**UNIVERSIDAD MAYOR REAL Y PONTIFICIA**

**DE**

**SAN FRANCISCO XAVIER DE CHUQUISACA**

**FACULTAD DE CIENCIAS Y TECNOLOGÍA**

**CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN** 

**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA FARMACORP**

**Materia:** Seguridad de la Información

**Universitarios:**

* Pereira Cuba Claudia
* Villca Jaita Lino Fernando
* Vera Miranda Luis Gustavo
* Martinez Rodriguez Milton Angel
* Santillan Jason
* Diaz Barron Ricardo
* Parraga Ortuste Diego Armando
* Victoria Avila Carlos Osmar

**Docente:** Ing. Roca Malale Deyler

**Sucre, 23 de noviembre del 2024**

ÍNDICE

[1. Introducción 1](#_Toc183215906)

[1.1. Antecedentes 1](#_Toc183215907)

[1.2. Actividad de la Empresa 2](#_Toc183215908)

[1.3. Organigrama de la Empresa 4](#_Toc183215909)

[1.4. Funciones del personal 4](#_Toc183215910)

[1.4.1. Director General (CEO) 4](#_Toc183215911)

[1.4.2. Dirección de Operaciones (COO) 4](#_Toc183215912)

[1.4.3. Dirección Financiera (CFO) 4](#_Toc183215913)

[1.4.4. Dirección de Recursos Humanos 4](#_Toc183215914)

[1.4.5. Dirección de Tecnología e Informática (CIO) 4](#_Toc183215915)

[1.4.6. Dirección de Ventas y Marketing 5](#_Toc183215916)

[1.4.7. Dirección de Investigación y Desarrollo (I+D) 5](#_Toc183215917)

[1.4.8. Gerentes Regionales 5](#_Toc183215918)

[1.4.9. Gerente de tienda 5](#_Toc183215919)

[1.4.10. Supervisores de Farmacia 6](#_Toc183215920)

[1.4.11. Farmacéuticos 6](#_Toc183215921)

[1.4.12. Asistente de farmacia 6](#_Toc183215922)

[1.4.13. Personal de atención al cliente 6](#_Toc183215923)

[1.4.14. Personal de logística y almacén 6](#_Toc183215924)

[1.4.15. Cajeros 6](#_Toc183215925)

[1.4.16. Personal de limpieza y mantenimiento 6](#_Toc183215926)

[1.5. Infraestructura tecnológica de la empresa 7](#_Toc183215927)

[1.5.1. Sucursales 7](#_Toc183215928)

[1.5.2. Hardware 8](#_Toc183215929)

[1.5.3. Software 8](#_Toc183215930)

[1.5.4. Redes 8](#_Toc183215931)

[1.5.5. Almacenamiento y Backup 8](#_Toc183215932)

[1.5.6. Seguridad 9](#_Toc183215933)

[1.5.7. Disponibilidad y Capacidad 9](#_Toc183215934)

[2. Objetivo y Alcance 10](#_Toc183215935)

[2.1. Objetivo General 10](#_Toc183215936)

[2.2. Objetivo Específico 10](#_Toc183215937)

[2.3. Alcance 10](#_Toc183215938)

[3. Marco Teórico 11](#_Toc183215939)

[3.1. ISO 27000 11](#_Toc183215940)

[3.1.1. ¿Qué es la ISO 27001:2013? 11](#_Toc183215941)

[3.1.2. Breve historia de la ISO 27001 11](#_Toc183215942)

[3.1.3. Descripción de la ISO 27001 12](#_Toc183215943)

[3.1.4. Beneficios de Implementar ISO 27001:2013 12](#_Toc183215944)

[3.2. Familias de la ISO 27000 13](#_Toc183215945)

[3.2.1. ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI) 13](#_Toc183215946)

[3.2.2. ISO/IEC 27002: Código de Práctica para los Controles de Seguridad de la Información 13](#_Toc183215947)

[3.2.3. ISO/IEC 27003: Directrices para la Implementación del SGSI 13](#_Toc183215948)

[3.2.4. ISO/IEC 27004: Gestión de la Medición de la Seguridad de la Información 13](#_Toc183215949)

[3.2.5. ISO/IEC 27005: Gestión de Riesgos de Seguridad de la Información 14](#_Toc183215950)

[3.2.6. ISO/IEC 27006: Requisitos para los Organismos que Realizan Auditoría y Certificación de SGSI 14](#_Toc183215951)

[3.2.7. ISO/IEC 27007: Directrices para la Auditoría de SGSI 14](#_Toc183215952)

[3.2.8. ISO/IEC 27008: Directrices para la Evaluación de Controles de Seguridad de la Información 14](#_Toc183215953)

[3.3. Ciclo de Vida 14](#_Toc183215954)

[3.3.1. Plan (Planificar) 15](#_Toc183215955)

[3.3.2. Do (Hacer) 16](#_Toc183215956)

[3.3.3. Check (Verificar) 16](#_Toc183215957)

[3.3.4. Act (Actuar) 17](#_Toc183215958)

[4. Desarrollo del Proyecto 18](#_Toc183215959)

[4.1. Cronograma del Proyecto 18](#_Toc183215960)

[4.2. Fase 1: Planificación 18](#_Toc183215961)

[4.2.1. Definir política. 18](#_Toc183215962)

[4.2.2. Identificar objetivos de la institución. 19](#_Toc183215963)

[4.2.3. Procesos y procedimientos. 20](#_Toc183215964)

[4.2.4. Definir criterios de evaluación. 25](#_Toc183215965)

[4.2.5. Inventario de Activos 28](#_Toc183215966)

[4.3. Fase 2. Hacer 28](#_Toc183215967)

[4.3.1. Catálogo de Amenazas 28](#_Toc183215968)

[4.3.2. Análisis de Riesgo 28](#_Toc183215969)

[4.3.3. Matriz de Riesgo 28](#_Toc183215970)

[4.3.4. Políticas de seguridad 28](#_Toc183215971)

[4.3.5. Anexos de Políticas de Seguridad 50](#_Toc183215972)

[5. Conclusiones 93](#_Toc183215973)

[6. Recomendaciones 93](#_Toc183215974)

[7. Referencia Bibliográfica 94](#_Toc183215975)

ÍNDICE DE FIGURAS

[**Figura 1**. Venta de medicamentos 3](#_Toc183256543)

[**Figura 2.** Venta de productos 3](#_Toc183256544)

[**Figura 3.** Estructura empresarial. 4](#_Toc183256545)

[**Figura 4.** Infraestructura tecnológica de la empresa 7](#_Toc183256546)

[**Figura 5.** Ciclo de vida PDCA 15](#_Toc183256547)

[**Figura 6.** Cronograma del Proyecto 18](#_Toc183256548)

ÍNDICE DE TABLAS

[Tabla 1. Procesos y procedimientos 20](#_Toc183263278)

[Tabla 2. Clasificación 25](#_Toc183263279)

[Tabla 3. Valor del Activo - Confidencialidad 26](#_Toc183263280)

[Tabla 4. Valor del Activo - Disponibilidad 26](#_Toc183263281)

[Tabla 5. Valor del Activo - Integridad 27](#_Toc183263282)

[Tabla 6. Inventario de Activos 30](#_Toc183263283)

[Tabla 7. Catálogo de Amenazas 31](#_Toc183263284)

[Tabla 8. Análisis de Riesgo 35](#_Toc183263285)

[Tabla 9. Matriz de Riesgo 42](#_Toc183263286)

[Tabla 10. Procedimientos para Política de Mitigación del Riesgo de Falla de Hardware del Sistema de Respaldo 43](#_Toc183263287)

[Tabla 11. Procedimientos para Política de Seguridad Física para Acceso No Autorizado 46](#_Toc183263288)

[Tabla 12. Procedimientos para Política de Lógica para Acceso No Autorizado 51](#_Toc183263289)

[Tabla 13. Procedimientos para Política de Modificación Deliberada de la Información en el Software de Gestión de Contratos 56](#_Toc183263290)

[Tabla 14. Procedimientos para Política de Ataque de Ransomware que afecte los Datos Respaldados 59](#_Toc183263291)

[Tabla 15. Procedimientos para Política de Protección contra la Pérdida y Destrucción de Datos en Software 61](#_Toc183263292)

[Tabla 16. Procedimientos para Política de Protección para la Configuración del Switch de Red 2 66](#_Toc183263293)

# Introducción

## Antecedentes

Farmacorp es una empresa boliviana con una historia que se remonta a 1937, cuando el bioquímico Osvaldo Gutiérrez fundó la primera Farmacia Gutiérrez en Santa Cruz de la Sierra. Lo que comenzó como una pequeña farmacia en el centro de la ciudad, a una cuadra de la plaza principal, fue creciendo bajo la administración familiar. En los años 60, las hijas de Gutiérrez se integraron al negocio, desempeñando un papel clave en su expansión, lo que llevó a la creación de la Farmacia Santa María en 1964. El crecimiento continuó en las décadas siguientes, con la incorporación de la tercera generación de la familia en los años 90, quienes impulsaron la modernización y profesionalización de la empresa, destacando la implementación de Buenas Prácticas de Farmacia en 1994.

El año 2000 marcó un punto de inflexión cuando se fusionaron las farmacias Gutiérrez y Santa María, dando origen a Farmacias Corporativas S.A., conocida como Farmacorp. Esta etapa inició la expansión a nivel nacional, abriendo sucursales en ciudades importantes como Cochabamba y La Paz. Además, se introdujeron servicios como el pago de servicios básicos, un programa de fidelización de clientes llamado Farmaclub, y el servicio de entrega a domicilio con Farmamóvil.

Entre 2010 y 2020, la empresa continuó innovando, adoptando una estrategia omnicanal que integró e-commerce, servicios de delivery, pick up, y la creación de centros de distribución estratégicamente ubicados para mejorar la logística. En 2019, Farmacorp lanzó la cadena Farmacias Dr. Osvaldo, enfocada en ofrecer medicamentos y productos a precios accesibles en zonas periféricas.

En 2022, Farmacorp diversificó aún más sus operaciones con la creación de Nexocorp, una marca que agrupa las distintas unidades de negocio del Grupo Gutiérrez. Bajo Nexocorp, se integran las cadenas farmacéuticas Farmacorp y Farmacias Dr. Osvaldo, los supermercados Amarket, franquicias internacionales como Pizza Hut, y negocios inmobiliarios bajo la marca Bendita, reflejando la visión de futuro y la expansión del grupo empresarial.Actividad de la empresa.

## Actividad de la Empresa

La empresa “FARMACORP” se dedica principalmente a la comercialización de productos relacionados con la salud y el bienestar, con un enfoque en medicamentos, que representan el 82% de su oferta como se muestra en la Figura 1. Además, comercializa alimentos, cosméticos y otros productos para el cuidado personal. Farmacorp también cuenta con líneas de marca blanca, que constituyen el 5% de su portafolio, aunque su principal oferta incluye reconocidas marcas internacionales en Bolivia, como GNC Live Well, About Time, Foster Grant, Jockey, Ubu y Scunci.

Con 70 años de experiencia en el sector, la Compañía mantiene una destacada participación de mercado del 46% en el segmento de cadenas de farmacias. Sus operaciones están concentradas principalmente en los departamentos de Santa Cruz y Cochabamba, aunque también cuenta con presencia en los demás departamentos de Bolivia.

Además de la venta de productos, Farmacorp ofrece servicios como el Farmaclub, un club de fidelización para sus clientes, Farma Móvil, que proporciona entrega puerta a puerta, y la posibilidad de realizar el pago de servicios disponible las 24 horas.

**Figura 1**.  
Venta de medicamentos



Nota. Adaptado de Escuela de regentes de Farmacorp. (BuenVivir, 2021)

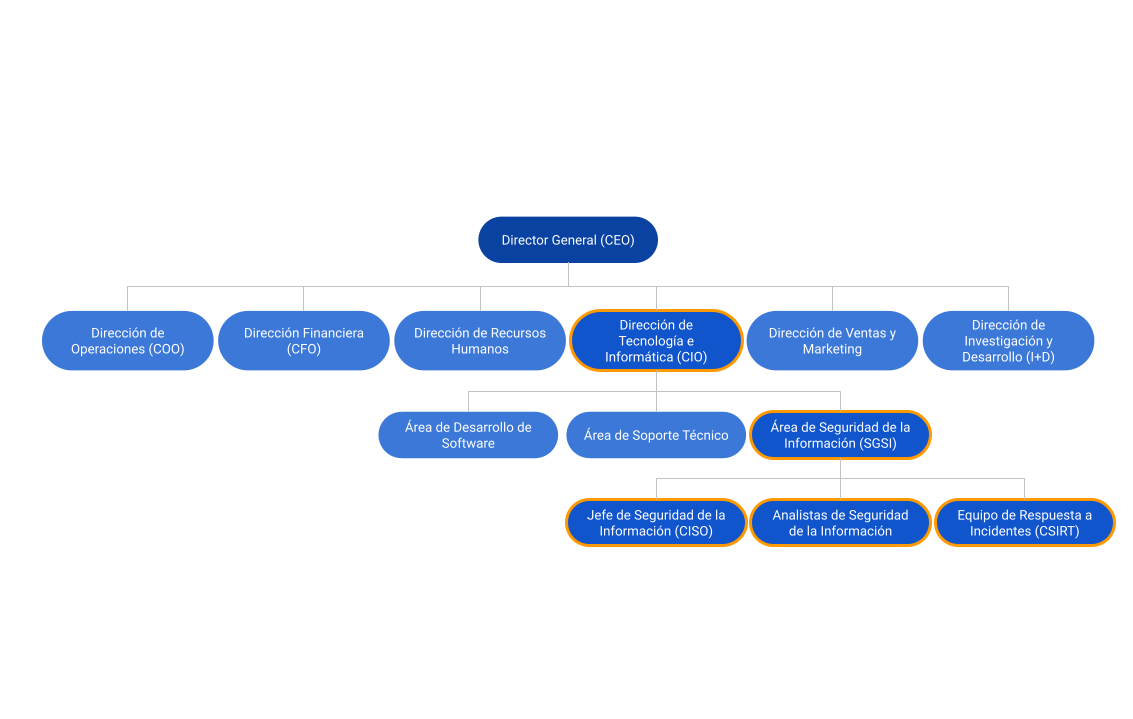
**Figura 2.**Venta de productos



Nota. Adaptado de Farmacorp, empresa líder del sector farmacéutico boliviano celebra 85 años de servicio a la comunidad. (GenteMotivandoGente, 2022)

## Organigrama de la Empresa

**Figura 3.**Estructura empresarial.



Nota. El grafico representa la estructura jerárquica y de composición de la empresa Farmacorp.

## Funciones del personal

### Director General (CEO)

Responsable de la gestión global y la toma de decisiones estratégicas de la empresa.

### Dirección de Operaciones (COO)

Supervisa las áreas de producción, logística y distribución de productos.

### Dirección Financiera (CFO)

Gestiona las finanzas, la planificación financiera y los riesgos de la empresa.

### Dirección de Recursos Humanos

Responsable de la gestión del talento, la contratación y la implementación de políticas laborales.

### Dirección de Tecnología e Informática (CIO)

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

#### Departamento de Informática

##### Área de Desarrollo de Software

Desarrollo y mantenimiento de sistemas internos y externos.

##### Área de Soporte Técnico

Soluciona problemas técnicos y realiza mantenimiento de hardware.

##### Área de Seguridad de la Información (SGSI)

###### Jefe de Seguridad de la Información (CISO)

Lidera la gestión del SGSI.

###### Analistas de Seguridad de la Información

Implementan controles de seguridad y monitorean posibles amenazas.

###### Equipo de Respuesta a Incidentes (CSIRT)

Equipo de Respuesta a Incidentes (CSIRT).

### Dirección de Ventas y Marketing

Promueve y gestiona la venta de productos farmacéuticos.

### Dirección de Investigación y Desarrollo (I+D)

Investigación de nuevos medicamentos y tecnologías farmacéuticas.

### Gerentes Regionales

Supervisan varias farmacias en una región, coordinan políticas empresariales y gestionan el rendimiento financiero regional.

### Gerente de tienda

Gestionan las operaciones diarias de una farmacia, incluyendo inventario, ventas y el cumplimiento de normativas.

### Supervisores de Farmacia

Asisten a los gerentes de tienda en la operación diaria, monitoreando el servicio al cliente y las ventas.

### Farmacéuticos

Dispensan medicamentos, brindan asesoramiento a los clientes y aseguren el cumplimiento de normativas de salud y seguridad. Supervisan a los asistentes de farmacia.

### Asistente de farmacia

Apoyan a los farmacéuticos en la gestión de inventarios, atención al cliente, y preparación de medicamentos.

### Personal de atención al cliente

Asesoran a los clientes en sus compras y procesan transacciones en el punto de venta.

### Personal de logística y almacén

Gestionan el inventario y la distribución de productos desde los centros de distribución a las farmacias.

### Cajeros

Procesan las transacciones de compra y manejan cobros. Son responsables del cuadre de caja al final del día.

