Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca
"Facultad de Ciencias y Tecnología"

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA FARMACORP

Materia: Seguridad de la Información

Universitarios:

1.

INTRODUCCIÓN

1.1. Antecedentes

1937: Fundación de Farmacia Gutiérrez en Santa Cruz por Osvaldo Gutiérrez.

1964: Apertura de Farmacia Santa María.

1994: Implementación de Buenas Prácticas de Farmacia.

2000: Fusión de Farmacias Gutiérrez y Santa María, nace Farmacorp. Inicio de expansión nacional y nuevos servicios (Farmaclub, Farmamóvil).

2010-2020: Estrategia omnicanal: e-commerce, delivery, pick-up y centros de distribución.

2019: Creación de Farmacias Dr. Osvaldo para zonas periféricas.

2022: Fundación de Nexocorp, integrando Farmacorp, Farmacias Dr. Osvaldo, Amarket, Pizza Hut y negocios inmobiliarios (Bendita).

1.2. Actividad de la Empresa

Comercialización de Productos

Medicamentos (82%)

Alimentos

Cosméticos

Cuidado personal

Líneas de marca blanca (5%)

Marcas internacionales: GNC Live Well, About Time, Foster Grant, Jockey, Ubu, Scunci.

1.2. Actividad de la Empresa

Presencia Geográfica

Santa Cruz y Cochabamba (principal)
La Paz
Oruro
Potosí
Tarija
Beni
Pando

Servicios Adicionales

Farmaclub (fidelización de clientes)

Farma Móvil (entrega puerta a puerta)

Pago de servicios 24/7

Participación de Mercado

46% en cadenas de farmacias

70 años de experiencia

1.3. Organigrama de la Empresa

1.4. Funciones del Personal

1.4. Funciones del Personal

1.4.5. Dirección de Tecnología e Informática (CIO)

Encargado de la infraestructura tecnológica y los procesos de digitalización de la empresa.

1.4.5.1.1. Área de Desarrollo de Software

Desarrollo y mantenimiento de sistemas internos y externos.

1.4.5.1.2. Área de Soporte Técnico

Soluciona problemas técnicos y realiza mantenimiento de hardware.

1.4.5.1.3. Área de Seguridad de la Información (SGSI)

Responsable de la protección de datos y la continuidad operativa en caso de incidentes relacionados con la seguridad de la información.

1.4.5.1.3. Área de Seguridad de la Información (SGSI)

FarmaCorp

1.4.5. Dirección de Tecnología e Informática (CIO)

Responsable de la protección de datos y la continuidad operativa en caso de incidentes relacionados con la seguridad de la información.

1.4.5.1.3.1. Jefe de Seguridad de la Información (CISO)

- Diseña y supervisa el SGSI.
- Establece políticas, evalúa riesgos y define controles.

