acceso	Gerencia de ventas y de sistemas	*							*				
Integración con Sistemas Contables	5	Política de Seguridad de la Información	Contabilidad	*	*										
Gestión de Incidentes	16	Gestión de Incidentes y de Seguridad de la Información	Área de sistemas	*	*										
Redes y comunicaciones Seguridad en la red (WIFI, POS, servidores)	13.1	Gestión de la seguridad de la red	Área de Tecnologia	*	*										
Gestion de Usuario y autentificacion	9.2-9.4	Gestión del acceso y control de autenticación	Área de sistemas y ventas	*	*										
Copia de seguridad y recuperación ante fallos	12.3	Información de respaldo	Área de sistemas	*	*										
Protección contra malware	12.2	Controles contra el malware	Sistemas y cajas POS	*	*										
Gestión de vulnerabilidades técnicas	12.6	Control de vulnerabilidades	Sistemas y servidores	*							*				
Seguridad en desarrollo de sistemas internos	14.2	Desarrollo seguro	Área de desarrollo o tercerizado	*							*				
Plan de continuidad operativa del sistema de ventas	17.1	Continuidad de la seguridad de la información	Gerencia + TI	*							*				

Item	Nro. Dominio	Dominio(ISO/IEC72002)	Area(s) Auditar
Auditoria de La seguridad Fisica y Lógica	5	Política de Seguridad de la Información	Gerencia de ventas y contabilidad de inventario
Gestión de Productos	5.1	Seguridad de acceso y control al sistema	Gerencia de ventas y contabilidad de inventario
Puntos de Venta (POS)	11	Seguridad Física y del Entorno	Punto de venta
Inventario en Tiempo Real	5,1	Seguridad de acceso y control	Contabilidad de inventario
Caja y Método de Pago	9	Control de Acceso	Punto de venta
Roles y Control de Acceso al Sistema de Ventas	9	Control de Acceso	Gerencia de ventas y de sistemas
Integración con Sistemas Contables	5	Política de Seguridad de la Información	Contabilidad
Gestión de Incidentes	16	Gestión de Incidentes y de Seguridad de la Información	Área de sistemas
Redes y comunicaciones Seguridad en la red (WIFI, POS, servidores)	13.1	Gestión de la seguridad de la red	Area de Tecnologia
Gestion de Usuario y autentificacion	9.2-9.4	Gestión del acceso y control de autenticación	Área de sistemas y ventas
Copia de seguridad y recuperación ante fallos	12.3	Información de respaldo	Área de sistemas
Protección contra malware	12.2	Controles contra el malware	Sistemas y cajas POS
Gestión de vulnerabilidades técnicas	12.6	Control de vulnerabilidades	Sistemas y servidores
Seguridad en desarrollo de sistemas internos	14.2	Desarrollo seguro	Área de desarrollo o tercerizado
Plan de continuidad operativa del sistema de ventas	17.1	Continuidad de la seguridad de la información	Gerencia + TI

4.4. Plan de auditoria

El plan de auditoría fue diseñado considerando auditorías internas sobre todos los procesos del sistema de ventas. Se definieron los siguientes elementos:

- **Ciudad**: Santa Cruz
- **Tipo de auditoría**: Interna
- **Criterios de auditoría**: Norma ISO/IEC 27002, políticas internas y procedimientos
- **Métodos aplicados**: Entrevistas, verificación documental y observación directa