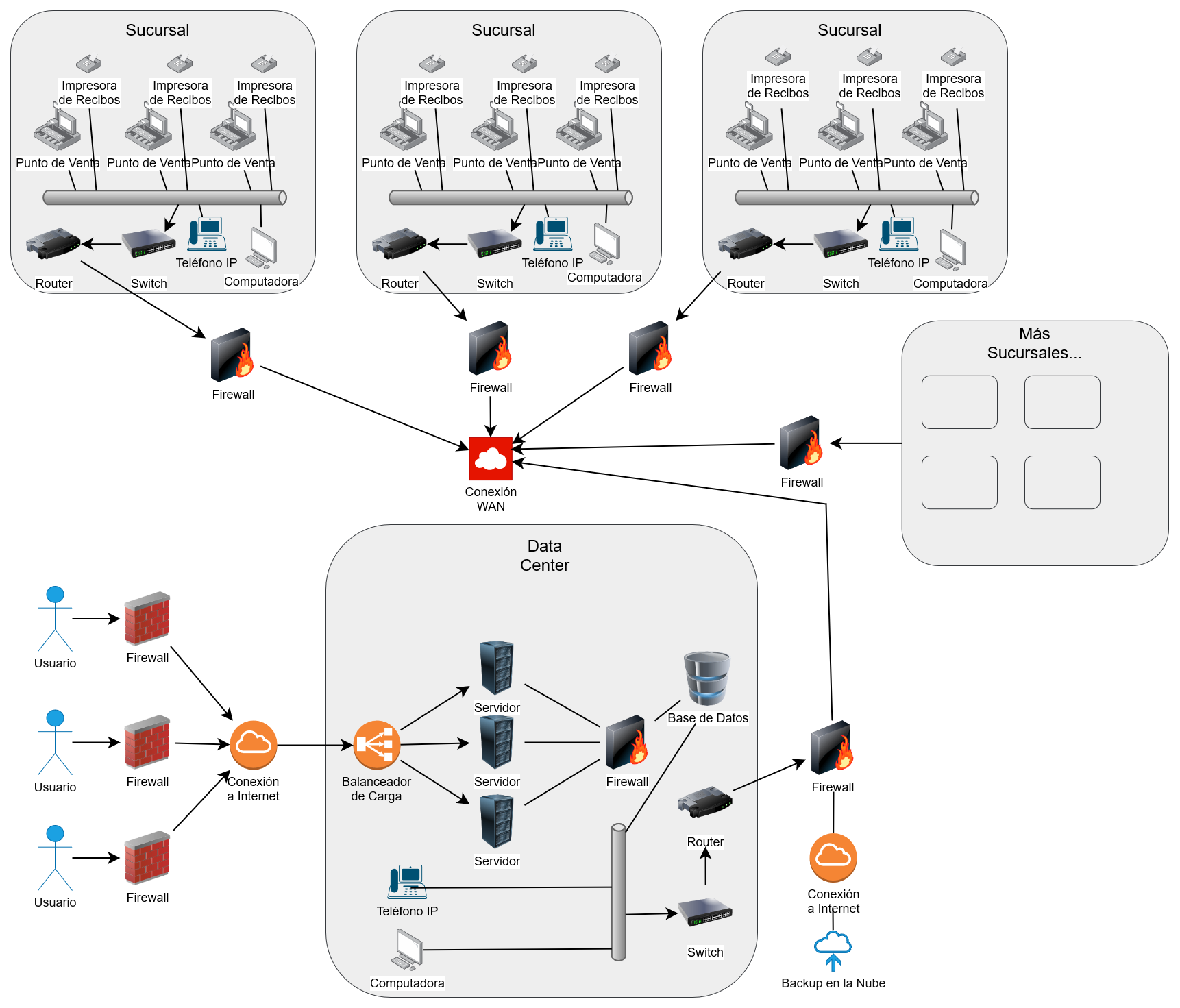
### Personal de limpieza y mantenimiento

Mantienen las instalaciones de la farmacia limpias y aseguran el cumplimiento de los estándares de higiene y seguridad.

## Infraestructura tecnológica de la empresa

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 como se puede observar en la Figura 4.

**Figura 4.**  
Infraestructura tecnológica de la empresa



Nota. El grafico representa la arquitectura física de los componentes de red de la empresa Farmacorp.

### Sucursales

Farmacorp cuenta con 176 sucursales en Bolivia, lo que demanda una infraestructura tecnológica robusta y distribuida para manejar la gestión de ventas, inventarios y atención al cliente en tiempo real en cada ubicación.

### Hardware

Farmacorp opera con una infraestructura de hardware que incluye servidores centrales ubicados en un data center principal para la gestión de datos y operaciones críticas. Además, cada sucursal está equipada con terminales de punto de venta (POS), computadoras y dispositivos móviles para garantizar una operación eficiente. A nivel administrativo, el personal cuenta con laptops y equipos de escritorio conectados a la red corporativa mediante VPN para asegurar el acceso a los sistemas desde cualquier ubicación.

### Software

El software de Farmacorp se basa en soluciones avanzadas para la gestión de precios y optimización de inventarios, utilizando el sistema **Revionics** desde 2014. Este software ha permitido a Farmacorp mejorar sus márgenes de utilidad y aumentar sus ventas en un 20%. La solución de Revionics se complementa con un ERP propio que gestiona inventarios, pedidos y la logística de las sucursales.

### Redes

La infraestructura de red de Farmacorp está construida sobre una red WAN que conecta todas sus sucursales a la oficina central. La conexión de las sucursales se realiza mediante enlaces seguros y redundantes, utilizando routers y switches de fabricantes reconocidos como Cisco. Además, cada sucursal está equipada con sistemas de respaldo para garantizar la continuidad de las operaciones en caso de fallos en la red principal.

### Almacenamiento y Backup

Farmacorp cuenta con una certificación en Buenas Prácticas de Almacenamiento otorgada por Agemed. A nivel digital, la empresa utiliza soluciones de almacenamiento en la nube para el resguardo de datos críticos, en combinación con servidores locales para los datos operativos. Se realizan copias de seguridad diarias, que son almacenadas en la nube y en servidores redundantes ubicados en diferentes sitios geográficos.

### Seguridad

Para proteger su infraestructura tecnológica, Farmacorp emplea una estrategia de seguridad de múltiples capas. Esto incluye firewalls perimetrales, soluciones de detección de intrusos (IDS) y protección antivirus en todos los terminales. El acceso a sistemas críticos está asegurado mediante autenticación multifactor (MFA) y políticas estrictas de contraseñas. Las auditorías de seguridad se realizan periódicamente para detectar y mitigar vulnerabilidades.

### Disponibilidad y Capacidad

La infraestructura tecnológica de Farmacorp está diseñada para manejar grandes volúmenes de transacciones diarias. Gracias a su infraestructura en la nube y a los servidores de alta disponibilidad, la empresa garantiza un tiempo de actividad del 95%. Las soluciones de almacenamiento elástico permiten que la capacidad de procesamiento y almacenamiento se expanda según la demanda, especialmente durante campañas promocionales.

# Objetivo y Alcance

## 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.

## Objetivo Específico

* Realizar un análisis de activos que tienen los diferentes departamentos, identificando y clasificando los activos críticos de cada área en base a los lineamientos que rige la ISO 27001.
* Realizar un análisis exhaustivo de los riesgos que afectan la seguridad de la información en FarmaCorp, en base al marco normativo de Magerit V3
* Diseñar políticas de seguridad para minimizar el impacto de los niveles de riesgo identificados por activo de FarmaCorp, creando políticas de seguridad que incluyan medidas preventivas y correctivas para proteger los activos, basadas en la ISO 27001.

## Alcance

El alcance de este proyecto abarca el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para FarmaCorp, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los datos sensibles y críticos de la empresa, cumpliendo con los estándares internacionales de la norma ISO 27001:2013. Para ello, se llevará a cabo un análisis detallado de los activos en cada departamento, identificando y clasificando los activos críticos, así como un análisis de los riesgos en base al marco normativo Magerit V3. Además, se diseñarán políticas de seguridad que mitiguen los riesgos identificados, incluyendo medidas preventivas y correctivas alineadas con la ISO 27001, para proteger de manera efectiva los activos de la empresa.

# Marco Teórico

## ISO 27000

### ¿Qué es la ISO 27001:2013?

La ISO 27001:2013 es un estándar internacional que proporciona un marco para la gestión de la seguridad de la información. Fue desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) y es parte de la familia de normas ISO/IEC 27000. Esta norma se centra en proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un sistema de gestión de seguridad de la información (SGSI). (International Organization for Standardization, 2013)

### Breve historia de la ISO 27001

La norma ISO 27001 tiene sus raíces en la norma británica BS 7799, publicada originalmente en 1995. La BS 7799 se dividió en dos partes: La primera parte (BS 7799-1) contenía el código de prácticas para la gestión de la seguridad de la información mientras que la segunda parte (BS 7799-2) especificaba los requisitos para un SGSI.

En 2005, estas normas británicas fueron adoptadas y modificadas por la ISO, dando lugar a la primera versión de la ISO/IEC 27001. En 2013, se publicó una revisión significativa del estándar, conocida como ISO/IEC 27001:2013, que alineó mejor la norma con otros sistemas de gestión ISO y actualizó los controles y requisitos para reflejar los cambios en el entorno de la seguridad de la información. (International Organization for Standardization, 2013)

### Descripción de la ISO 27001

La ISO 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Algunos elementos clave de la misma incluyen:

* Contexto de la Organización: Entender el contexto interno y externo de la organización y las partes interesadas relevantes para la seguridad de la información.
* Liderazgo: Establecimiento de roles y responsabilidades claros, compromiso de la alta dirección y la creación de políticas de seguridad de la información.
* Planificación: Identificación de riesgos y oportunidades, y establecimiento de objetivos de seguridad de la información.
* Soporte: Provisión de recursos necesarios, competencia, toma de conciencia, comunicación y control de la documentación.
* Operación: Implementación de controles de seguridad y procesos de tratamiento de riesgos.
* Evaluación del Desempeño: Monitoreo, medición, análisis y evaluación del SGSI.
* Mejora: Gestión de no conformidades y acciones correctivas, y mejora continua del SGSI.

### Beneficios de Implementar ISO 27001:2013

* Protección de la Información: Asegura la confidencialidad, integridad y disponibilidad de la información.
* Cumplimiento Regulatorio: Ayuda a cumplir con leyes y regulaciones relacionadas con la seguridad de la información.
* Confianza de los Clientes: Mejora la confianza de clientes y partes interesadas al demostrar un compromiso con la seguridad de la información.
* Gestión de Riesgos: Proporciona un enfoque sistemático para la gestión de riesgos de seguridad de la información.
* Ventaja Competitiva: Diferencia a la organización en el mercado al demostrar conformidad con un estándar reconocido internacionalmente.

## Familias de la ISO 27000

### ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI)

Proporciona un marco para establecer, implementar, mantener y mejorar un SGSI, asegurando la protección de la información sensible mediante la gestión de riesgos y la implementación de controles de seguridad**.** (International Organization for Standardization, 2013)

### ISO/IEC 27002: Código de Práctica para los Controles de Seguridad de la Información

Ofrece directrices detalladas sobre los controles de seguridad de la información basados en las mejores prácticas internacionales. (International Organization for Standardization, 2022)

### ISO/IEC 27003: Directrices para la Implementación del SGSI

Proporciona orientación sobre la implementación de un SGSI conforme a ISO/IEC 27001. (International Organization for Standardization, 2017)

### ISO/IEC 27004: Gestión de la Medición de la Seguridad de la Información

Proporciona directrices sobre el desarrollo y la operación de un programa de medición de la seguridad de la información, así como sobre la evaluación de la efectividad del SGSI. (International Organization for Standardization, 2016)

### ISO/IEC 27005: Gestión de Riesgos de Seguridad de la Información

Proporciona directrices para la gestión de riesgos relacionados con la seguridad de la información, complementando el enfoque de ISO/IEC 27001. (International Organization for Standardization, 2022)

### ISO/IEC 27006: Requisitos para los Organismos que Realizan Auditoría y Certificación de SGSI

Establece los requisitos para los organismos que ofrecen servicios de auditoría y certificación de SGSI, asegurando su competencia, coherencia e imparcialidad. (International Organization for Standardization, 2024)

### ISO/IEC 27007: Directrices para la Auditoría de SGSI

Proporciona directrices sobre cómo realizar auditorías de SGSI, complementando ISO 19011, que trata sobre la auditoría de sistemas de gestión. (International Organization for Standardization, 2020)

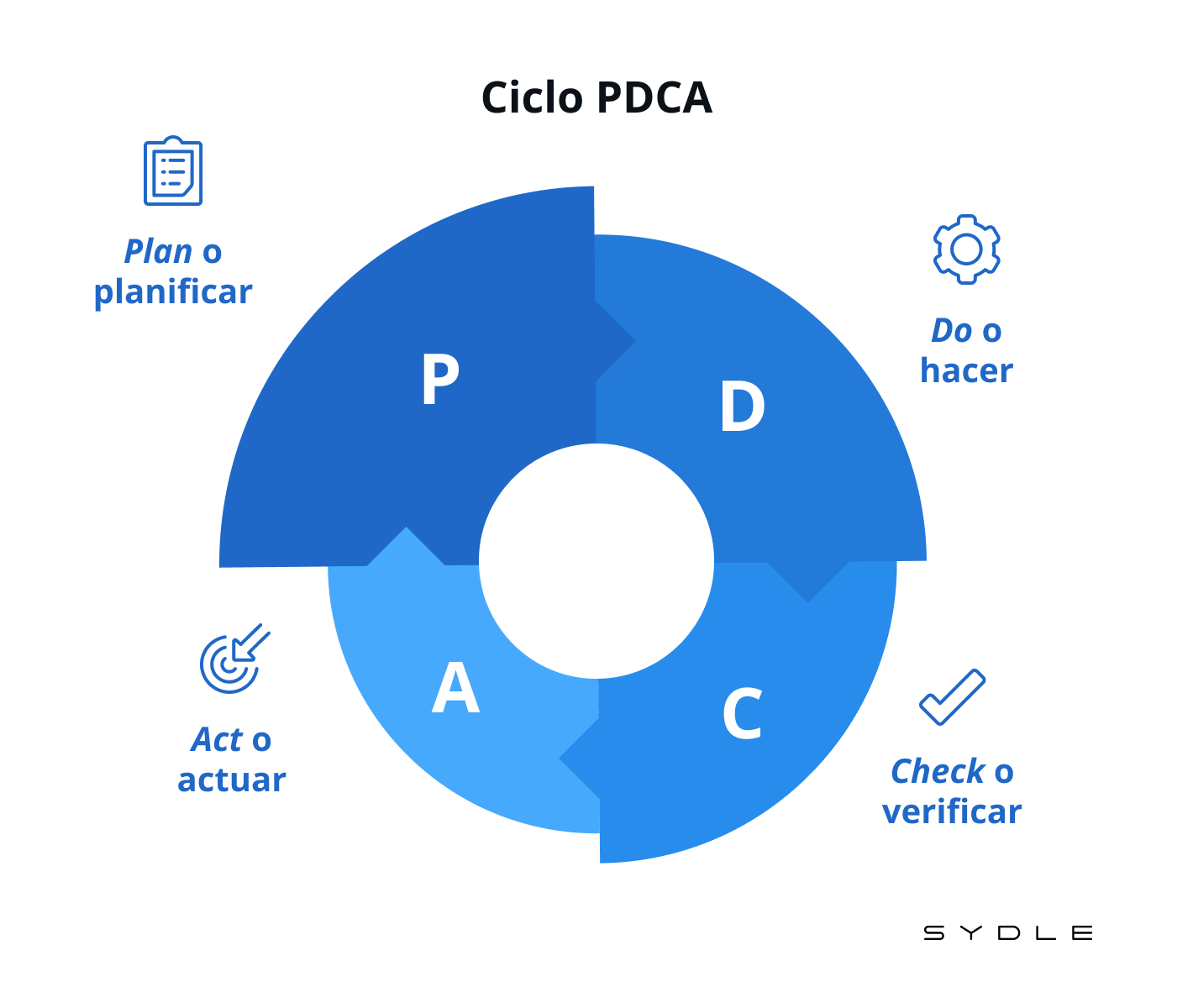
### ISO/IEC 27008: Directrices para la Evaluación de Controles de Seguridad de la Información

Proporciona orientación sobre la evaluación de los controles de seguridad de la información dentro del SGSI. (International Organization for Standardization, 2019)

## Ciclo de Vida

El ciclo de vida PDCA del SGSI está basado en la ISO/IEC 27001. Los tiempos definidos para la realización de cada etapa se muestran reflejados en la Figura 5.

**Figura 5.**Ciclo de vida PDCA



Nota. Adaptada de Mejora continua: descubre sus beneficios y cómo aplicarla. (Sydle, 2022)

### Plan (Planificar)

En esta etapa de planificación se definirá la política de seguridad de la información, estableciendo los principios y objetivos que guiarán la protección de los datos. Se identificarán los objetivos de la institución, asegurando que el SGSI esté alineado con las metas generales de FarmaCorp. Se procederá a documentar los procesos y procedimientos, cubriendo aspectos como la seguridad en el acceso a datos que manejan información sensible. Se definirán los criterios de evaluación de riesgos, lo que permitirá identificar y clasificar los riesgos potenciales que podrían comprometer la seguridad de la información. Se elaborará un inventario de activos, que incluirá todos los recursos físicos, digitales y de software que se deben proteger. Se realizará una valoración de activos, determinando la importancia de cada recurso y su nivel de vulnerabilidad frente a posibles amenazas.

### Do (Hacer)

Durante la fase de implementación, se ejecutarán las medidas planificadas para establecer el SGSI en FarmaCorp. Se comenzará con la identificación de amenazas y vulnerabilidades de los activos, evaluando qué riesgos pueden afectar la seguridad de la información. Con la información recopilada, se elaborará una matriz de riesgos que permita visualizar y priorizar los riesgos según su probabilidad e impacto, ayudando a determinar las áreas que requieren mayor atención.

Con base en la matriz de riesgos, se implementarán los controles identificados, y políticas de acceso seguro. También se establecerán y aplicarán políticas y procedimientos específicos que regulen el uso seguro de la información, la gestión de contraseñas, la protección de datos personales y la respuesta ante incidentes de seguridad. Finalmente se procederá con la capacitación del personal, asegurando que todos comprendan las políticas de seguridad y los procedimientos a seguir para mantener un entorno seguro en la operación diaria de la farmacia.

### Check (Verificar)

Para verificar la efectividad de las acciones tomadas se revisarán los incidentes de seguridad que hayan ocurrido, para identificar si hubo violaciones, pérdida de datos o intentos de ciberataques, y se analizarán las acciones correctivas aplicadas en cada caso. También se realizarán auditorías internas del SGSI para comprobar el cumplimiento de las políticas y la eficacia de los controles implementados, garantizando que todos los procedimientos se estén aplicando correctamente. Los resultados obtenidos se compararán con los objetivos y criterios definidos en la etapa de planificación, permitiendo determinar si se han alcanzado los niveles de seguridad esperados. En caso de discrepancias, se documentarán las áreas de mejora necesarias y se identificarán las posibles causas de cualquier fallo en la implementación de las medidas de seguridad.