1.4.5.1.3.2. Analistas de Seguridad de la Información

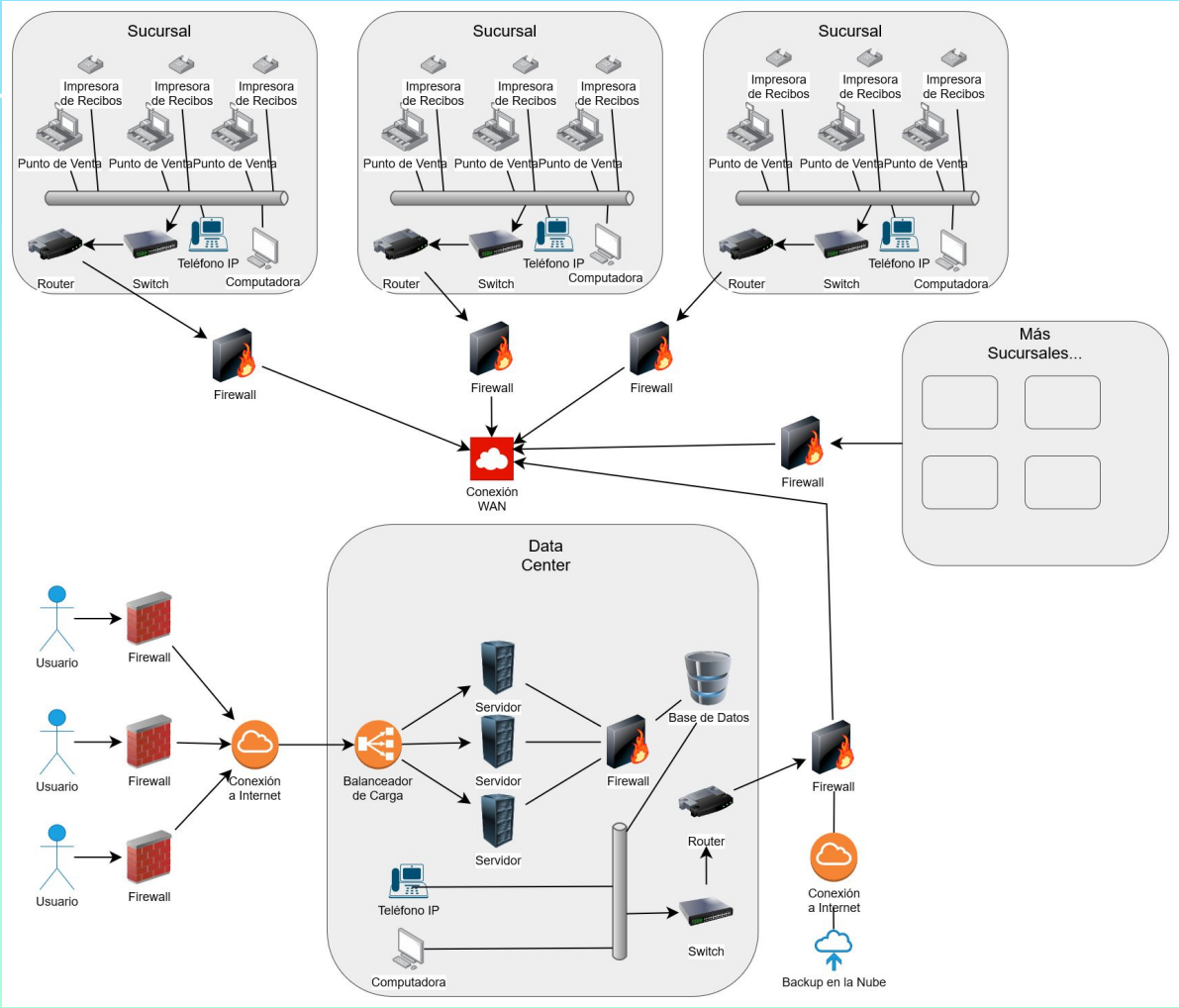
- Implementan y monitorean controles de red y sistemas.
- Realizan auditorías y gestionan herramientas como firewalls e IDS.

1.4.5.1.3.3. Equipo de Respuesta a Incidentes (CSIRT)

- Gestiona incidentes en tiempo real.
- Realiza análisis forenses y define estrategias de recuperación.

1.5. Infraestructura Tecnológica

Farmacorp, al ser una de las cadenas farmacéuticas más grandes de Bolivia, cuenta con una infraestructura tecnológica robusta que respalda sus operaciones comerciales y de atención al cliente en sus múltiples sucursales a nivel nacional