Empresa	Programa de auditoria																	CODIGO:RGC-01 VERSIÓN:1 FECHA DE VIGENCIA:01-01-2023
OBJETIVO	s																Periodo:	AÑO 2023
																	Metodo de auditoría	Entrevista al personal Verificación de documentos Observación directa mediante recorrido por
Alcance										Todos los procesos del sistemas de gestion desarrollados en Santa Cruz y Cochabamba								
Nro. Item	**Item**	**Nro. Dominio**	**Area(s) Auditar**	**Ciudad**	**Tipo de Auditoria**	**Auditor**	**Responsable**	**Cargo**	**Formación Profesional**	**2023**								**CRITERIO DE AUDITORIA**
										Ene	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**	
1	Auditoria de La seguridad Fisica y Lógica	5	Unidad de Informatica	Santa Cruz	Interna	Auditores internos de la empresa	Jefe de Informática	Coordinador de Seguridad	Ingeniero en Sistemas	X			X	X		X	X		X	X		Norma ISO 27002 Normativa legal aplicable Procedimientos internos.
2	Gestión de Productos	5.1	Seguridad de acceso y control al sistema	Santa Cruz	Interna	Auditores internos de la empresa	Supervisor de Procesos de Ventas	Coordinador de Área	Lic. en Administración	X	X		X	X	X		X			X	X	Norma ISO 27002 Seguridad de accesos Políticas internas de productos y procesos
3	Puntos de Venta (POS)	11	Punto de Venta	Santa Cruz	Interna	Auditores internos de la empresa	Supervisor de Punto de Venta	Encargado de Operaciones	Técnico en Administración		X			X		x		X	X			Norma ISO 27002 Seguridad Física y del Entorno
4	Inventario en Tiempo Real	5.1	Contabilidad de inventario	Santa Cruz	Interna	Auditores internos de la empresa	Contabilidad de inventario	Técnico Contable	Técnico en Administración	X	X	X		X	X		X		X	X	X	Norma ISO 27002 Seguridad de accesos Políticas internas de productos y procesos
5	Caja y Método de Pago	9	Punto de Venta	Santa Cruz	Interna	Auditores internos de la empresa	Cajero Principal	Cajero Principal	Técnico Contable	X	X		X	X				x		X	X	Norma ISO 27002 Control de Acceso
6	Seguridad y Control de Acceso	9	Gerencia de ventas y sistemas	Santa Cruz	Interna	Auditores internos de la empresa	Jefe de Sistemas	Responsable de Seguridad	Ing. en Redes y Seguridad		X	X		X	X		X	X				Norma ISO 27002 Control de Acceso
7	Integración con Sistemas Contables	5	Contabilidad	Santa Cruz	Interna	Auditores internos de la empresa	Contador General	Especialista Contable	Lic. en Contaduría Pública	X	X		X	X						X	X	Norma ISO 27002 Política de Seguridad de la Información
8	Gestión de Incidentes	16	Área de Sistemas	Santa Cruz	Interna	Auditores internos de la empresa	Coordinador de Continuidad TI	Líder de Seguridad	Ingeniero en Sistemas		X	X		X	X	X	X		X	X		Norma ISO 27002 Gestión de Incidentes y Seguridad de la Información
9	Redes y comunicaciones (WiFi, POS, servidores)	13.1	Área de Tecnología	Santa Cruz	Interna	Auditores internos de la empresa	Responsable de Redes	Encargado de Infraestructura	Ing. en Redes	X	X		X	X		X			X	X		Norma ISO 27002 Gestión de la Seguridad de la Red
10	Gestión de Usuario y Autentificación	9.2 - 9.4	Área de Sistemas y Ventas	Santa Cruz	Interna	Auditores internos de la empresa	Supervisor de TI	Responsable de Accesos	Lic. en Informática	x			x			x			x			Norma ISO 27002 Gestión del acceso y control de autenticación
11	Copia de seguridad y recuperación ante fallos	12.3	Área de Sistemas	Santa Cruz	Interna	Auditores internos de la empresa	Encargado de Backup	Técnico de Soporte	Técnico en Sistemas	X			X		X	X	X	X	X		X	Norma ISO 27002 Información de respaldo
12	Protección contra malware	12.2	Sistemas y cajas POS	Santa Cruz	Interna	Auditores internos de la empresa	Encargado de Antivirus	Técnico de Seguridad	Técnico en Sistemas	X			X	X	X	X			X	X	X	Norma ISO 27002 Controles contra el malware
13	Gestión de vulnerabilidades	12.6	Sistemas y servidores	Santa Cruz	Interna	Auditores internos de la empresa	Administrador de Redes	Administrador de Sistemas	Ing. en Redes		X	X			X	X	X	X		X	X	Norma ISO 27002 Control de vulnerabilidades
14	Seguridad en desarrollo de sistemas internos	14.2	Área de desarrollo o tercerizado	Santa Cruz	Interna	Auditores internos de la empresa	Desarrollador Senior	Líder de Desarrollo	Lic. en Ingeniería de Sistemas	X			X	X		X	X	X	X			Norma ISO 27002 Desarrollo seguro
15	Plan de continuidad operativa del sistema de ventas	17.1	Gerencia + TI	Santa Cruz	Interna	Auditores internos de la empresa	Jefe de Tecnología	Gerente TI	Ing. en Sistemas	X	X		X	X				X	X		X	Norma ISO 27002 Continuidad de la seguridad de la información