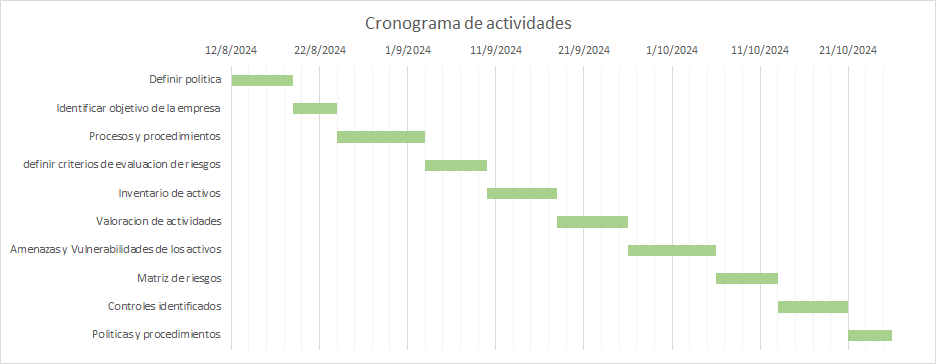
### Act (Actuar)

Con base en los resultados de la verificación, se tomarán decisiones para ajustar y mejorar el SGSI de forma continua. Si se detectan fallos, riesgos no mitigados o nuevas amenazas, se procederá a realizar ajustes en los controles de seguridad existentes, actualizar las políticas y procedimientos, y reforzar la formación del personal. Además, se estandarizarán los procesos que hayan demostrado ser efectivos, para asegurar que se mantengan de manera consistente en toda la organización. Todas las mejoras y cambios se documentarán para fortalecer el sistema y facilitar futuros ciclos de mejora continua. Este proceso de retroalimentación asegurará que el SGSI de FarmaCorp evolucione y se mantenga actualizado, adaptándose a las nuevas amenazas y cambios en el entorno, garantizando la protección constante de la información sensible de la empresa. Los plazos para la implementación de mejoras se definirán en función de la prioridad de cada riesgo identificado y la complejidad de las acciones requeridas.

# Desarrollo del Proyecto

## Cronograma del Proyecto

**Figura 6.**Cronograma del Proyecto



Nota. El grafico es un cronograma de las diferentes actividades para poder concluir el proyecto en sus diferentes fechas.

## Fase 1: Planificación

### Definir política.

#### Objetivo.

La presente política tiene como finalidad garantizar la confidencialidad, integridad y disponibilidad de la información en Farmacorp, en conformidad con la norma ISO 27001:2013 y los requisitos legales vigentes, asegurando su correcta administración, almacenamiento, acceso y transmisión. Asimismo, busca alinearse con los objetivos estratégicos de la organización, que incluyen la provisión segura y eficiente de productos y servicios de salud a través de sus sucursales y plataformas digitales.

#### Alcance.

Esta política aplica a todos los empleados, contratistas y proveedores de Farmacorp que accedan a los sistemas de información y datos, tanto digitales como físicos de Farmacorp. Cubre todas las tecnologías, datos, sistemas y recursos informáticos que soportan las operaciones diarias de la empresa, tanto en sus instalaciones físicas como en sus canales digitales.

#### Directrices

##### Confidencialidad

Toda la información sensible debe ser protegida contra acceso no autorizado. Solo personal autorizado y capacitado podrá acceder a dicha información.

##### Integridad

La información debe ser precisa y completa. Todos los sistemas y procesos deben ser diseñados para prevenir la alteración no autorizada de los datos.

##### Disponibilidad

La información debe estar disponible para los usuarios autorizados cuando sea necesaria para sus funciones.

### Identificar objetivos de la institución.

* El objetivo principal de Farmacorp es garantizar el acceso de las familias bolivianas a medicamentos y servicios de salud de alta calidad, asegurando la satisfacción del cliente a través de la innovación, el cumplimiento de normativas y la mejora continua en base a una infraestructura segura.
* El objetivo de implementar un Sistema de Gestión de Seguridad de la Información en Farmacorp es proteger la integridad, confidencialidad y disponibilidad de la información sensible y crítica relacionada con la salud y los medicamentos. El sistema busca asegurar la continuidad y eficiencia de los procesos internos y servicios prestados, en cumplimiento con normativas del sector farmacéutico y de seguridad de la información.
* El objetivo de asegurar el cumplimiento de normativas y estándares internacionales en Farmacorp es garantizar que la gestión de la seguridad de la información cumpla con regulaciones internacionales, como ISO/IEC 27001. Este objetivo busca proteger la información, asegurando la correcta gestión de riesgos y el cumplimiento de los requisitos legales, particularmente en relación con datos de los clientes y proveedores del sector salud.

El objetivo de fortalecer la seguridad de la información en Farmacorp es asegurar la identificación y mitigación de riesgos relacionados con, accesos no autorizados y vulnerabilidades tecnológicas que puedan comprometer la protección de la información sensible.

### Procesos y procedimientos.

Tabla 1. Procesos y procedimientos

|  |  |  |
| --- | --- | --- |
| Proceso | Procedimiento | Acciones |
| Falta de un gobierno de Seguridad en Farmacorp | Creación de un Comité de Seguridad de la Información | Formar un comité formado por miembros de la alta dirección y responsables de cada área seleccionada.  Definir roles y responsabilidades dentro del comité.  Crear un plan de reuniones para revisar las políticas de seguridad |
| Elaboración de un Plan de Seguridad | Realizar una evaluación de riesgos y establecer prioridades estratégicas.  Definir objetivos de seguridad alineados con los objetivos organizacionales de la empresa de Farmacorp.  Desarrollar un plan de acción con plazos y responsables claros. |
| Falta de un Proceso Formal para la Gestión de Incidentes de Seguridad | Establecimiento de un Proceso de Gestión de Incidentes de Seguridad | Definir y documentar un proceso detallado para la identificación, clasificación, y respuesta a incidentes de seguridad.  Crear un sistema de registro de incidentes accesible a todos los empleados. |
|
| Formación en Gestión de Incidentes | Formar al equipo de respuesta en técnicas de análisis forense, contención y mitigación de incidentes  Realizar simulacros de incidentes para mejorar la preparación y la respuesta coordinada  Actualizar el proceso de gestión de incidentes basándose en las lecciones aprendidas de incidentes reales y simulaciones |
| Inexistencia de Políticas y Procedimientos de Seguridad | Definición de Políticas de Seguridad de la Información | Desarrollar políticas específicas para la protección de datos médicos y control de acceso.  Aprobar y comunicar las políticas a todos los empleados de Farmacorp. |
| Creación de Procedimientos Operativos | Establecer procedimientos específicos para la gestión de accesos, manejo de incidentes, y uso de tecnologías de la información.  Documentar cada procedimiento con pasos claros y detallados.  Capacitar a los empleados en la implementación y seguimiento de estos procedimientos. |
| Ausencia de Control de Acceso y Gestión de Identidades en Sistemas de Información Médica | Implementación de un Sistema de Gestión de Identidades | Implementar una solución para gestionar identidades y accesos en sistemas de salud, protegiendo la confidencialidad de los datos médicos.  Definir procesos claros para la creación, modificación y eliminación de cuentas de usuario, limitando el acceso solo a personal autorizado.  Incorporar autenticación robusta y autorización basada en roles para restringir el acceso según las funciones del personal. |
|
| Desarrollo de Políticas de Control de Acceso | Definir y documentar políticas de acceso basadas en la necesidad de saber y el principio de privilegios mínimos.  Realizar revisiones periódicas de los accesos otorgados y ajustar según cambios en roles o responsabilidades.  Implementar monitoreo y auditoría continua de los accesos a la información. |
| Ausencia de un Programa de Concienciación en Seguridad | Implementación de un Programa de Concienciación en Seguridad | Desarrollar materiales educativos que promuevan la cultura de seguridad de la información en Farmacorp.  Realizar capacitaciones, talleres, seminarios y cursos eventualmente sobre buenas prácticas de seguridad de la información en la industria farmacéutica y médica |
|
| Campañas de Sensibilización Continua | Desplegar boletines informativos y actualizaciones sobre amenazas emergentes y mejores prácticas.  Utilizar diferentes medios (intranet, correos, posters) para mantener la concienciación sobre la importancia de la seguridad de la información. |
| Falta de un Proceso Formal para la Gestión de Incidentes de Seguridad | Establecimiento de un Proceso de Gestión de Incidentes de Seguridad | Definir y documentar un proceso detallado para la identificación, clasificación, y respuesta a incidentes de seguridad.  Crear un sistema de registro de incidentes accesible a todos los empleados. |
| Capacitación en Gestión de Incidentes | Formar al equipo de respuesta en técnicas de análisis forense, contención y mitigación de incidentes  Realizar simulacros de incidentes en seguridad para mejorar la respuesta coordinada |
| Insuficiente Protección de Información de Pacientes y Personal en Farmacorp | Evaluación y Mejora de la Protección de Información | Realizar una evaluación exhaustiva de riesgos centrada en los sistemas que almacenan información crítica sobre pacientes y personal,  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 |
|
| Implementación de Medidas de Seguridad de la Información | Desarrollar un plan de capacitación para el personal en buenas prácticas de seguridad de la información, incluyendo la gestión de contraseñas y el manejo seguro de datos.  Realizar auditorías periódicas de seguridad para evaluar la eficacia de las medidas implementadas y hacer ajustes según sea necesario. |

### Definir criterios de evaluación.

Para los criterios de evaluación de los activos en Farmacorp, utilizaremos las siguientes categorías que aseguran que cada activo de información se clasifique y gestione adecuadamente, de acuerdo con su nivel de sensibilidad, impacto potencial en las operaciones y la seguridad de la organización.

#### Clasificación

Clasificamos los activos de información se clasifican en tres categorías principales. Esta clasificación asegura que cada activo se maneje según su nivel de sensibilidad y el impacto que una eventual falla o acceso no autorizado pueda tener en la operación diaria, la seguridad de los pacientes y el cumplimiento regulatorio.

Tabla 2. Clasificación

|  |  |
| --- | --- |
| Clasificación | |
| Pública | Información, sistema o instalaciones a disposición del público |
| Privada | Información, sistemas o instalaciones se restringe exclusivamente para uso interno de la institución |
| Confidencial | Información sensible de la institución, restringida a un grupo limitado de personas |

#### Valoración de activos

Para la valoración de activos se tienen los siguientes criterios basados en el triaje d la información (Confidencialidad, Integridad y Disponibilidad.)

##### Confidencialidad

Es fundamental evaluar la confidencialidad de los activos de información relacionados con los pacientes, personal y proveedores de Farmacorp. Estos activos deben manejarse de acuerdo a su nivel de sensibilidad para asegurar que solo las personas autorizadas puedan acceder a ellos. Los criterios para evaluar la confidencialidad de los activos proporcionan una guía clara sobre cómo clasificar y proteger esta información, garantizando que se mantenga privada y segura.

Tabla 3. Valor del Activo - Confidencialidad

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Muy bajo | De conocimiento público |
| 2 | Bajo | De conocimiento interno |
| 3 | Medio | De conocimiento privado |
| 4 | Alto | De conocimiento confidencial |
| 5 | Muy Alto | De conocimiento restringido |

##### Disponibilidad

Para asegurar la continuidad de las operaciones farmacéuticas en Farmacorp, los activos de información se clasifican también en función de su disponibilidad. Esta clasificación ayuda a determinar el impacto potencial que tendría la falta de acceso o la pérdida de un activo sobre la operación diaria, la cadena de suministro de medicamentos y los servicios esenciales que brindamos a las familias bolivianas.

Tabla 4. Valor del Activo - Disponibilidad

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Muy bajo | Disponible en cuestion de minitos |
| 2 | Bajo | Disponible en cuestion de horas |
| 3 | Medio | Disponible en 2 a 4 dias |
| 4 | Alto | Disponible en mas de una semana |
| 5 | Muy Alto | Irrecuperable |

##### Integridad

Para proteger la integridad de los activos de información en Farmacorp, es crucial clasificar los activos según su importancia y el impacto potencial que podría tener una modificación no autorizada o un daño. La integridad de la información es esencial para garantizar que los datos sean precisos, completos y confiables, ya que cualquier alteración podría afectar gravemente las operaciones y la toma de decisiones. La siguiente clasificación describe cómo se valora la integridad de los activos y justifica su uso en la empresa.

Tabla 5. Valor del Activo - Integridad

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Muy bajo | Facil de obtener o reemplazar |
| 2 | Bajo | Se puede obtener pero no de manera inmediata |
| 3 | Medio | Se puede obtener a costos razonables |
| 4 | Alto | Se puede obtener con mucha dificultad |
| 5 | Muy Alto | Imposible de recuperar al 100% |

##### Estimación de Impacto

En la empresa de Farmacorp, la estimación del impacto se centra en evaluar las consecuencias que un incidente relacionado con la seguridad de la información podría generar en las operaciones, la reputación y el cumplimiento normativo. Este criterio clasifica el impacto en niveles desde muy bajo hasta muy alto, considerando la capacidad de la organización para manejar las consecuencias con recursos disponibles.

Tabla 6. Valor del Activo – Estimación de Impacto

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Muy bajo | El impacto es mínimo y apenas puede afectar a la institución, las consecuencias son facilmente manejables |
| 2 | Bajo | El impacto es bajo y tiene un efecto limitado para la institución, puede resolverse con recursos moderados. |
| 3 | Medio | El impacto es moderado y afecta significativamente a la institución, requiere una atención y recursos considerables para su resolución. |
| 4 | Alto | El impacto es alto y puede causar daños considerables para la institución, requiere una acción inmediata y recursos importantes para mitigarlo. |
| 5 | Muy Alto | El impacto es muy alto y tiene consecuencias devastadoras para la institución, requiere una acción urgente y asignación masiva de recursos para su manejo. |

##### Probabilidad de Ocurrencia

El análisis de probabilidad en Farmacorp determina la posibilidad de que ocurra un incidente de seguridad de la información. Este criterio permite priorizar riesgos al identificar áreas con mayor vulnerabilidad y necesidades de mejora en controles.

Tabla 7. Valor del Activo – Probabilidad de Ocurrencia

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Muy bajo | No es necesario controles, es irrelevante |
| 2 | Bajo | Controles seguros, baja probabilidad de incidentes futuros |
| 3 | Medio | Controles moderados, mediana probabilidad de incidentes futuros |
| 4 | Alto | Controles ineficientes, alta probabilidad de incidentes futuros |
| 5 | Muy Alto | Inexistencias de controles |

##### Riesgo o Nivel de Riesgo

El nivel de riesgo en Farmacorp combina el impacto y la probabilidad de ocurrencia para evaluar la amenaza que un incidente representa para la organización. Esto permite priorizar riesgos críticos y asignar recursos adecuados para su mitigación.

Tabla 8. Valor del Activo – Inventario de Activos

|  |  |  |
| --- | --- | --- |
| Valor | | Descripción |
| 1 | Bajo | El riesgo es manejable y las consecuencias son mínimas o fácilmente mitigables |
| 2 | Medio | El riesgo tiene un impacto significativo y puede requerir acciones para mitigarlo. |
| 3 | Alto | El riesgo representa una amenaza considerable y puede causar daños importantes si no se gestiona adecuadamente |
| 4 | Extremo | El riesgo es muy significativo y puede tener consecuencias graves si no se controla de manera efectiva |
| 5 | Catastrófico | El riesgo representa una amenaza catastrófica y puede resultar en pérdidas irreparables o la pérdida total. |

### Inventario de Activos

Tabla 6. Inventario de Activos





## Fase 2. Hacer

### Catálogo de Amenazas

El catálogo de amenazas es fundamental para identificar, analizar y gestionar los riesgos que podrían afectar a los activos del SGSI de Farmacorp. Al considerar las posibles amenazas, como ciberataques, errores humanos, fallos tecnológicos o desastres naturales, se garantiza un enfoque preventivo y reactivo en la protección de la confidencialidad, integridad y disponibilidad de la información. Este catálogo permite priorizar recursos y establecer controles efectivos para minimizar impactos, alineándose con los objetivos de seguridad y la normativa ISO 27001.