Sucursal
Impresora de Recibos
Impresora de Recibos
Impresora de Recibos
Punto de Venta
Punto de Venta
Punto de Venta
Teléfono IP
Router
Switch
Computadora
Sucursal
Impresora de Recibos
Impresora de Recibos
Impresora de Recibos
Punto de Venta
Punto de Venta
Punto de Venta
Teléfono IP
Router
Switch
Computadora
Sucursal
Impresora de Recibos
Impresora de Recibos
Impresora de Recibos
Punto de Venta
Punto de Venta
Punto de Venta
Teléfono IP
Router
Switch
Computadora
Firewall
Firewall
Firewall
Más Sucursales...
Conexión WAN
Firewall
Data Center
Usuario
Usuario
Usuario
Firewall
Firewall
Firewall
Conexión a Internet
Balanceador de Carga
Servidor
Servidor
Servidor
Firewall
Base de Datos
Router
Switch
Teléfono IP
Computadora
Firewall
Conexión a Internet
Backup en la Nube

1.5. Infraestructura Tecnológica

Sucursales

176 sucursales en Bolivia

Hardware

POS, Computadoras, Impresoras, Servidores, etc

Software

Ha estado utilizando el sistema **Revionics** desde 2014

Redes

Se utiliza routers y switches para conectar todas las sucursales a la oficina central

Almacenamiento y Backup

Cuenta con una certificación en Buenas Prácticas de Almacenamiento

Seguridad

Cuenta con seguridad de múltiples capas

Disponibilidad y Capacidad

Está diseñada para manejar grandes volúmenes de transacciones diarias

2.

OBJETIVO Y ALCANCE

2.1. Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la confidencialidad, integridad y disponibilidad de los datos sensibles y críticos de la farmacia, cumpliendo con la normativa Internacional ISO 27001:2013.

2.2. Objetivos Específicos

Análisis de Activos

Identificar y clasificar activos críticos según ISO 27001.

Gestión de Riesgos

Evaluar riesgos con el marco Magerit V3.

Políticas de Seguridad

Diseñar políticas preventivas y correctivas para mitigar riesgos identificados.

2.3. Alcance

Análisis detallado de activos en cada departamento.

Diseño de políticas de seguridad alineadas con ISO 27001.

Mitigación de riesgos con medidas preventivas y correctivas.

3.

Marco Teorico

3.1. ISO 27001:2013

Que es?

Norma internacional para gestionar la seguridad de la información.

Objetivo

Proteger la confidencialidad, integridad y disponibilidad de la información.

Origen y Desarrollo

- Basada en la norma británica BS 7799 (1995).
- Adoptada por ISO en 2005.
- Versión actual: ISO/IEC 27001:2013.

3.1. ISO 27001:2013

Elementos Clave

- Contexto de la Organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del Desempeño
- Mejora Continua

Beneficios

- Protección de la Información
- Cumplimiento Normativo
- Confianza de Clientes
- Gestión de Riesgos
- Ventaja Competitiva

3.2 Familias de la ISO 27000

ISO/IEC 27001

Sistema de Gestión de Seguridad de la Información (SGSI)

ISO/IEC 27002

Código de Práctica para los Controles de Seguridad de la Información

ISO/IEC 27003

Directrices para la Implementación de SGSI

ISO/IEC 27004

Gestión de la Medición de la Seguridad de la Información.

ISO/IEC 27005

Gestión de Riesgos de Seguridad de la Información.

ISO/IEC 27006

Requisitos para los Organismos que Realizan Auditoría y Certificación de SGSI.

3.2 Familias de la ISO 27000

ISO/IEC 27007

Directrices para la Auditoría de SGSI.

ISO/IEC 27008

Directrices para la Evaluación de Controles de Seguridad de la Información.

3. 3 Ciclo de vida del SGSI

Ciclo de vida

PLANIFICAR

Definición de la política de seguridad: Principios y objetivos que guiarán la protección de datos.
Alineación institucional: Asegurar que el SGSI apoye las metas de FarmaCorp.
Gestión de riesgos: Definir criterios para identificar y clasificar riesgos.
Inventario de activos: Recursos físicos, digitales y de software a proteger.
Valoración de activos: Determinar importancia y vulnerabilidad de cada recurso.