5. PLAN DE TRABAJO

Se establecieron 5 áreas clave de análisis, y se integraron los ítems de la matriz en cada una de ellas para un diagnóstico más estructurado:

Area 1: Seguridad de Acceso y Control al Sistema

- Evaluación del control de accesos, usuarios y autenticación (Ítem 10).
- Revisión de permisos por rol (cajeros, supervisores, gerentes).
- Validación de auditorías de login y trazabilidad.

Area 2: Seguridad Física y del Entorno

- Análisis de seguridad en servidores, POS y puntos de red (Ítem 9).
- Verificación de medidas de protección y redes segmentadas.
- Inspección de equipos físicos y control de acceso a infraestructura.

Area 3: Continuidad del Negocio y Respaldo

- Verificación de planes de respaldo y recuperación (Ítems 11 y 15).
- Evaluación de simulacros, disponibilidad y redundancias.
- Análisis de documentación del plan de continuidad operativa.

Area 4: Gestión de Incidentes y Seguridad en la Red

- Revisión del protocolo de incidentes y alertas (Ítem 8).
- Análisis de protección antivirus y detección de malware (Ítem 12).
- Evaluación de actualizaciones de seguridad y gestión de vulnerabilidades (Ítem 13).

Area 5: Cumplimiento y Desarrollo Seguro

- Revisión de prácticas seguras de desarrollo (Ítem 14).
- Validación de entornos de prueba y producción.
- Revisión de integración contable y sistemas críticos (Ítem 7).

6. CONCLUSION

La auditoría realizada al sistema de ventas del supermercado nos permitió conocer claramente el estado actual de sus controles de seguridad, eficiencia y cumplimiento, basándonos en la norma ISO/IEC 27002 y las buenas prácticas de ITIL.

Identificamos fortalezas importantes, como la definición clara de roles en los módulos POS, la integración entre ventas y contabilidad, y avances en las políticas de respaldo de información. Sin embargo, también detectamos

áreas que necesitan atención urgente: falta de procedimientos formales para la gestión de incidentes, pruebas de recuperación de datos pocos frecuentes y sin documentación, deficiencias en el monitoreo de redes y gestión de vulnerabilidades, ausencia de separación entre ambientes de desarrollo y producción, y políticas de seguridad que no se actualizan regularmente.

Por ello, recomendamos a la gerencia implementar un plan de mejora continua que incluya auditorías internas periódicas, capacitación al personal, actualización de políticas y el uso de herramientas modernas para proteger el sistema. También es clave reforzar los protocolos de respaldo, continuidad operativa y monitoreo de seguridad.

Esta auditoría fue realizada por el equipo interno conformado por Mario Barba, José Miguel Fanola, Franz Huanca, Mi persona Wilfredo Mamani Vera y Luz Madelen Lazaro, Donde trabajamos con responsabilidad y compromiso para mejorar los procesos tecnológicos de la empresa. Con las recomendaciones aplicadas, el sistema de ventas podrá ser más seguro, confiable y alineado con estándares.