Tabla 7. Catálogo de Amenazas









### Análisis de Riesgo

Tabla 8. Análisis de Riesgo

















### Matriz de Riesgo

Tabla 9. Matriz de Riesgo



### Políticas de seguridad

#### Política de Mitigación del Riesgo de Falla de Hardware del Sistema de Respaldo

* **Objetivo:** Minimizar el impacto de una posible falla de hardware en el sistema de respaldo mediante evaluaciones, monitoreo, mantenimiento preventivo y simulaciones de fallos. Estas acciones, junto con la implementación de redundancias y la capacitación del personal, asegurarán la disponibilidad de los datos y la continuidad de los servicios críticos, permitiendo una respuesta rápida y efectiva ante fallas de hardware.
* **Procedimientos:**

Tabla 10. Procedimientos para Política de Mitigación del Riesgo de Falla de Hardware del Sistema de Respaldo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividad | Sub actividad | Registros |
| PS-01 | Área de soporte técnico. | Realizar una evaluación inicial del sistema de respaldo, incluyendo el análisis de su capacidad actual y el estado de hardware. | Evaluar la capacidad de almacenamiento, el procesamiento actual y el estado físico y funcional del hardware. (Anexo P01.1) | Informe de evaluación de capacidad y estado del hardware. |
| Identificar necesidades de actualización o reemplazo de componentes. (Anexo P01.2) |
| Documentar anomalías o signos de desgaste en el hardware. (Anexo P01.3) |
| PS-02 | Área de soporte técnico. | Establecer un cronograma de mantenimiento preventivo para el sistema de respaldo. | Crear un calendario de mantenimiento periódico (trimestral/semestral) para inspección de hardware. | Calendario de mantenimiento y registros de mantenimiento realizados. |
| Registrar los resultados y acciones correctivas de cada mantenimiento. (Anexo P01.4) |
| Ajustar el cronograma en función de los hallazgos en cada revisión para optimizar la prevención de fallos. |
| PS-03 | Dirección de Tecnología e informática (CIO). | Monitorear y gestionar la redundancia en el sistema de respaldo para mitigar el impacto fallas de hardware. | Manejar el método RAID para la redundancia en el hardware. (Anexo P01.5) | Documentación de redundancia de hardware y pruebas de funcionalidad. |
| Realizar pruebas periódicas de funcionalidad para asegurar la efectividad de la redundancia. |
| Documentar la configuración y el proceso de implementación de la redundancia. (Anexo P01.6) |
| PS-04 | Área de seguridad de la Información (SGSI). | Realizar simulaciones de fallas en el hardware del sistema de respaldo para probar y mejorar los procedimientos de recuperación. | Planificar y ejecutar simulaciones periódicas de fallas en componentes clave del sistema de respaldo. (Anexo P01.7) | Informe de pruebas de recuperación, incluyendo resultados y recomendaciones de mejora. |
| Registrar tiempo de respuesta y los resultados de cada simulación. (Anexo P01.8) |
| Analizar los resultados y recomendar mejoras en los procedimientos de recuperación si es necesario. |
| PS-05 | Área de seguridad de la Información (SGSI). | Monitorear continuamente el hardware del sistema de respaldo para detectar fallas inminentes. | Realizar el procedimiento de monitoreo en tiempo real para supervisar el estado del hardware con Zabbix. (Anexo P01.9) | Registro de monitoreo continuo y reportes de alertas. |
| Documentar y notificar cualquier anomalía detectada al área de soporte técnico para su resolución. (Anexo P01.10) |
| PS-06 | Jefe de seguridad de la información (CISO). | Capacitar al personal involucrado en la operación y mantenimiento de hardware del sistema de respaldo para que comprendan los procedimientos de respuesta ante fallas. | Organizar sesiones de capacitación sobre procedimientos de respuesta y recuperación. | Registro de capacitación y actualización de habilidades del personal. |
| Evaluar periódicamente el conocimiento y habilidades del personal para asegurar su preparación. |

#### Política de Seguridad Física para Acceso No Autorizado

* **Objetivo:** Reforzar o 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.
* **Procedimientos:**

Tabla 11. Procedimientos para Política de Seguridad Física para Acceso No Autorizado

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividades | Sub Actividades | Registros |
| 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) | **Listado de personal autorizado, registros de acceso físico, informe de auditoría de acceso.**  Registro de clasificación y actualización de áreas restringidas.  Registro de cambios en la configuración de dispositivos de control de acceso físico.  Registro de eventos de acceso físico (logs de entrada y salida).  Registro de auditorías de acceso físico y sus resultados. |
| **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 de los controles de acceso físico y detectar posibles fallas o vulnerabilidades en el sistema. (Anexo P02.3) |
| PS-08 | Supervisor de Seguridad junto con el Equipo de Monitoreo de Seguridad Física. | **2. Vigilancia y Monitoreo en Áreas Críticas** | **Supervisión de Cámaras Instaladas**  Supervisar y verificar el correcto funcionamiento de las cámaras de seguridad previamente instaladas en las áreas críticas. (Anexo P02.4) | **Registro de mantenimiento de equipos, grabaciones de vigilancia, informe de monitoreo.**  Registro de inspecciones de funcionamiento de cámaras.  Registro de eventos o incidentes detectados durante el monitoreo.  Registro de almacenamiento y acceso a grabaciones.  Registro de mantenimiento y revisión técnica de los equipos de vigilancia. |
| **Monitoreo Continuo de Video Vigilancia**  Realizar la observación constante de las áreas críticas a través del sistema de vigilancia, identificando cualquier incidente o irregularidad en tiempo real. (Anexo P02.5) |
| **Gestión de Grabaciones de Video**  Controlar, organizar y garantizar el almacenamiento seguro de las grabaciones generadas por las cámaras de seguridad. |
| **Inspecciones y Mantenimiento de Equipos de Vigilancia**  Realizar revisiones periódicas de los equipos de vigilancia para asegurar su operatividad y evitar fallos en el sistema. |
| PS-09 | Administrador de Credenciales y Acceso, supervisado por el Departamento de Recursos Humanos y el Departamento de Seguridad. | **3. Gestión de Identificación y Credenciales Físicas** | **Control de Credenciales Emitidas**  Supervisar y gestionar las credenciales de identificación ya emitidas, asegurando que se mantengan actualizadas y sean asignadas exclusivamente al personal autorizado. (Anexo P02.6) | **Base de datos de credenciales emitidas, registros de acceso con verificación de identidad.** Registro maestro de credenciales emitidas (fecha, usuario, nivel de acceso).  Registro de credenciales revocadas o actualizadas.  Registro de incidentes de acceso y validaciones realizadas. |
| **Revocación y Actualización de Credenciales Activas**  Reconfigurar, actualizar o revocar las credenciales físicas de identificación de acuerdo con los cambios en los permisos de acceso o la desvinculación de personal. (Anexo P02.7) |
| **Validación y Autenticación en Puntos de Acceso**  Monitorear el uso correcto de credenciales físicas mediante controles de autenticación en los puntos de acceso. (Anexo P02.8) |

#### Política de Lógica 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.
* **Procedimientos:**

Tabla 12. Procedimientos para Política de Lógica para Acceso No Autorizado

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividades | Sub Actividades | Registros |
| P1-02 | Administrador de Seguridad Lógica, en colaboración con el Departamento de TI. | 1. Gestión de Autenticación y Autorización | Reconfigurar Políticas de Contraseñas  Ajustar las políticas de contraseñas existentes para cumplir con estándares actuales de seguridad, incluyendo criterios de longitud, complejidad, y caducidad. (Anexo P03.1) | Documento donde se detalla la nueva configuración realizada, incluyendo la fecha y responsable.  Registro de modificaciones realizadas como resultado de la validación.  Registro de logs donde se registran todos los intentos de acceso exitosos y fallidos. |
| Validar Roles y Permisos Asignados  Realizar una revisión exhaustiva de los roles y permisos asignados a usuarios para garantizar que se aplican principios de privilegio mínimo. |
| Monitorear Intentos de Acceso  Supervisar continuamente los intentos de acceso al sistema para identificar patrones sospechosos o intentos reiterados de acceso no autorizado. (Anexo P03.2) |
| Equipo de Seguridad de la Información, supervisado por el Oficial de Cumplimiento de Seguridad. | 2. Monitoreo y Detección de Acceso No Autorizado | Reconfigurar Parámetros de Monitoreo de Accesos  Ajustar las configuraciones de los sistemas de monitoreo para incluir alertas en tiempo real de intentos de acceso fallidos, accesos desde ubicaciones no reconocidas, o fuera de horarios laborales. (Anexo P03.3) | Registro que documente los parámetros ajustados, fecha, responsable y motivo.  Resumen periódico con base a los logs de alertas críticas detectadas y su estado.  Registro de logs de acciones aplicadas para mitigar los riesgos detectados. |
| Alertas Generadas por el Sistema  Revisar las alertas generadas por los sistemas de monitoreo para identificar patrones o eventos que podrían indicar intentos de acceso no autorizado. |
| Escalar y Mitigar Incidentes Detectados  Escalar los incidentes de acceso no autorizado detectados al equipo de seguridad correspondiente y aplicar medidas de contención como bloqueo de cuentas, cierre de sesiones, o ajustes en los permisos afectados. |
| Administrador de Redes y Seguridad. | 3. Seguridad en VPN y Acceso Remoto | Reconfigurar los Parámetros de Seguridad de la VPN  Actualizar las configuraciones de la VPN para fortalecer su seguridad, como habilitar cifrado avanzado, configurar autenticación multifactor (MFA) y restringir direcciones IP permitidas. | Documento que detalle los parámetros ajustados, el responsable, y la fecha de aplicación.  Logs donde se detallen todas las conexiones realizadas a través de la VPN.  Registro de equipos o cuentas bloqueadas por actividad anómala. |
| Monitorear Actividad de Acceso Remoto  Supervisar los accesos a través de la VPN, detectando conexiones desde ubicaciones inusuales, horarios no autorizados, o dispositivos no reconocidos. |
| Escalar y Responder a Accesos Sospechosos  Responder a eventos sospechosos, como conexiones no autorizadas o intentos reiterados de acceso, bloqueando las sesiones comprometidas y notificando al equipo de seguridad. |
| Administrador de Seguridad de la Información junto con el Equipo de Auditoría de TI. | 4. Auditoría de Accesos y Permisos | Recolectar y Consolidar Registros de Acceso  Extraer y unificar los registros de accesos y permisos asignados desde los sistemas de información relevantes (logs de acceso, bases de datos de permisos, y sistemas de monitoreo). | Validación de la integridad de los datos recolectados.  Comparativa de los permisos asignados frente a los definidos en los roles.  Registro de logs de los cambios realizados en los permisos, indicando usuarios, fecha, responsable y justificación. |
| Analizar y Comparar Permisos Asignados con Roles Definidos  Evaluar los permisos otorgados a los usuarios comparándolos con los roles establecidos para identificar excesos de privilegios o inconsistencias. |
| Reconfigurar Permisos No Conformes Detectados  Realizar los ajustes necesarios en los permisos identificados como inconsistentes o excesivos, devolviéndolos al marco definido por los roles establecidos. |

#### Política de Modificación Deliberada de la Información en el Software de Gestión de Contratos

* **Objetivo:** Proteger la integridad y disponibilidad de la información en el Software de Gestión de Contratos mediante la implementación de medidas estratégicas y operativas, con el fin de garantizar la confiabilidad de los datos, prevenir modificaciones no autorizadas y asegurar la continuidad operativa del sistema.
* **Procedimientos:**

Tabla 13. Procedimientos para Política de Modificación Deliberada de la Información en el Software de Gestión de Contratos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividad | Sub Actividades | Registros |
| PS-10 | Área de Seguridad de la Información | Capacitación sobre Política de Seguridad para el Personal | Organizar sesiones de capacitación para todo el personal involucrado en la gestión de contratos. | Lista de Asistencia y Evaluación de Capacitación |
| Proporcionar y distribuir material educativo, como manuales y guías prácticas, sobre el uso seguro del sistema y la correcta gestión de la información. |
| Capacitar a los empleados sobre políticas de modificación y acceso a la información. |
| Evaluar la comprensión del personal sobre los protocolos de seguridad. |
| **PS-11** | Área de Soporte Técnico | Gestión de Backup y Recuperación de Información | Realizar copias de seguridad de la base de datos de contratos, asegurando que los datos esenciales estén protegidos. | Registro de Copias de Seguridad y Recuperación |
| Probar la recuperación de la información a partir de las copias de seguridad realizadas, verificando su integridad y disponibilidad para su uso inmediato. |
| Corregir cualquier problema o error encontrado durante las pruebas de recuperación. (P04.1) |
| **PS-12** | Equipo de respuesta a incidentes | Detección y Respuesta ante Intentos de Modificación no Autorizados | Mantener actualizados los sistemas IDS. (P04.2) | Informe de alertas de seguridad que contiene registro de todas las alertas generadas por intentos de acceso no autorizados y modificaciones detectadas. |
| Monitorear continuamente el tráfico y actividades en el software |
| Alertas en caso de intento de modificación no autorizado. |
| Ejecutar protocolos de respuesta rápida en caso de confirmarse una alteración malintencionada. (P04.3) |
| **PS-13** | Administrador de Seguridad de TI | Control de Acceso al Sistema | Establecer los roles y funciones de cada usuario. (P04.4) | Registro de Control de Acceso y Permisos de Usuarios |
| Asignar y configurar permisos específicos de acceso y modificación en el software. (P04.5) |
| Revisar los accesos y permisos periódicamente, asignando accesos únicamente al personal autorizado. (P04.6) |
| Supervisar el uso de autenticación multifactor para usuarios con permisos de modificación de información, verificando el correcto funcionamiento y la seguridad de este sistema de autenticación. (P04.7) |
| **PS-14** | Jefe de Seguridad de la Información | Auditorías Periódicas | Programar auditorías internas trimestrales para revisar los accesos y modificaciones en el sistema. | Informe de Auditoría Trimestral |
| Analizar los registros de acceso y modificación para verificar que se mantenga la integridad de la información, documentando cualquier anomalía encontrada. |
| Generar un informe detallado con hallazgos, recomendaciones y cualquier medida correctiva propuesta para asegurar la continuidad en la seguridad de los datos. (P04.8) |

#### Política de Ataque de Ransomware que afecte los Datos Respaldados

* **Objetivo:** Prevenir y mitigar los riesgos asociados con los ataques de ransomware mediante la implementación de controles que protejan la información crítica, aseguren la continuidad operativa y garanticen una respuesta eficiente para minimizar el impacto de estos incidentes.
* **Procedimientos:**

Tabla 14. Procedimientos para Política de Ataque de Ransomware que afecte los Datos Respaldados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividad | Sub Actividades | Registros |
| PS-15 | Área de Seguridad de la Información | Sensibilización y Formación en Ciberseguridad | Implementar un sistema de certificación interna para empleados capacitados. | Listado de Participantes y Resultados de Simulaciones |
| Realizar simulaciones de ataques de phishing para evaluar la respuesta del personal. (Anexo P05.1) |
| Organizar talleres interactivos sobre riesgos asociados al ransomware. |
| PS-16 | Área de Soporte Técnico | Estrategias de Respaldo y Recuperación de Datos | Establecer un plan de respaldo automatizado con frecuencia diaria para los datos críticos. | Reporte de Auditorías de Respaldos y Pruebas de Recuperación |
| Asegurar que los respaldos se mantengan en entornos aislados y protegidos contra alteraciones externas. (Anexo P05.2) |
| Realizar simulacros de recuperación total para validar los tiempos de respuesta y efectividad. |
| PS-17 | Equipo de respuesta a incidentes | Detección y Respuesta ante Intentos de modificación malintencionada | Mantener la copia paralela de los datos en un entorno diferente al respaldo principal | Informe de alertas de seguridad que contiene registro de todas las alertas generadas por intentos de modificación no autorizado |
| Monitorear de forma continua el acceso a los datos |
| PS-18 | Administrador de Seguridad de TI | Control de acceso a los datos | Establecer roles y permisos restringidos hacia los datos a los por parte de los usuarios. (Anexo P05.3) | Informe de accesos realizados y cambios en los permisos de usuario |
| Hacer revisiones periódicas de los permisos de los usuarios |
| Mantener la los sistemas de seguridad actualizados contra intrusiones |

#### Política de Protección contra la Pérdida y Destrucción de Datos en Software

* **Objetivo:** Minimizar el riesgo asociado a la destrucción no autorizada o accidental de información en el software, garantizando la disponibilidad y la integridad de los datos críticos para asegurar la continuidad de los servicios y la protección de la información.
* **Procedimientos:**

Tabla 15. Procedimientos para Política de Protección contra la Pérdida y Destrucción de Datos en Software

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividad | Sub. Actividades | Registros |
| PS-19 | Encargado de Jefe de Seguridad de la Información (CISO) | Configurar registros detallados de auditoría que registren todas las acciones relacionadas con la modificación o eliminación de datos. | Identificar y definir qué tipos de eventos deben ser registrados, tales como modificaciones, eliminaciones, accesos no autorizados o intentos fallidos de modificación. (Anexo P06.1) | Informes periódicos de registros de auditoría. |
| Uso de las herramientas o tecnologías más adecuadas en el software para llevar a cabo el registro de auditoría. (Anexo P06.2) |
| Configurar la funcionalidad de auditoría en el sistema de software, asegurando que se registren las acciones de modificación y eliminación de datos de acuerdo con los requisitos establecidos. (Anexo P06.3) |
| Seguir el procedimiento para almacenar los registros de auditoría de manera segura, asegurando que no sean modificados o eliminados por usuarios no autorizados. Se generan informes de estos periódicamente. (Anexo P06.4) |
| PS-20 | Encargado de Jefe de Seguridad de la Información (CISO) | Establecer regulaciones de quién y cómo puede eliminar datos en el sistema. Limitar la eliminación de datos solo a personal autorizado y bajo condiciones específicas. | Clasificar los tipos de datos que son susceptibles de eliminación, diferenciando entre datos temporales, datos sensibles, y datos que deben conservarse por razones legales o de auditoría. (Anexo P06.5) | Formularios de eliminación, Informe de la capacitación sobre las regulaciones de eliminación de información |
| Establecer los niveles de autorización necesarios para la eliminación de datos. Por ejemplo, especificar que solo personal con ciertos roles o jerarquías pueda aprobar la eliminación de datos, y qué documentos o registros de aprobación se requieren. (Anexo P06.6) |
| Seguir un proceso formal para que el personal solicite la eliminación de datos, incluyendo un formulario de solicitud o un sistema de gestión de tickets que permita la aprobación o rechazo de dichas solicitudes. (Anexo P06.7) |
| PS-21 | Encargado de Jefe de Seguridad de la Información (CISO) | Configurar copias de seguridad regulares y automáticas de la base de datos  y de la información crítica almacenada en el software. | Clasificar los datos críticos que deben ser respaldados, como bases de datos, archivos de configuración del software, registros de auditoría, y cualquier otro dato sensible o importante para la operación. (Anexo P06.8) | Documentación detallada sobre el proceso de creación de copias de seguridad, las políticas de retención, los métodos de restauración de datos y los procedimientos de emergencia |
| Establecer la frecuencia con la que se realizarán las copias de seguridad automáticas (diarias, semanales, mensuales) y los horarios más adecuados para ejecutar estos respaldos (por ejemplo, fuera del horario laboral para minimizar el impacto en el rendimiento). (Anexo P06.9) |
| Configurar herramientas o software especializado en copias de seguridad automáticas (como soluciones de backup en la nube, software de backup local, o soluciones híbridas) para realizar los respaldos de manera regular en el software de la empresa. (Anexo P06.10) |
| Crear y mantener documentación detallada sobre el proceso de creación de copias de seguridad, las políticas de retención, los métodos de restauración de datos y los procedimientos de emergencia en caso de pérdida de información. (Anexo P06.11) |

#### Política de Protección para la Configuración del Switch de Red 2

* **Objetivo:** Garantizar la protección de la configuración del Switch de Red 2 (INF 17.1) frente a ataques deliberados de origen humano que puedan comprometer la seguridad, la disponibilidad y la integridad de la infraestructura tecnológica de Farmacorp. Esta política busca establecer un conjunto de medidas y controles para prevenir manipulaciones no autorizadas del equipo, resguardando la continuidad operativa y la confianza de los clientes y socios estratégicos en los servicios que ofrece la empresa.
* **Procedimientos:**