Ciclo de vida

HACER

Identificación de riesgos: Detectar amenazas y vulnerabilidades en los activos.
Matriz de riesgos: Visualizar, priorizar riesgos por probabilidad e impacto.
Implementación de controles: Políticas de acceso seguro, gestión de contraseñas y protección de datos personales.
Capacitación: Asegurar que el personal comprenda políticas y procedimientos de seguridad.

Ciclo de vida

VERIFICAR

Revisión de incidentes: Analizar violaciones, pérdidas de datos y acciones correctivas.
Auditorías internas: Evaluar cumplimiento de políticas y eficacia de controles.
Comparación con objetivos: Verificar si se alcanzaron los niveles de seguridad esperados.

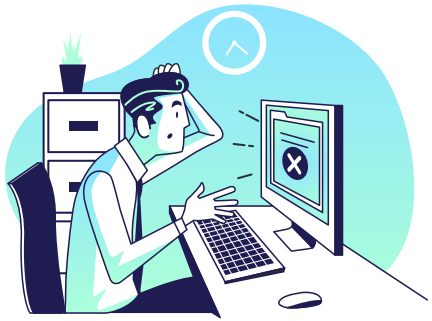
Ciclo de vida

ACTUAR

Ajustes continuos: Corregir fallos, mitigar riesgos no atendidos y afrontar nuevas amenazas.
Estandarización: Consolidar procesos efectivos en toda la organización.
Documentación: Registrar mejoras para fortalecer el sistema.

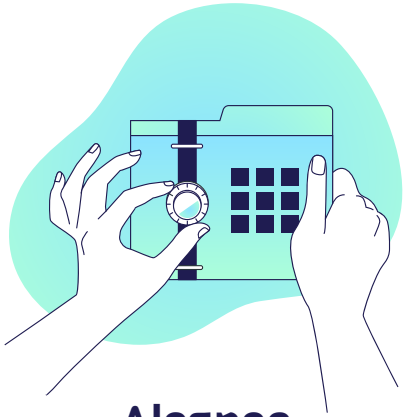
4.2 ETAPA DE PLANIFICACIÓN

Objetivo y alcance del SGSI



Objetivo

Garantizar la **confidencialidad, integridad y disponibilidad** de la información en Farmacorp, alineándose con la norma ISO 27001:2013 y los requisitos legales.



Alcance

Aplica a todos los empleados, contratistas y proveedores con acceso a sistemas y datos, abarcando tecnologías, sistemas y recursos físicos y digitales de Farmacorp.

4.2.3 Procesos y procedimientos

Falta de un gobierno de Seguridad en Farmacorp

Falta de un Proceso Formal para la Gestión de Incidentes de Seguridad

Inexistencia de Políticas y Procedimientos de Seguridad

Ausencia de Control de Acceso y Gestión de Identidades en Sistemas de Información Médica

Insuficiente Protección de Información de Pacientes y Personal en Farmacorp

Falta de un Proceso Formal para la Gestión de Incidentes de Seguridad

Procesos y procedimientos : Insuficiente Protección de Información de Pacientes y Personal en Farmacorp

Procedimiento:

Realizar una evaluación exhaustiva de riesgos centrada en los sistemas que almacenan información crítica sobre pacientes y personal,

Acciones: Identificar las áreas críticas dentro de los sistemas de información de Farmacorp, desarrollando políticas específicas para el control de acceso, gestión de incidentes y protección de datos sensibles

4.3.4 Políticas de Seguridad

Conjunto de:

- Reglas
- Directrices
- Procedimientos

Es empleado para la protección de amenazas y riesgos

Políticas de seguridad

Para la realización de las políticas se detallaron:

1. Objetivos.

2. Procedimientos.
   - ID De la actividad
   - Responsable
   - Actividad
   - Sub Actividad
   - Registros

3. Anexos de Actividades para cada política
   - Mención de la Actividad
   - Objetivo de la actividad
   - Procedimiento a emplear

Política de Seguridad Física para Acceso No Autorizado

- **Objetivo:** Mejorar las medidas de control físico en las instalaciones para restringir el acceso no autorizado a los equipos críticos, mediante sistemas de acceso controlado y monitoreo constante, garantizando la seguridad e integridad de los recursos físicos de la infraestructura de red.