Tabla 16. Procedimientos para Política de Protección para la Configuración del Switch de Red 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Responsable | Actividad | Sub actividad | Registros |
|  | Jefe de Seguridad de la Información | Realizar una evaluación inicial en el Switch de Red 2 | Realizar un inventario detallado del equipo, incluyendo su ubicación física, configuración actual y su software instalado. (Anexo P07.1) | Informe de evaluación inicial  Inventario del equipo y su configuración actual. |
| Revisar las configuraciones actuales y los métodos de autenticación utilizados |
| Evaluar el estado de los controles de acceso físico al área donde se encuentra el switch. |
| Inspeccionar la configuración lógica del switch, revisando políticas de acceso, roles asignados y posibles vulnerabilidades conocidas. |
| Elaborar un informe de evaluación inicial que contenga recomendaciones específicas para fortalecer las áreas identificadas como vulnerables. |
|  | Jefe de Seguridad Física y Administrativa | Proteger físicamente el área donde se encuentra instalado el Switch de Red 2, reduciendo los riesgos de acceso no autorizado o manipulación de equipos. | Implementar cerraduras con autenticación biométrica en puertas de acceso a las salas de servidores donde se encuentra el Switch de Red 2. (Anexo P07.2) | Informes periódicos de inspecciones físicas y lista de ingreso al área técnica. |
| Instalar cámaras de videovigilancia con monitoreo continuo y capacidad de almacenamiento amplio. |
| Establecer procedimientos de ingreso controlado mediante tarjetas de identificación electrónicas únicas y personalizadas. |
| Limitar el acceso al área técnica exclusivamente al personal autorizado, registrando cada entrada y salida en una lista física y digital. |
| Realizar rondas de inspección diarias por parte del equipo de seguridad física para verificar el estado del área y reportar anomalías de inmediato. |
|  | Administrador de Red | Configurar y mantener medidas de protección lógica que minimicen los riesgos de accesos no autorizados y manipulaciones de la configuración del Switch de Red 2. | Configurar autenticación de dos factores (2FA) para accesos remotos al switch, asegurando que solo usuarios autorizados puedan operar el dispositivo. (Anexo P07.3) | Informes de respaldos automáticos cifrados.  Reportes de evaluación de privilegios de usuarios.  Logs de auditoría del switch. |
| Definir roles de acceso específicos y limitar los permisos al mínimo necesario según las funciones asignadas al personal autorizado. |
| Establecer contraseñas robustas para las cuentas administrativas, que incluyan al menos 12 caracteres, combinando letras, números y símbolos, con un cambio obligatorio cada 90 días. |
| Configurar reglas para bloquear conexiones desde IP no autorizadas y limitar el tráfico administrativo solo a las redes internas de la empresa. |
| Implementar un sistema de respaldos regulares y encriptados de la configuración del switch, almacenados en una ubicación segura, fuera del alcance de modificaciones directas. |
| Habilitar logs de actividad que registren en detalle todas las modificaciones realizadas en el switch, incluyendo quién las realizó, la fecha y la hora exacta. |
|  | Equipo de Respuesta a Incidentes | Detectar, analizar y mitigar intentos de manipulación en tiempo real, asegurando una respuesta inmediata y la restauración segura de la configuración del switch. | Configurar un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) que permita supervisar en tiempo real los eventos registrados en el switch. (Anexo P07.4) | Generar informes detallados que incluyan incidentes documentados.  Logs analizados durante la investigación.  Planes de acción y recuperación implementados. |
| Establecer alertas automáticas para eventos críticos como intentos de acceso no autorizado, cambios anómalos en la configuración o fallos de hardware. |
| Analizar los logs y demás registros del sistema para identificar el origen y alcance del intento de manipulación, documentando las evidencias obtenidas. |
|  | Responsable de Capacitación de TI | Implementar un programa de capacitación continua para todo el personal involucrado en la operación, configuración y mantenimiento de switches de red, con el objetivo de asegurar que sigan las mejores prácticas de seguridad. | Crear y mantener un plan de formación que cubra aspectos fundamentales de seguridad de la red, incluidos los protocolos de acceso, autenticación, configuración segura de switches y manejo de incidentes. | Informe de las sesiones de capacitación realizadas, incluyendo fechas, asistentes y temas cubiertos.  Plan de capacitación anual con actividades de actualización de seguridad. |
| Incluir temas como las políticas de contraseñas, el control de accesos físicos y lógicos, y las técnicas de protección contra manipulación de equipos. |
| Realizar sesiones de inducción para nuevos empleados que tengan acceso a los switches de red, explicando los riesgos de manipulación y cómo evitar violaciones de seguridad. |
| Organizar capacitaciones periódicas, como mínimo cada seis meses, para todo el personal encargado de la administración de redes, en las cuales se actualicen los conocimientos en nuevas amenazas y mejores prácticas de seguridad. |
|  | Auditoría Interna y Jefe de Seguridad de la Información (CISO) | Ejecutar auditorías internas anuales para evaluar si se están cumpliendo correctamente los procedimientos establecidos en esta política, asegurando que las configuraciones del Switch de Red 2 se gestionen de manera segura. | Definir el alcance de la auditoría, que incluirá la revisión de configuraciones de los switches, medidas de seguridad, controles de acceso físico y lógico, y gestión de incidentes. | Informe detallado con los hallazgos de la auditoría, incluyendo deficiencias y recomendaciones de mejora. |
| Verificar que los controles de acceso físico y lógico estén implementados correctamente y que solo personal autorizado tenga acceso. |
|  |  |  | Evaluar que las configuraciones de red cumplan con las políticas de seguridad y que se realicen respaldos regulares y cifrados. |

### Anexos de Políticas de Seguridad

1. Procedimiento de evaluación de la capacidad de almacenamiento, el procesamiento actual y el estado físico y funcional del hardware

|  |
| --- |
| PROCEDIMIENTO DE EVALUACIÓN DE LA CAPACIDAD DE ALMACENAMIENTO, EL PROCESAMIENTO ACTUAL Y EL ESTADO FÍSICO Y FUNCIONAL DEL HARDWARE |
| Actividad: Evaluar la capacidad de almacenamiento, el procesamiento actual y el estado físico y funcional del hardware.  Objetivo: Evaluar la capacidad del sistema de respaldo y el estado del hardware para garantizar que se encuentra operativo y con capacidad suficiente para soportar las necesidades actuales y futuras. |
| Procedimiento a emplear |
| 1. Revisar la cantidad de almacenamiento disponible y utilizado en los discos duros, SSD o sistemas de almacenamiento conectado a la red (NAS/SAN). 2. Comparar la capacidad de almacenamiento con las proyecciones de uso futuro para determinar si es necesario ampliar. 3. Verificar el rendimiento de los procesadores en los servidores o sistemas que soportan el sistema de respaldo. 4. Realizar pruebas de carga para verificar si el sistema puede manejar el volumen actual de datos sin afectar el rendimiento. 5. Inspeccionar visualmente el estado de los componentes físicos, como cables, puertos y unidades de almacenamiento, para detectar posibles daños. 6. Ejecutar diagnósticos de hardware para comprobar que todos los componentes están funcionando correctamente (discos, procesadores, memoria RAM). 7. Generar un informe detallado que documente la capacidad de almacenamiento, el procesamiento, el estado físico y funcional del hardware, con recomendaciones de acción si es necesario. |

1. Procedimiento de identificar necesidades de actualización o reemplazo de componentes

|  |
| --- |
| PROCEDIMIENTO DE IDENTIFICAR NECESIDADES DE ACTUALIZACIÓN O REEMPLAZO DE COMPONENTES |
| Actividad: Identificar necesidades de actualización o reemplazo de componentes  Objetivo: Identificar los componentes del sistema de respaldo que requieren actualización o reemplazo para asegurar su rendimiento y fiabilidad a largo plazo. |
| Procedimiento a emplear |
| 1. Identificar componentes que están mostrando signos de lentitud, fallos frecuentes o que no cumplen con los requisitos del sistema. 2. Comprobar las especificaciones y fechas de fabricación de los componentes (como discos duros, tarjetas madre, etc.) para detectar posibles necesidades de actualización. 3. Verificar con los proveedores las opciones disponibles para reemplazar o actualizar componentes específicos. 4. Documentar los componentes a actualizar o reemplazar, así como las justificaciones para estas decisiones. |

1. Procedimiento de documentar anomalías o signos de desgaste en el hardware.

|  |
| --- |
| PROCEDIMIENTO DE DOCUMENTAR ANOMALÍAS O SIGNOS DE DESGASTE EN EL HARDWARE. |
| Actividad: Documentar anomalías o signos de desgaste en el hardware  Objetivo: Identificar y documentar cualquier anomalía o signo de desgaste en el hardware para tomar acciones correctivas oportunas. |
| Procedimiento a emplear |
| Revisar indicadores como ruidos extraños, temperaturas altas, ralentización en el rendimiento, o errores de hardware en los registros.  Documentar cualquier anomalía o signo de desgaste en un sistema centralizado de tickets o en un informe de evaluación.  Registrar detalles de las anomalías detectadas, incluyendo fecha, tipo de fallo y recomendaciones para su resolución. |

1. Procedimiento de registrar los resultados y acciones correctivas de cada mantenimiento.

|  |
| --- |
| PROCEDIMIENTO DE REGISTRAR LOS RESULTADOS Y ACCIONES CORRECTIVAS DE CADA MANTENIMIENTO. |
| Actividad: Registrar los resultados y acciones correctivas de cada mantenimiento  Objetivo: Asegurar que se registren adecuadamente los resultados y acciones correctivas tomadas durante las actividades de mantenimiento del sistema de respaldo. |
| Procedimiento a emplear |
| 1. Anotar todos los resultados del mantenimiento realizado, incluyendo el estado del hardware antes y después de la intervención. 2. Si se detecta algún problema durante el mantenimiento, implementar las acciones correctivas adecuadas (reemplazo de piezas, actualizaciones de software, ajustes de configuración, etc.). 3. Incluir detalles como fecha de la intervención, tipo de mantenimiento realizado, piezas reemplazadas o reparadas y cualquier ajuste en la configuración. 4. Generar un informe detallado de cada actividad de mantenimiento, que incluya los problemas encontrados y las soluciones implementadas. |

1. Procedimiento de manejar el método RAID para la redundancia en el hardware

|  |
| --- |
| PROCEDIMIENTO DE MANEJAR EL MÉTODO RAID PARA LA REDUNDANCIA EN EL HARDWARE |
| Actividad: Manejar el método RAID para la redundancia en el hardware  Objetivo: Implementar y gestionar la configuración RAID en el hardware de respaldo para garantizar redundancia y protección de los datos. |
| Procedimiento a emplear |
| 1. Evaluar y seleccionar el nivel de RAID (RAID 1, RAID 5, RAID 10, etc.) que ofrezca el balance adecuado entre redundancia y rendimiento. 2. Implementar la configuración RAID seleccionada, asegurando que todos los discos y componentes estén correctamente configurados. 3. Ejecutar pruebas de redundancia para verificar que el sistema pueda recuperar datos en caso de falla de un disco. 4. Documentar el nivel de RAID implementado, las configuraciones específicas y los resultados de las pruebas de redundancia. |

1. Procedimiento de documentar la configuración y el proceso de implementación de la redundancia

|  |
| --- |
| PROCEDIMIENTO DE DOCUMENTAR LA CONFIGURACIÓN Y EL PROCESO DE IMPLEMENTACIÓN DE LA REDUNDANCIA |
| Actividad: Documentar la configuración y el proceso de implementación de la redundancia  Objetivo: Asegurar que la configuración y el proceso de implementación de la redundancia estén bien documentados para facilitar el mantenimiento y las futuras actualizaciones. |
| Procedimiento a emplear |
| 1. Describir el proceso y la configuración de la redundancia, incluidos los detalles sobre los discos, configuraciones RAID, y otros elementos de redundancia. 2. Especificar cómo se deben recuperar los datos en caso de una falla del sistema o disco. 3. Mantener una documentación clara y accesible sobre la configuración y los procesos de redundancia implementados. |

1. Procedimiento de planificar y ejecutar simulaciones periódicas de fallas en componentes clave del sistema de respaldo

|  |
| --- |
| PROCEDIMIENTO DE PLANIFICAR Y EJECUTAR SIMULACIONES PERIÓDICAS DE FALLAS EN COMPONENTES CLAVE DEL SISTEMA DE RESPALDO |
| Actividad: Planificar y ejecutar simulaciones periódicas de fallas en componentes clave del sistema de respaldo  Objetivo: Validar la efectividad de las soluciones de redundancia mediante simulaciones de fallos en los componentes clave. |
| Procedimiento a emplear |
| 1. Establecer un calendario para ejecutar simulaciones periódicas de fallas en componentes clave del sistema, como discos duros o fuentes de alimentación. 2. Realizar las simulaciones de fallas siguiendo un guion preestablecido para garantizar que todos los escenarios posibles sean cubiertos. 3. Documentar los resultados de cada simulación, incluyendo tiempos de respuesta, recuperación y problemas encontrados. |

1. Procedimiento de registrar tiempo de respuesta y los resultados de cada simulación

|  |
| --- |
| PROCEDIMIENTO DE REGISTRAR TIEMPO DE RESPUESTA Y LOS RESULTADOS DE CADA SIMULACIÓN |
| Actividad: Registrar tiempo de respuesta y los resultados de cada simulación  Objetivo: Medir la eficiencia de los procedimientos de recuperación ante fallos y tomar acciones correctivas si es necesario. |
| Procedimiento a emplear |
| 1. Medir y registrar el tiempo que tarda el sistema en recuperarse de cada simulación de fallo. 2. Incluir los resultados de la simulación, destacando cualquier área donde los tiempos de respuesta puedan mejorar. 3. Mantener un registro de los tiempos de respuesta de cada simulación y las acciones correctivas necesarias. |

1. Procedimiento de realizar el procedimiento de monitoreo en tiempo real para supervisar el estado del hardware con Zabbix

|  |
| --- |
| PROCEDIMIENTO DE REALIZAR EL PROCEDIMIENTO DE MONITOREO EN TIEMPO REAL PARA SUPERVISAR EL ESTADO DEL HARDWARE CON ZABBIX |
| Actividad: Realizar el procedimiento de monitoreo en tiempo real para supervisar el estado del hardware con Zabbix  Objetivo: Implementar monitoreo en tiempo real para detectar fallas o irregularidades en el hardware antes de que afecten el rendimiento del sistema. |
| Procedimiento a emplear |
| 1. Configurar Zabbix para monitorear el estado de los componentes del hardware, como la temperatura, la carga de CPU, y el uso de disco. 2. Establecer alertas para detectar cualquier anomalía en el rendimiento o el estado del hardware. 3. Registrar los eventos o alertas detectadas durante el monitoreo. |

1. Procedimiento de documentar y notificar cualquier anomalía detectada al área de soporte técnico para su resolución

|  |
| --- |
| PROCEDIMIENTO DE DOCUMENTAR Y NOTIFICAR CUALQUIER ANOMALÍA DETECTADA AL ÁREA DE SOPORTE TÉCNICO PARA SU RESOLUCIÓN |
| Actividad: Documentar y notificar cualquier anomalía detectada al área de soporte técnico para su resolución  Objetivo: Asegurar que cualquier anomalía detectada sea documentada y notificada de inmediato para su resolución. |
| Procedimiento a emplear |
| 1. Registrar cualquier anomalía detectada en el sistema de monitoreo. 2. Notificar inmediatamente al área de soporte técnico para que tomen las medidas correctivas necesarias. 3. Mantener un registro de todas las anomalías detectadas y las acciones correctivas tomadas. |

* 1. Procedimiento de Control de Acceso Físico a Zonas Restringidas

|  |
| --- |
| PROCEDIMIENTO DE MONITOREO DE ÁREAS RESTRINGIDAS |
| ACTIVIDAD: Monitorear continuamente el acceso físico 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 física 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 físicamente 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.). 16. Registrar cualquier anomalía observada en el sistema de incidentes con una captura de video como evidencia. 17. Registro de Eventos: 18. Documentar eventos normales y excepcionales, detallando hora, ubicación, descripción y el operador a cargo. 19. Reportar actividades sospechosas inmediatamente al supervisor del SGSI. 20. Verificación Semanal de Grabaciones: 21. Revisar grabaciones almacenadas de forma aleatoria para asegurar la continuidad del registro. 22. Validar que no haya interrupciones en los registros y que las fechas y horas sean precisas. 23. Emisión de Informes Periódicos: 24. Generar reportes semanales sobre las actividades de monitoreo, destacando incidentes relevantes y su resolución. 25. Enviar el informe al responsable de seguridad física y al gestor del SGSI para su análisis y acción. 26. Respaldo y Eliminación de Grabaciones: 27. Resguardar las grabaciones de las últimas cuatro semanas en un servidor seguro. 28. Eliminar automáticamente grabaciones más antiguas de acuerdo con la política de retención de datos, previa autorización del supervisor. 29. Revisión y Actualización del Procedimiento: 30. Cada tres meses, evaluar la efectividad del monitoreo y realizar mejoras en el procedimiento si es necesario. 31. Documentar los cambios implementados y capacitar al personal nuevamente. |

* 1. Procedimiento de Reconfiguración de Medidas de Control de Acceso

|  |
| --- |
| PROCEDIMIENTO DE RECONFIGURACIÓN DE MEDIDAS DE CONTROL DE ACCESO |
| ACTIVIDAD: Ajustar y actualizar las medidas de control de acceso físico en las zonas restringidas de FarmaCorp.  OBJETIVO: Asegurar que las medidas de control de acceso sean efectivas y estén alineadas con las necesidades operativas y de seguridad de la organización. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Análisis Preliminar de Necesidades de Reconfiguración: 2. Revisar las políticas de acceso existentes y detectar áreas que requieran ajustes. 3. Identificar nuevas amenazas o cambios en los requisitos de seguridad (e.g., entrada de nuevo personal, modificación de roles). 4. Consultar con los responsables de las áreas restringidas para confirmar necesidades específicas. 5. Validación de Cambios Solicitados: 6. Confirmar la lista de accesos requeridos para cada usuario o grupo de usuarios. 7. Validar los cambios con el departamento de seguridad física y el responsable del SGSI. 8. Aprobar las solicitudes mediante un formulario oficial que documente los cambios requeridos. 9. Evaluación Técnica del Sistema Actual: 10. Revisar la funcionalidad del sistema de control de acceso físico (lectores de tarjetas, cerraduras electrónicas, sistemas biométricos). 11. Identificar componentes que requieran actualización o reconfiguración. 12. Asegurarse de que el sistema permita aplicar los cambios sin interrumpir las operaciones. 13. Planificación de la Reconfiguración: 14. Definir el cronograma de actualización, priorizando horarios de menor impacto operativo. 15. Notificar al personal afectado sobre posibles interrupciones temporales. 16. Preparar un plan de respaldo, como acceso manual en caso de fallo del sistema. 17. Ejecución de la Reconfiguración: 18. Actualizar las bases de datos del sistema de control con los nuevos permisos y restricciones. 19. Configurar y probar los dispositivos de control (lectores de tarjetas, sensores, cámaras, etc.) en las áreas involucradas. 20. Registrar las modificaciones realizadas en un informe detallado. 21. Pruebas de Validación: 22. Realizar pruebas con usuarios autorizados para asegurar que los cambios funcionan correctamente. 23. Confirmar que los accesos no autorizados sean bloqueados. 24. Documentar resultados de las pruebas y corregir fallos detectados. 25. Capacitación al Personal Afectado: 26. Informar a los usuarios sobre los nuevos procedimientos de acceso y uso de credenciales. 27. Capacitar al personal de seguridad en la operación de las nuevas configuraciones. 28. Registro y Documentación Final: 29. Actualizar los registros del SGSI con los cambios realizados, incluyendo detalles técnicos y aprobaciones correspondientes. 30. Generar un informe final con la evaluación de la reconfiguración y enviarlo al responsable del SGSI. 31. Monitoreo Continuo: 32. Supervisar el desempeño de las nuevas configuraciones durante un período inicial (por ejemplo, 2 semanas). 33. Registrar incidentes o ajustes necesarios y realizar correcciones en caso de detectar vulnerabilidades. 34. Revisión y Mejoras: 35. Programar revisiones periódicas (e.g., cada 6 meses) para mantener las configuraciones actualizadas y alineadas con los objetivos del SGSI. |

* 1. Procedimiento de Auditorías de Control de Acceso

|  |
| --- |
| PROCEDIMIENTO DE AUDITORÍAS DE CONTROL DE ACCESO |
| ACTIVIDAD: Realizar auditorías periódicas de los sistemas de control de acceso físico.  OBJETIVO: Identificar vulnerabilidades en las medidas implementadas y garantizar el cumplimiento de las políticas de acceso físico en FarmaCorp. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Planificación de la Auditoría: 2. Establecer los objetivos específicos de la auditoría (e.g., detección de accesos no autorizados, evaluación de registros, inspección de dispositivos). 3. Definir el alcance de la auditoría (e.g., áreas restringidas específicas, turnos de vigilancia, equipos de monitoreo). 4. Seleccionar un equipo de auditores calificados, garantizando la independencia del proceso. 5. Revisión de Documentación: 6. Recopilar y analizar registros previos de acceso físico (logs, reportes de incidentes, configuraciones actuales de acceso). 7. Revisar las políticas y procedimientos actuales de control de acceso para identificar criterios de evaluación. 8. Confirmar los permisos autorizados para usuarios activos. 9. Inspección Física de Dispositivos de Control de Acceso: 10. Verificar el estado operativo de los equipos (lectores de tarjetas, cámaras, cerraduras electrónicas). 11. Revisar el mantenimiento preventivo y correctivo registrado en el historial de equipos. 12. Confirmar la existencia de señalización adecuada en las áreas restringidas. 13. Validación de Permisos y Accesos: 14. Comparar los permisos registrados en el sistema de control con las listas de personal autorizado. 15. Identificar accesos no autorizados o inconsistencias en los registros. 16. Realizar pruebas de acceso para validar la configuración del sistema. 17. Entrevistas y Observaciones Directas: 18. Entrevistar a operadores de seguridad para evaluar su conocimiento y cumplimiento de los procedimientos. 19. Observar en tiempo real cómo se ejecutan los controles de acceso en las áreas restringidas. 20. Identificar posibles desviaciones de los procedimientos documentados. 21. Registro de Hallazgos: 22. Documentar de manera detallada las observaciones, clasificando los hallazgos por nivel de criticidad (baja, media, alta). 23. Registrar ejemplos específicos de vulnerabilidades detectadas (e.g., accesos fuera de horario sin justificación). 24. Adjuntar evidencia como fotos, capturas de pantalla de registros o resultados de pruebas realizadas. 25. Análisis y Evaluación de Resultados: 26. Comparar los hallazgos con las políticas del SGSI y las normativas aplicables para identificar incumplimientos. 27. Evaluar la efectividad del sistema de control de acceso actual y los procedimientos asociados. 28. Elaboración del Informe de Auditoría: 29. Preparar un informe detallado que incluya: 30. Objetivos de la auditoría. 31. Metodología utilizada. 32. Hallazgos clasificados por nivel de criticidad. 33. Recomendaciones específicas para mitigar riesgos identificados. 34. Enviar el informe a los responsables del SGSI y al departamento de seguridad física. 35. Implementación de Acciones Correctivas: 36. Diseñar un plan de acción para abordar las vulnerabilidades detectadas. 37. Priorizar las acciones correctivas según el nivel de criticidad de los hallazgos. 38. Monitorear la implementación de las correcciones y documentar su progreso. 39. Revisión Posterior: 40. Programar una auditoría de seguimiento para confirmar la implementación y efectividad de las acciones correctivas. 41. Evaluar mejoras en el desempeño del sistema de control de acceso desde la última auditoría. |

* 1. Procedimiento de Vigilancia y Monitoreo en Áreas Críticas

|  |
| --- |
| PROCEDIMIENTO DE MONITOREO ACTIVO DE ÁREAS CRÍTICAS |
| ACTIVIDAD: Supervisar en tiempo real las áreas críticas de FarmaCorp mediante sistemas de video vigilancia.  OBJETIVO: Detectar y responder a incidentes en tiempo real, minimizando riesgos de accesos no autorizados y amenazas de seguridad. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Identificación de Áreas Críticas: 2. Revisar las áreas designadas como críticas en el mapa de instalaciones. 3. Verificar la sensibilidad de los activos dentro de estas áreas (e.g., servidores, laboratorios). 4. Preparación del Equipo de Monitoreo: 5. Configurar cámaras y sensores de vigilancia en puntos estratégicos. 6. Confirmar que el software de monitoreo esté actualizado y operativo. 7. Realizar una prueba de los sistemas para garantizar grabaciones y alertas en tiempo real. 8. Supervisión en Tiempo Real: 9. Asignar personal capacitado para el monitoreo continuo de las transmisiones. 10. Configurar alertas automáticas en caso de detectar movimientos sospechosos o accesos no autorizados. 11. Registrar cualquier evento observado, incluso si no parece crítico, para análisis posterior. 12. Respuesta a Incidentes: 13. Notificar de inmediato al supervisor en caso de detectar actividades no autorizadas. 14. Activar el protocolo de respuesta a incidentes definido por el SGSI. 15. Documentar todos los detalles del incidente (hora, lugar, descripción, acciones tomadas). 16. Análisis y Reportes: 17. Generar un informe diario con los eventos registrados. 18. Destacar incidentes relevantes y su resolución. 19. Compartir el informe con los responsables de seguridad. |

* 1. Procedimiento de Mantenimiento Correctivo de Equipos de Monitoreo

|  |
| --- |
| PROCEDIMIENTO DE MANTENIMIENTO CORRECTIVO DE EQUIPOS DE MONITOREO |
| ACTIVIDAD: Realizar revisiones periódicas y reparaciones en los equipos de vigilancia para garantizar su correcto funcionamiento.  OBJETIVO: Asegurar la operatividad continua de los sistemas de video vigilancia y minimizar el riesgo de fallos en la seguridad de las áreas críticas. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Detección de Fallas: 2. Revisar los reportes de monitoreo para identificar interrupciones en las transmisiones o alertas. 3. Realizar inspecciones periódicas para identificar señales de desgaste en los equipos. 4. Notificación y Registro de Fallas: 5. Reportar fallas detectadas al departamento técnico utilizando un formulario estandarizado. 6. Registrar las fallas en el sistema de gestión de mantenimiento, indicando ubicación y descripción. 7. Evaluación Técnica Inicial: 8. Realizar un diagnóstico preliminar del equipo afectado para determinar la naturaleza del problema (hardware o software). 9. Decidir si la reparación puede realizarse internamente o si requiere el soporte de un proveedor externo. 10. Reparación y Pruebas: 11. Reparar el equipo según las instrucciones del fabricante o manual técnico. 12. Realizar pruebas operativas para asegurar que el problema esté resuelto. 13. Documentar las acciones realizadas y los resultados de las pruebas. 14. Reintegración al Sistema: 15. Reconectar el equipo al sistema de monitoreo. 16. Confirmar que la funcionalidad del sistema sea restaurada en su totalidad. 17. Informe de Mantenimiento: 18. Generar un reporte final detallando la causa de la falla, las acciones tomadas y los costos involucrados (si aplicable). 19. Compartir el informe con los responsables del área crítica y el gestor del SGSI. 20. Revisión Periódica de Equipos: 21. Programar mantenimientos preventivos futuros para minimizar riesgos de fallos similares. |

* 1. Procedimiento de Gestión de Identificación y Credenciales Físicas

|  |
| --- |
| PROCEDIMIENTO DE EMISIÓN Y CONTROL DE CREDENCIALES |
| ACTIVIDAD: Supervisar la emisión y gestión de credenciales para los empleados y visitantes de FarmaCorp.  OBJETIVO: Garantizar que las credenciales de acceso se emitan de manera controlada y segura, y que sean utilizadas únicamente por personal autorizado. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Identificación de Requisitos de Credenciales: 2. Consultar con los departamentos correspondientes sobre los requisitos de acceso para nuevos empleados, contratistas o visitantes. 3. Verificar la categoría del usuario (e.g., empleado regular, personal temporal) para determinar el tipo de credencial necesaria. 4. Verificación de Autorización: 5. Confirmar que la persona que solicita la credencial esté registrada en el sistema de recursos humanos. 6. Validar las autorizaciones de acceso proporcionadas por el supervisor del área correspondiente. 7. Generación de Credenciales: 8. Utilizar el sistema de gestión de credenciales para crear las credenciales físicas, asegurando que la información (nombre, rol, foto, permisos) esté correctamente registrada. 9. Personalizar las credenciales según el nivel de acceso (e.g., color, código de barras, chip RFID). 10. Entrega y Activación de Credenciales: 11. Proporcionar las credenciales a la persona autorizada, asegurándose de que comprenda las reglas de uso y los procedimientos para acceder a las áreas restringidas. 12. Activar la credencial en el sistema, vinculándola a los permisos específicos del usuario. 13. Documentación y Registro: 14. Registrar la emisión de cada credencial en el sistema de gestión de credenciales, incluyendo la fecha de emisión y el nombre del responsable. 15. Mantener un inventario actualizado de todas las credenciales emitidas. 16. Revisión de Credenciales No Utilizadas: 17. Realizar revisiones periódicas de las credenciales emitidas para detectar las que no han sido activadas o no se utilizan. 18. Inactivar credenciales no necesarias y actualizar el registro de acceso. |

* 1. Procedimiento de Revocación y Actualización de Credenciales Activas

|  |
| --- |
| PROCEDIMIENTO DE ACTUALIZACIÓN Y REVOCACIÓN DE CREDENCIALES |
| ACTIVIDAD: Modificar, desactivar o revocar credenciales de acceso de acuerdo con los cambios de roles o la desvinculación de empleados en FarmaCorp.  OBJETIVO: Prevenir el uso indebido de credenciales y garantizar que solo el personal autorizado tenga acceso. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Identificación de Credenciales a Revocar o Actualizar: 2. Consultar el sistema para identificar las credenciales que deben ser revocadas o actualizadas (e.g., cambios de rol, salida de personal, fallos en el sistema de acceso). 3. Validar con el departamento de recursos humanos o supervisor correspondiente los cambios que requieran modificación en las credenciales. 4. Revocación de Credenciales: 5. Acceder al sistema de gestión de credenciales y desactivar la credencial del usuario cuya autorización haya expirado o ya no sea válida. 6. Asegurarse de que el acceso al sistema y las áreas restringidas sea bloqueado inmediatamente para evitar brechas de seguridad. 7. Actualización de Credenciales: 8. Actualizar la base de datos de credenciales con nuevos permisos para aquellos usuarios que han cambiado de rol o responsabilidades. 9. Reprogramar las credenciales con los nuevos niveles de acceso, asegurándose de que los permisos sean coherentes con la nueva autorización. 10. Destrucción Física de Credenciales Revocadas: 11. Recoger las credenciales revocadas de los usuarios y destruirlas de forma segura (e.g., corte de tarjeta, destrucción de chips RFID). 12. Registrar la destrucción de las credenciales en el sistema, incluyendo fecha, método de destrucción y responsable. 13. Notificación al Usuario: 14. Informar a los usuarios afectados sobre la revocación o actualización de sus credenciales, indicando las razones del cambio y proporcionándoles la nueva credencial si corresponde. 15. Capacitar a los usuarios en los nuevos procedimientos de acceso si es necesario. 16. Documentación y Registro: 17. Mantener un registro detallado de las revocaciones y actualizaciones realizadas, incluyendo la fecha, el motivo y las acciones tomadas. 18. Generar informes periódicos de revocaciones y actualizaciones para su revisión por parte del SGSI. |

* 1. Procedimiento de Verificación de Identidad en el Acceso

|  |
| --- |
| PROCEDIMIENTO DE VERIFICACIÓN DE IDENTIDAD EN EL ACCESO |
| ACTIVIDAD: Confirmar la identidad del personal que accede a zonas restringidas mediante credenciales y sistemas complementarios como biometría o contraseñas.  OBJETIVO: Garantizar que las personas que ingresan a áreas críticas sean quienes afirman ser y cuenten con los permisos necesarios. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Establecimiento de Puntos de Control: 2. Identificar los puntos críticos de acceso donde se realizará la verificación de identidad (entradas a zonas restringidas, áreas de alto riesgo). 3. Asegurar que cada punto de control esté equipado con el sistema adecuado para verificar las credenciales (lectores de tarjetas, biometría). 4. Verificación de Credenciales: 5. Al momento de un acceso, el usuario debe presentar su credencial (tarjeta de acceso, huella dactilar, etc.). 6. El sistema debe verificar automáticamente si la credencial es válida, comparando la información registrada (nombre, permisos de acceso). 7. Verificación Manual Adicional (si es necesario): 8. Si el sistema no puede validar automáticamente la credencial, realizar una verificación manual comparando la foto en la credencial con el usuario o consultando el registro de acceso. 9. Confirmar con el responsable de seguridad si la situación persiste, procediendo con los protocolos establecidos. 10. Acceso Aprobado o Denegado: 11. Si la verificación es positiva, el sistema permitirá el acceso, registrando la hora y el punto de acceso. 12. Si la verificación es negativa, se denegará el acceso y se generará una alerta para que el personal de seguridad actúe según los procedimientos de seguridad establecidos. 13. Registro de Verificación de Acceso: 14. Registrar todos los intentos de acceso, tanto exitosos como fallidos, en el sistema de gestión de accesos. 15. Los registros deben incluir el nombre del usuario, hora, tipo de acceso y el resultado de la verificación. 16. Notificación de Incidentes de Acceso: 17. Si se detecta un acceso no autorizado, el sistema debe generar una alerta inmediata al personal de seguridad para que tome las acciones correspondientes. 18. Reportar el incidente en el informe de seguridad y tomar medidas correctivas según las políticas del SGSI. |

* + 1. Procedimiento de reconfiguración de políticas de contraseñas

|  |
| --- |
| Procedimiento de reconfiguración de políticas de contraseñas |
| ACTIVIDAD: Ajustar las políticas de contraseñas en el sistema para fortalecer los controles de acceso, cumpliendo con los estándares de seguridad organizacionales y normativos.  OBJETIVO: Garantizar que las contraseñas usadas por los usuarios sean seguras y cumplan con los requisitos mínimos de longitud, complejidad y periodicidad de cambio. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar los estándares de seguridad actuales: 2. Consultar los lineamientos internos y externos aplicables (por ejemplo, ISO 27001 o NIST). 3. Comparar las configuraciones actuales con las recomendaciones de mejores prácticas. 4. Actualizar las configuraciones en el sistema de gestión de autenticación: 5. Modificar los requisitos de longitud y complejidad (caracteres alfanuméricos y especiales). 6. Configurar la caducidad de contraseñas. 7. Probar las nuevas configuraciones: 8. Realizar pruebas en cuentas de prueba para validar la funcionalidad de las políticas ajustadas. 9. Verificar que los cambios no generen problemas de compatibilidad con sistemas vinculados. 10. Informar a los usuarios sobre los cambios: 11. Comunicar las nuevas políticas y sus fechas de implementación. 12. Proporcionar instrucciones claras sobre cómo actualizar las contraseñas. 13. Monitorear el cumplimiento de la nueva política: 14. Supervisar los registros de cambios de contraseñas para detectar posibles errores o incumplimientos. 15. Generar un informe de cumplimiento inicial. |