ID	Responsable	Actividades	Sub Actividades
PS-07	Oficial de Seguridad Física, en coordinación con el Departamento de Seguridad de la Información.	**1. Control de Acceso Físico a Zonas Restringidas**	**Revisión y Actualización de Áreas Restringidas:** Inspeccionar y ajustar la clasificación de las áreas restringidas, asegurando que los niveles de seguridad sean adecuados y reflejen cualquier cambio en la infraestructura o riesgos. (Anexo P02.1)
			Reconfiguración de Medidas de Control de Acceso Físico: Actualizar la configuración de dispositivos de acceso físico como cerraduras electrónicas, lectores de tarjetas, y escáneres biométricos, asegurando que los permisos de acceso se ajusten a las necesidades de seguridad actuales. (Anexo P02.2)
			Monitoreo y Registro de Accesos Físicos: Realizar el seguimiento y registro de todos los accesos a las áreas restringidas mediante sistemas de monitoreo, con el fin de identificar accesos no autorizados y patrones de comportamiento.
			Auditorías Periódicas de Acceso Físico: Realizar auditorías regulares de los registros de acceso para verificar la efectividad

4.3.5 Sub Actividad P02.1

PROCEDIMIENTO DE MONITOREO DE ÁREAS RESTRINGIDAS
ACTIVIDAD: Monitorear continuamente el acceso fisico a las zonas restringidas de las instalaciones de FarmaCorp OBJETIVO: Garantizar que únicamente personal autorizado pueda ingresar a áreas críticas de las instalaciones, mediante el uso de tecnologías y vigilancia fisica efectiva.
PROCEDIMIENTO A EMPLEAR
1) Identificación de Áreas Restringidas: 2) Verificar las zonas designadas como restringidas en el plano de instalaciones. 3) Confirmar la cobertura de cámaras de vigilancia y sensores en estas áreas. 4) Etiquetar fisicamente las áreas restringidas con señalización visible. 5) Verificación Inicial de Equipos de Monitoreo: 6) Inspeccionar cámaras de seguridad, sensores de movimiento y grabadores digitales (DVR). 7) Realizar una prueba de funcionamiento para asegurar grabación continua y emisión de alertas. 8) Confirmar que los registros de monitoreo se almacenan de forma segura en el sistema. 9) Configuración de Turnos de Supervisión: 10) Asignar turnos a operadores para la supervisión en tiempo real de los monitores de seguridad. 11) Registrar en el sistema el operador asignado y su horario. 12) Capacitar al personal sobre los procedimientos de respuesta ante incidentes. 13) Supervisión en Tiempo Real: 14) Revisar de manera continua las transmisiones en vivo de las cámaras instaladas en las áreas restringidas. 15) Establecer puntos clave para una atención prioritaria (puertas de acceso, puntos ciegos minimizados, etc.).

Políticas realizadas

Se realizaron las políticas para los riesgos identificados como extremos y catastróficos:

- Acceso no autorizado (Físico, Lógico)
- Modificación deliberada de la información
- Falla de hardware del sistema de respaldo
- Destrucción de la información

5. Conclusiones

- Se realizó el Sistema de Gestión de Seguridad de la Información (SGSI) que cumple con los estándares de la norma ISO 27001:2013.

- Realización de:
  - Identificación de los Activos
  - Análisis de activos
  - Clasificación según su nivel de sensibilidad e impacto
  - Se identificaron Amenazas y Vulnerabilidades
  - Se realizaron políticas.

4. Recomendaciones

Actualización del SGSI

Implementación de simulacros para la gestión de incidentes

programas de capacitación al personal

Automatización de controles

programas de capacitación al personal

GRACIAS