* + 1. Procedimiento para monitorear intentos de acceso

|  |
| --- |
| Procedimiento para monitorear intentos de acceso |
| ACTIVIDAD: Supervisar constantemente los intentos de acceso a los sistemas y recursos de la organización para identificar y mitigar amenazas potenciales en tiempo real.  OBJETIVO: Detectar intentos de acceso no autorizado o comportamientos anómalos que puedan comprometer la seguridad del sistema.. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Configurar herramientas de monitoreo de accesos: 2. Verificar que las herramientas de monitoreo estén funcionando y actualizadas. 3. Configurar alertas para accesos fallidos reiterados o accesos desde ubicaciones sospechosas 4. Recopilar registros de intentos de acceso: 5. Consolidar logs de acceso desde sistemas y dispositivos críticos. 6. Asegurar la integridad de los registros recopilados. 7. Analizar los patrones de acceso: 8. Identificar comportamientos anómalos como intentos fallidos consecutivos. 9. Evaluar el origen geográfico y horario de los accesos detectados. 10. Responder a incidentes detectados: 11. Bloquear cuentas afectadas en caso de intentos sospechosos. 12. Notificar al área de seguridad para realizar análisis forenses. 13. Generar reportes periódicos: 14. Elaborar informes mensuales sobre incidentes y actividades de acceso. 15. Incluir un análisis de tendencias y recomendaciones para mejorar la seguridad. 16. Ajustar las configuraciones de monitoreo según las tendencias: 17. Reconfigurar las alertas en función de patrones emergentes. 18. Actualizar políticas de acceso para mitigar nuevos riesgos detectados. |

* + 1. Procedimiento de Verificación de Identidad en el Acceso

|  |
| --- |
| Procedimiento de Verificación de Identidad en el Acceso |
| ACTIVIDAD: Revisar y ajustar los roles y permisos asignados a los usuarios para garantizar que cada uno acceda únicamente a los recursos necesarios para su función.  OBJETIVO: Reducir el riesgo de accesos no autorizados mediante la aplicación estricta del principio de privilegio mínimo. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar roles y permisos en base a perfiles de puesto: 2. Comparar los permisos asignados con las funciones asociadas a cada puesto. 3. Detectar roles que excedan los privilegios requeridos. 4. Ajustar permisos incorrectos: 5. Eliminar accesos no justificados para ciertos usuarios. 6. Corregir configuraciones erróneas detectadas en la revisión. 7. Validar con los responsables de las áreas: 8. Presentar ajustes a los responsables de los recursos para su validación. 9. Recibir retroalimentación y ajustar si es necesario. 10. Actualizar y documentar la matriz de roles y permisos: 11. Registrar los cambios realizados en el sistema y en los documentos oficiales. 12. Generar un reporte detallado de los ajustes. 13. Comunicar los ajustes a los usuarios afectados: 14. Informar a los usuarios sobre cambios en sus permisos y su justificación. 15. Resolver dudas o problemas derivados de los ajustes. |

* + - 1. Procedimiento de Documentación y Corrección de Errores en Pruebas de Recuperación de la Información

|  |
| --- |
| PROCEDIMIENTO DE DOCUMENTACIÓN Y CORRECCIÓN DE ERRORES EN PRUEBAS DE RECUPERACIÓN DE LA INFORMACIÓN |
| ACTIVIDAD: Documentar y corregir cualquier problema o error encontrado durante las pruebas de recuperación de la base de datos.  OBJETIVO: Garantizar que cualquier error o inconveniente en el proceso de recuperación de la información se documente y resuelva de manera eficaz. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Iniciar un registro de prueba en el Registro de Copias de Seguridad y Recuperación con la fecha, hora y el nombre del responsable de la prueba de recuperación. 2. Indicar el tipo de recuperación realizada (por ejemplo, total o parcial de la base de datos) y la herramienta o software utilizado. 3. Verificar que el entorno de prueba esté aislado del entorno de producción para evitar cualquier alteración en la información en uso activo. 4. Cargar los archivos de respaldo en el sistema de prueba, asegurándose de que el respaldo seleccionado sea el más reciente y corresponda al archivo o base de datos que se desea verificar. 5. Iniciar el proceso de recuperación a través de la herramienta o software designado, siguiendo los pasos específicos del sistema. 6. Documentar cada paso importante en la ejecución de la prueba, como el tiempo de inicio, cualquier mensaje o alerta mostrada por el sistema y el tiempo de finalización. 7. Monitorear y verificar la integridad de los datos recuperados y la correcta sincronización con el sistema de gestión de contratos. 8. Revisar detalladamente la recuperación de datos y registrar cualquier error encontrado, especificando el tipo de problema (por ejemplo, pérdida parcial de datos, corrupción de archivos, o errores de autenticación). 9. Documentar la ubicación de los errores (si es posible) y describir su impacto en el proceso de recuperación. 10. Evaluar la causa raíz del error y determinar si se debe a problemas en la copia de seguridad original, la herramienta de recuperación, o algún otro factor interno. 11. Aplicar las correcciones necesarias según el diagnóstico realizado (como ajustes en el software de respaldo, cambios en la configuración de la base de datos, o mejoras en los métodos de copiado). 12. Probar nuevamente la recuperación para confirmar que los problemas han sido resueltos. 13. Registrar las acciones correctivas implementadas y el resultado de la nueva prueba en el Registro de Copias de Seguridad y Recuperación. 14. Incluir recomendaciones para futuras pruebas, indicando posibles ajustes en la programación o metodología del sistema de respaldo si es necesario. 15. Revisar toda la documentación registrada para asegurar que se haya documentado cada paso de forma clara y completa. 16. Cerrar el registro de prueba, archivando los detalles en la base de datos de procedimientos para referencia en futuras pruebas de recuperación. |

* + - 1. Procedimiento de mantener actualizados los sistemas IDS

|  |
| --- |
| PROCEDIMIENTO DE MANTENER ACTUALIZADOS LOS SISTEMAS IDS |
| ACTIVIDAD: Mantener actualizados los sistemas IDS (Intrusion Detection Systems).  OBJETIVO: Asegurar que los sistemas IDS operen con eficacia máxima para identificar y alertar sobre actividades sospechosas o intentos de modificación no autorizados en el software. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar semanalmente el sitio web del proveedor del sistema IDS para identificar actualizaciones de software, firmas y parches de seguridad. 2. Consultar boletines de seguridad o foros técnicos relacionados con el IDS utilizado para estar informado sobre vulnerabilidades conocidas o actualizaciones críticas. 3. Descargar e instalar las actualizaciones proporcionadas por el proveedor del IDS. 4. Verificar en los registros del sistema IDS que las actualizaciones han sido aplicadas sin errores. 5. Confirmar que las nuevas firmas detectan correctamente las amenazas para las que fueron diseñadas, utilizando escenarios controlados. 6. Actividades relacionadas con garantizar el funcionamiento correcto del IDS: 7. Revisar mensualmente las configuraciones predeterminadas del IDS para garantizar que se ajusten al entorno operativo del software y las políticas de seguridad de la organización. 8. Ejecutar pruebas periódicas (al menos trimestralmente) para verificar que el sistema IDS detecta correctamente intentos de intrusión simulados, utilizando herramientas de evaluación de seguridad. 9. Registrar y analizar los resultados de las pruebas, ajustando las configuraciones si se detectan fallas o falsos positivos/negativos. 10. Registrar cada actualización y cambio de configuración realizado en un archivo de control, incluyendo la fecha, la versión instalada y la persona responsable. |

* + - 1. Procedimiento de respuesta rápida ante alteraciones malintencionadas

|  |
| --- |
| PROCEDIMIENTO DE RESPUESTA RÁPIDA ANTE ALTERACIONES MALINTENCIONADAS |
| ACTIVIDAD: Ejecutar protocolos de respuesta rápida en caso de confirmarse una alteración malintencionada.  OBJETIVO: Responder de manera eficaz y rápida ante alteraciones malintencionadas en los sistemas, minimizando el impacto en la organización y asegurando la protección de los datos. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar la alerta generada por el sistema IDS y verificar los detalles específicos del incidente, incluyendo la fecha, hora, origen y tipo de intento de modificación no autorizada. 2. Consultar el Informe de Alertas de Seguridad para corroborar antecedentes o incidentes similares que puedan relacionarse con el intento actual. 3. Notificar al Equipo de Respuesta a Incidentes y al Área de Seguridad de TI sobre la alteración confirmada. 4. Aislar de inmediato el sistema o dispositivo afectado para prevenir una propagación del incidente a otros sistemas o redes. 5. Desconectar o limitar los accesos del usuario o sistema que haya sido identificado como el posible origen de la alteración. 6. Iniciar el proceso de recopilación de datos relacionados con el incidente, incluyendo logs del sistema, información de la red, capturas de pantalla, y cualquier otra evidencia digital. 7. Registrar el contexto del incidente en el Informe de Alertas de Seguridad, detallando las acciones tomadas hasta el momento y cualquier anomalía observada. 8. Determinar el alcance de la alteración malintencionada y evaluar si hay datos críticos o sistemas sensibles comprometidos. 9. Asignar un nivel de prioridad a la respuesta según el impacto potencial y activar recursos adicionales si el incidente es considerado crítico. 10. Implementar medidas de mitigación como restaurar el sistema desde una copia de seguridad o realizar un análisis profundo para eliminar cualquier acceso no autorizado. 11. Asegurarse de que el sistema o dispositivo afectado cumpla con los requisitos de seguridad antes de reestablecer su conexión o su funcionamiento en la red principal. 12. Completar el Informe de Alertas de Seguridad con todos los detalles del incidente, las evidencias recopiladas, las acciones correctivas tomadas y el resultado de dichas acciones. 13. Notificar a las partes interesadas, incluyendo la dirección de la organización y cualquier autoridad externa requerida, si el incidente tiene repercusiones legales o regulatorias. 14. Realizar una reunión post-incidente con el Equipo de Respuesta a Incidentes para revisar el protocolo seguido y evaluar la efectividad de la respuesta. 15. Identificar áreas de mejora y actualizar los protocolos de respuesta rápida en función de las lecciones aprendidas para reducir el riesgo de incidentes similares en el futuro. |

* + - 1. Procedimiento para establecer roles y funciones de cada usuario

|  |
| --- |
| PROCEDIMIENTO PARA ESTABLECER ROLES Y FUNCIONES DE CADA USUARIO |
| ACTIVIDAD: Establecer y gestionar los roles y funciones de cada usuario de acuerdo a su nivel de acceso y responsabilidades en el sistema.  OBJETIVO: Definir y asignar roles y funciones de cada usuario, asegurando que cada uno tenga acceso únicamente a las funciones necesarias para sus actividades, de acuerdo con el principio de mínimo privilegio, y manteniendo la seguridad y el control de acceso en el sistema. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar la estructura organizativa y los requisitos específicos de cada área para identificar roles necesarios. 2. Consultar con los supervisores de cada área para validar las funciones y responsabilidades asociadas a cada rol de usuario. 3. Definir y documentar los nombres de roles específicos, como "Administrador", "Usuario General", "Supervisor" o "Auditor", junto con sus responsabilidades principales. 4. Documentar los roles en el Registro de Control de Roles y Funciones, detallando las áreas responsables y las descripciones de cada rol. 5. Informar a los supervisores y al personal correspondiente sobre los roles definidos, obteniendo su validación antes de proceder con la implementación en el sistema. 6. Capacitar a los usuarios sobre el significado y los límites de sus roles en el sistema. |

* + - 1. Procedimiento para asignar y configurar permisos específicos de acceso y modificación en el software de acuerdo a los roles

|  |
| --- |
| PROCEDIMIENTO PARA ASIGNAR Y CONFIGURAR PERMISOS ESPECÍFICOS DE ACCESO Y MODIFICACIÓN EN EL SOFTWARE DE ACUERDO A LOS ROLES |
| ACTIVIDAD: Configurar y gestionar los permisos de acceso y modificación en el software con base en los roles previamente definidos, asegurando que los usuarios tengan únicamente los privilegios necesarios para cumplir con sus responsabilidades de manera segura y eficiente.  OBJETIVO: Implementar técnicamente los roles definidos configurando permisos específicos en el sistema, alineados con las funciones y responsabilidades de cada usuario. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Crear perfiles de usuario en el software basados en los roles previamente definidos. 2. Configurar los permisos de acceso y modificación para cada rol en el sistema, asegurándose de que se respete el principio de mínimo privilegio. 3. Determinar permisos específicos para cada rol (e.g., acceso solo lectura, edición, eliminación). 4. Validar que los permisos configurados se alineen con las funciones descritas en el Registro de Control de Roles y Funciones. 5. Realizar pruebas iniciales para verificar que los permisos configurados cumplen con las políticas de seguridad y los objetivos operativos. 6. Configurar autenticación multifactor (MFA) exclusivamente para los roles que manejan información crítica o realizan modificaciones importantes. 7. Supervisar que las configuraciones de permisos y MFA funcionen correctamente mediante pruebas controladas con usuarios autorizados. 8. Registrar las configuraciones realizadas en el Registro de Control de Accesos, incluyendo: rol, permisos configurados, y usuarios asignados a cada rol. |

* + - 1. Procedimiento para revisar los accesos y permisos asignando accesos únicamente al personal autorizado

|  |
| --- |
| PROCEDIMIENTO PARA REVISAR LOS ACCESOS Y PERMISOS ASIGNANDO ACCESOS ÚNICAMENTE AL PERSONAL AUTORIZADO |
| ACTIVIDAD: Auditar y actualizar periódicamente los accesos y permisos de los usuarios, garantizando que únicamente el personal autorizado cuente con los privilegios necesarios, alineados con sus responsabilidades actuales.  OBJETIVO: Asegurar que los permisos de acceso estén actualizados, minimizando riesgos de accesos indebidos y manteniendo el control sobre la información sensible y las funcionalidades críticas del sistema. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Notificar al equipo responsable de seguridad TI y a los supervisores sobre las fechas de revisión. 2. Exportar una lista completa de usuarios, roles asignados y permisos configurados desde el sistema. 3. Identificar usuarios inactivos, roles duplicados o permisos que no correspondan al rol asignado. 4. Revisar con los responsables de cada área si los accesos asignados a los usuarios son adecuados para sus funciones actuales. 5. Detectar cambios en responsabilidades que requieran ajustes en los permisos o revocaciones de acceso. 6. Eliminar usuarios inactivos o permisos obsoletos. 7. Ajustar o reasignar permisos para reflejar cambios en las funciones de los usuarios. 8. Documentar en el Registro de Control de Accesos todas las modificaciones realizadas, indicando la fecha, los ajustes específicos y el motivo del cambio. 9. Informar a los usuarios sobre modificaciones relevantes en sus accesos y permisos. 10. Proveer una explicación sobre cualquier cambio que limite o modifique sus privilegios de acceso. 11. Realizar pruebas para confirmar que los accesos y permisos actualizados funcionan correctamente y cumplen con las políticas de seguridad. 12. Documentar los resultados en un informe de auditoría de accesos. |

* + - 1. Procedimiento para supervisar el uso de autenticación multifactor para usuarios con permisos de modificación de información

|  |
| --- |
| PROCEDIMIENTO PARA SUPERVISAR EL USO DE AUTENTICACIÓN MULTIFACTOR PARA USUARIOS CON PERMISOS DE MODIFICACIÓN DE INFORMACIÓN |
| ACTIVIDAD: Supervisar e implementar controles para garantizar el correcto uso y funcionamiento del sistema de autenticación multifactor (MFA) en usuarios con permisos de modificación de información crítica, verificando que este mecanismo sea seguro y efectivo.  OBJETIVO: Asegurar que la autenticación multifactor esté configurada correctamente, se utilice de manera adecuada y brinde la protección necesaria contra accesos no autorizados a información y funcionalidades críticas. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Verificar que todos los usuarios con permisos de modificación de información tengan el MFA habilitado y correctamente configurado. 2. Comprobar que los métodos de autenticación secundarios (token, SMS, app de autenticación, etc) sean seguros y estén actualizados. 3. Analizar logs de acceso para identificar posibles anomalías, como intentos fallidos recurrentes o accesos desde ubicaciones inusuales. 4. Reportar y analizar cualquier comportamiento sospechoso. 5. Simular escenarios de autenticación para confirmar que el sistema responde correctamente en condiciones normales y ante intentos no autorizados. 6. Proveer asistencia en la configuración y solución de problemas relacionados con el MFA. 7. Revisar los métodos de autenticación secundaria disponibles, actualizando a tecnologías más seguras si es necesario. 8. Documentar los cambios realizados en la configuración del MFA, fechas de revisión, pruebas realizadas y resultados obtenidos. 9. Compartir los resultados con los responsables de la seguridad del sistema. |

* + - 1. Procedimiento de generación de informe de auditoría

|  |
| --- |
| PROCEDIMIENTO DE GENERACIÓN DE INFORME DE AUDITORÍA |
| ACTIVIDAD: Generar un informe detallado con hallazgos, recomendaciones y cualquier medida correctiva propuesta para asegurar la continuidad en la seguridad de los datos.  OBJETIVO: Documentar y comunicar los hallazgos de la auditoría, brindando recomendaciones y proponiendo medidas correctivas para mantener la seguridad y la integridad de los datos en la organización. |
| PROCEDIMIENTO A EMPLEAR |
| 1. Revisar exhaustivamente los registros de acceso y modificación para identificar posibles anomalías o incumplimientos de políticas de seguridad. 2. Verificar consistencia en los registros y asegurar la integridad de la información evaluada. 3. Documentar cualquier hallazgo relevante, incluyendo accesos no autorizados, cambios no documentados o inconsistencias en los permisos otorgados. 4. Clasificar los hallazgos según su nivel de riesgo y criticidad. 5. Proponer recomendaciones para corregir o prevenir los problemas encontrados, en función de las políticas y estándares de seguridad de la organización. 6. Detallar acciones específicas para corregir las debilidades encontradas, incluyendo asignación de responsabilidades y fechas para su implementación. 7. Estructurar el informe de manera clara y precisa, incluyendo secciones de introducción, hallazgos, recomendaciones y medidas correctivas. 8. Someter el informe a revisión del Jefe de Seguridad de la Información para obtener su aprobación. 9. Incorporar cualquier ajuste sugerido durante la revisión antes de finalizar el informe. 10. Registrar el Informe de Auditoría Trimestral en los sistemas de control documental de la organización. 11. Asegurarse de que el informe esté disponible para consultas futuras y auditorías externas. |

* + - * 1. Procedimiento para realizar simulaciones de ataques de phishing para evaluar la respuesta del personal.

|  |
| --- |
| Procedimiento para realizar simulaciones de ataques de phishing para evaluar la respuesta del personal |
| Actividad: Diseñar y ejecutar simulaciones de ataques de phishing para evaluar la capacidad del personal de identificar intentos de suplantación de identidad y medir la efectividad de las políticas de ciberseguridad.  Objetivo: Identificar vulnerabilidades en la respuesta del personal frente a ataques de phishing. Los resultados permitirán implementar estrategias de capacitación y concientización para fortalecer la seguridad organizacional. |
| Procedimiento a emplear |
| 1. Determinar los objetivos específicos de la simulación (por ejemplo, identificar tasas de clics en enlaces maliciosos, respuesta al reporte de correos sospechosos, etc.). 2. Establecer un alcance claro (departamentos, equipos o personal específico) y las fechas del ejercicio. 3. Crear correos electrónicos de phishing realistas pero controlados, ajustados a los contextos laborales de los usuarios objetivo. 4. Incluir señuelos comunes como enlaces falsos, archivos adjuntos y solicitudes urgentes de acción. 5. Obtener la aprobación de los responsables de ciberseguridad y del área de Recursos Humanos para realizar la simulación. 6. Asegurarse de cumplir con las políticas internas y normativas legales relacionadas con la privacidad y seguridad. 7. Enviar los correos electrónicos a los usuarios seleccionados en el período establecido. 8. Realizar un seguimiento en tiempo real de las interacciones, como clics en enlaces, descargas de archivos o reportes de correos sospechosos. 9. Registrar métricas clave como:    1. Porcentaje de usuarios que interactuaron con el correo (clics o descargas).    2. Tiempo de reacción para identificar y reportar el intento de phishing.    3. Usuarios que ignoraron el correo o lo eliminaron.    4. Evaluar el desempeño del personal y las posibles brechas en la seguridad 10. Elaborar un informe detallado de (Tasa de éxito del ataque simulado, Principales debilidades identificadas). 11. Recomendaciones para mejorar la respuesta del personal. 12. Compartir los resultados con los directivos y responsables de áreas involucradas. 13. Reforzar las políticas de ciberseguridad y mejores prácticas. 14. Asegurarse de que todos los datos recolectados durante la simulación se mantengan confidenciales y se utilicen únicamente con fines de mejora de la seguridad. |

* + - * 1. Procedimiento para asegurar que los respaldos se mantengan en entornos aislados y protegidos contra alteraciones externas

|  |
| --- |
| Procedimiento para asegurar que los respaldos se mantengan en entornos aislados y protegidos contra alteraciones externas |
| Actividad: Implementar y mantener medidas que garanticen la protección, integridad y aislamiento de los respaldos de información crítica, protegiéndolos contra alteraciones no autorizadas y fallos de seguridad.  Objetivos: Asegurar que los respaldos sean accesibles únicamente para fines autorizados, estén protegidos contra ataques cibernéticos y permanezcan funcionales y actualizados para su restauración en caso de incidentes. |
| Procedimiento a emplear |
| 1. Determinar qué información y sistemas requieren respaldos regulares basándose en la criticidad para la operación del negocio. 2. Definir una política clara que especifique:    1. Frecuencia de los respaldos (diaria, semanal, mensual).    2. Tipos de respaldos (completos, incrementales, diferenciales). 3. Configurar entornos de almacenamiento de respaldos aislados de la red principal (por ejemplo, soluciones offline, almacenamiento en cinta, o air-gapped). 4. Emplear servicios en la nube con medidas de seguridad avanzadas, asegurando que los datos estén cifrados en tránsito y en reposo. 5. Cifrar todos los respaldos antes de almacenarlos. 6. Configurar controles de acceso estrictos que permitan únicamente a personal autorizado gestionar los respaldos. 7. Implementar autenticación multifactor (MFA) para el acceso a las herramientas de administración de respaldos. 8. Asegurarse de que el equipo encargado de realizar los respaldos sea diferente del equipo con acceso a los sistemas operativos de producción. 9. Minimizar el riesgo de acceso indebido o alteración interna. 10. Implementar funciones de solo lectura o protección contra escritura en las copias de respaldo. 11. Utilizar sistemas que integren verificaciones de integridad mediante hash para identificar modificaciones no autorizadas. 12. Verificar la consistencia de los datos y evaluar el tiempo necesario para una restauración completa. 13. Establecer alertas para anomalías en el entorno de respaldo. 14. Documentar todos los procedimientos relacionados con la creación, almacenamiento y restauración de respaldos. |

* + - * 1. Procedimiento para establecer roles y permisos restringidos hacia los datos a los por parte de los usuarios

|  |
| --- |
| Procedimiento para establecer roles y permisos restringidos hacia los datos a los por parte de los usuarios |
| Actividad: Establecer y gestionar los roles y permisos de cada usuario en el sistema, asegurando que únicamente tengan acceso a los datos y funcionalidades necesarias para desempeñar sus responsabilidades.  Objetivo: Definir y asignar roles y permisos a cada usuario, garantizando la seguridad, el control de acceso, y el cumplimiento del principio de mínimo privilegio en la gestión de los datos. Esto busca minimizar riesgos asociados con accesos no autorizados o indebidos. |
| Procedimiento a emplear |
| 1. Revisar la estructura organizativa y las funciones de cada área. 2. Identificar los requisitos específicos que determinan los roles de acceso a los datos. 3. Colaborar con los responsables de área para definir claramente las funciones y responsabilidades de los usuarios. 4. Creación de perfiles de roles:    1. Administrador: Acceso total al sistema y a los datos críticos.    2. Supervisor: Supervisión con permisos de revisión.    3. Usuario General: Permisos de consulta según necesidades operativas.    4. Auditor: Acceso a reportes y revisiones de conformidad. 5. Configurar permisos de acceso basados en las funciones de cada rol. 6. Asegurar que los permisos sean coherentes con las responsabilidades asignadas. 7. Realizar pruebas funcionales para confirmar que los permisos asignados operan correctamente y están alineados con las restricciones establecidas. 8. Registrar cada rol y sus permisos en un Registro de Control de Acceso. 9. Detallar nombres de usuarios, roles asignados y niveles de acceso. 10. Guardar toda la documentación en un lugar seguro para auditorías futuras. 11. Informar a los usuarios sobre los roles y permisos asignados. 12. Brindar capacitación sobre el uso del sistema y las políticas de acceso. |

Procedimiento de identificación y definición de qué tipos de eventos deben ser registrados

|  |
| --- |
| PROCEDIMIENTO DE IDENTIFICACIÓN Y DEFINICIÓN DE QUÉ TIPOS DE EVENTOS DEBEN SER REGISTRADOS |
| Actividad: Identificar y definir qué tipos de eventos deben ser registrados, tales como modificaciones, eliminaciones, accesos no autorizados o intentos fallidos de modificación  Objetivo: Establecer qué eventos son críticos para el seguimiento y auditoría, asegurando que se registre cualquier acción que pueda impactar la integridad de los datos, como modificaciones, eliminaciones, accesos no autorizados y errores en intentos de modificación. |
| Procedimientos a emplear |
| 1. Analizar los requisitos regulatorios y de seguridad internos para identificar los eventos clave que deben ser monitoreados, como accesos no autorizados y modificaciones a datos sensibles. 2. Definir y clasificar los eventos en categorías como: 3. Modificaciones de datos: Añadir, actualizar o eliminar información. 4. Accesos no autorizados: Intentos de acceso a datos restringidos. 5. Errores o fallos en operaciones: Intentos fallidos de modificación o eliminación de datos. 6. Crear una lista detallada de eventos críticos que deberán ser registrados, incluyendo una descripción clara de cada evento. |

Procedimiento de uso de las herramientas tecnológicas para auditoría

|  |
| --- |
| PROCEDIMIENTO DE USO DE LAS HERRAMIENTAS TECNOLÓGICAS PARA AUDITORÍA |
| Actividad: Uso de las herramientas o tecnologías más adecuadas en el software para llevar a cabo el registro de auditoría.  Objetivo: Seleccionar las herramientas o tecnologías más adecuadas para implementar el registro de auditoría, asegurando que sean eficaces, escalables y seguras para los datos del sistema. |
| Procedimientos a emplear |
| 1. Verificar que las herramientas cumplan con los requisitos de seguridad necesarios, como el cifrado de los logs y el acceso restringido. 2. Configuración de las herramientas para que trabajen de la manera más óptima. 3. Probar las herramientas en un entorno de pruebas para asegurarse de que puedan capturar los eventos definidos en la subactividad. |

Procedimiento de configuración de funcionalidades de la auditoría en el sistema de software de la institución

|  |
| --- |
| PROCEDIMIENTO DE CONFIGURACIÓN DE FUNCIONALIDADES DE LA AUDITORÍA EN EL SISTEMA DE SOFTWARE DE LA INSTITUCIÓN |
| Actividad: Configurar la funcionalidad de auditoría en el sistema de software, asegurando que se registren las acciones de modificación y eliminación de datos de acuerdo con los requisitos establecidos.  Objetivo: Implementar y configurar el sistema de auditoría en el software para que registre correctamente todas las acciones de modificación, eliminación y accesos no autorizados, garantizando que se sigan los requisitos definidos. |
| Procedimientos a emplear |
| 1. Identificar los módulos o funciones del software donde se realizan las modificaciones, eliminaciones o accesos a datos sensibles. 2. Configurar el sistema de software para que capture los eventos definidos en la subactividad 1 (modificaciones, eliminaciones, accesos no autorizados). 3. Establecer permisos específicos para la visualización de los registros de auditoría, asegurando que solo personal autorizado pueda acceder a los registros. 4. Realizar pruebas de auditoría en el sistema para verificar que todos los eventos importantes se registran correctamente y que la información se guarda en el formato adecuado. 5. Crear una guía detallada para el equipo de TI que describa cómo se configuran y mantienen los registros de auditoría, así como los pasos para realizar el monitoreo y revisión. |

Procedimiento para almacenar los registros de auditoría de manera segura

|  |
| --- |
| PROCEDIMIENTO PARA ALMACENAR LOS REGISTROS DE AUDITORÍA DE MANERA SEGURA |
| Actividad: Establecer un procedimiento para almacenar los registros de auditoría de manera segura, asegurando que no sean modificados o eliminados por usuarios no autorizados. Se generan informes de estos periódicamente.  Objetivo: Asegurar que los registros de auditoría sean almacenados de forma segura, protegidos contra alteraciones o eliminaciones no autorizadas, y que se generen informes periódicos de los registros de auditoría. |
| Procedimientos a emplear |
| 1. Definición de ubicación segura (Establecer ubicaciones físicas o virtuales seguras). 2. Implementar cifrado en reposo y en tránsito para los registros de auditoría, asegurando que los datos sean ilegibles sin las credenciales adecuadas. 3. Configurar controles de acceso basados en roles (RBAC) para que solo los usuarios autorizados puedan consultar o modificar los registros de auditoría. 4. Establecer tareas en el software de forma automática que genera y almacena informes regulares de auditoría que resuman los eventos registrados, permitiendo la revisión periódica por el equipo de seguridad. |

Procedimiento de clasificación de los tipos de datos que son susceptibles de eliminación

|  |
| --- |
| PROCEDIMIENTO DE CLASIFICACIÓN DE LOS TIPOS DE DATOS QUE SON SUSCEPTIBLES DE ELIMINACIÓN |
| Actividad: Clasificar los tipos de datos que son susceptibles de eliminación, diferenciando entre datos temporales, datos sensibles, y datos que deben conservarse por razones legales o de auditoría.  Objetivo: Identificar qué tipos de datos pueden ser eliminados y establecer una clasificación de los mismos, diferenciando entre datos temporales, datos sensibles y datos que deben conservarse por razones legales o de auditoría. |
| Procedimientos a emplear |
| 1. Realizar un inventario de los datos almacenados en el sistema y clasificar cada tipo de dato según su naturaleza. 2. Colaborar con los equipos legales y de auditoría para identificar qué datos deben conservarse por razones legales o de auditoría, y cuáles pueden eliminarse sin comprometer el cumplimiento. 3. Establecer un conjunto de criterios claros para clasificar los datos 4. Crear un documento que detalle las categorías de datos y los requisitos asociados para su conservación o eliminación. |

Procedimiento de definición de niveles de autorización

|  |
| --- |
| PROCEDIMIENTO DE DEFINICIÓN DE NIVELES DE AUTORIZACIÓN |
| Actividad: Establecer los niveles de autorización necesarios para la eliminación de datos. Por ejemplo, especificar que solo personal con ciertos roles o jerarquías pueda aprobar la eliminación de datos, y qué documentos o registros de aprobación se requieren.  Objetivo: Establecer los niveles de autorización adecuados para la eliminación de datos, asegurando que solo el personal autorizado pueda aprobar y realizar estas acciones. |
| Procedimientos a emplear |
| 1. Definir claramente los roles y las jerarquías dentro de la organización que están autorizados para aprobar la eliminación de datos. 2. Crear un sistema de niveles de autorización que incluya aprobaciones múltiples en casos críticos, para evitar la eliminación indebida de datos sensibles o legales. 3. Documentar un proceso formal en el que los responsables de la eliminación de datos deban presentar una solicitud que sea revisada y aprobada por los responsables de los niveles jerárquicos establecidos. 4. Asegurarse de que todos los procesos de eliminación de datos queden registrados con detalles sobre las aprobaciones, como el nombre de quien aprobó, la fecha y la razón de la eliminación. 5. Configurar sistemas que limiten las acciones de eliminación a solo aquellos con permisos apropiados. |

Procedimiento de creación de un proceso formal para que el personal solicite la eliminación de datos

|  |
| --- |
| PROCEDIMIENTO DE CREACIÓN DE UN PROCESO FORMAL PARA QUE EL PERSONAL SOLICITE LA ELIMINACIÓN DE DATOS |
| Actividad: Seguir un proceso formal para que el personal solicite la eliminación de datos, incluyendo un formulario de solicitud o un sistema de gestión de tickets que permita la aprobación o rechazo de dichas solicitudes.  Objetivo: Establecer un proceso claro y formal para la solicitud de eliminación de datos, utilizando formularios o un sistema de gestión que permita el seguimiento de las solicitudes y su aprobación o rechazo. |
| Procedimientos a emplear |
| 1. Crear un formulario estandarizado en el que el personal pueda solicitar la eliminación de datos, incluyendo campos para la descripción del dato a eliminar, la razón de la solicitud, y la aprobación requerida. 2. Definir qué información será necesaria en cada solicitud para garantizar que la solicitud esté completa y cumpla con los requisitos establecidos para la eliminación de datos. 3. Asegurar que todas las solicitudes de eliminación de datos se registren de manera centralizada, para mantener un historial completo de las acciones solicitadas y aprobadas. |

Procedimiento de Clasificación de datos críticos que deben ser respaldados

|  |
| --- |
| PROCEDIMIENTO DE CLASIFICACIÓN DE DATOS CRÍTICOS QUE DEBEN SER RESPALDADOS |
| Actividad: Clasificar los datos críticos que deben ser respaldados, como bases de datos, archivos de configuración del software, registros de auditoría, y cualquier otro dato sensible o importante para la operación.  Objetivo: Identificar y clasificar los datos esenciales para la operación del software, como bases de datos, archivos de configuración, registros de auditoría, y otros datos sensibles que deben ser respaldados para evitar su pérdida. |
| Procedimientos a emplear |
| 1. Realizar un inventario de todos los datos almacenados en el sistema, incluyendo bases de datos, archivos de configuración, logs, y otros elementos que sean fundamentales para la operación. 2. Establecer una clasificación de los datos en función de su importancia para la operación y su sensibilidad. 3. Establecer criterios sobre qué datos deben ser respaldados, cómo deben ser clasificados. 4. Crear una lista detallada y documentada de los tipos de datos que deben ser respaldados, para facilitar la gestión de las copias de seguridad. |

Procedimiento de frecuencia con la que se realizarán las copias de seguridad automáticas

|  |
| --- |
| PROCEDIMIENTO DE FRECUENCIA CON LA QUE SE REALIZARÁN LAS COPIAS DE SEGURIDAD AUTOMÁTICAS |
| Actividad: Establecer la frecuencia con la que se realizarán las copias de seguridad automáticas (diarias, semanales, mensuales) y los horarios más adecuados para ejecutar estos respaldos (por ejemplo, fuera del horario laboral para minimizar el impacto en el rendimiento).  Objetivo: Determinar la frecuencia y los horarios más adecuados para realizar las copias de seguridad, garantizando que los datos críticos se respaldan de manera regular y sin afectar el rendimiento del sistema. |
| Procedimientos a emplear |
| 1. Evaluar la importancia de los datos y la frecuencia con la que se actualizan o modifican para determinar la necesidad de respaldos frecuentes o periódicos. 2. Establecimiento de la frecuencia de respaldo(diaria, semanal). 3. Definir horarios de respaldo automáticos fuera del horario laboral. 4. Crear una política escrita que detalle los horarios y la frecuencia de los respaldos, así como los procedimientos de ejecución. |

Procedimiento de configuración de herramientas o software especializado en copias de seguridad automáticas

|  |
| --- |
| PROCEDIMIENTO DE CONFIGURACIÓN DE HERRAMIENTAS O SOFTWARE ESPECIALIZADO EN COPIAS DE SEGURIDAD AUTOMÁTICAS |
| Actividad: Configurar herramientas o software especializado en copias de seguridad automáticas (como soluciones de backup en la nube, software de backup local, o soluciones híbridas) para realizar los respaldos de manera regular en el software de la empresa.  Objetivo: Configuración herramientas de software que permite realizar copias de seguridad automáticas de manera regular, asegurando que todos los datos críticos sean respaldados adecuadamente. |
| Procedimientos a emplear |
| 1. Configuración de software de respaldo especializado en copias de seguridad automática de la empresa 2. Realizar pruebas para asegurar que las copias de seguridad se realicen correctamente y que los datos puedan ser restaurados sin problemas en caso de una pérdida de información. 3. Configurar alertas automáticas que notifiquen a los administradores si alguna copia de seguridad falla o si no se ha completado correctamente. |

Procedimiento de creación de documentación

|  |
| --- |
| Procedimiento de creación de documentación |
| Actividad: Crear y mantener documentación detallada sobre el proceso de creación de copias de seguridad, las políticas de retención, los métodos de restauración de datos y los procedimientos de emergencia en caso de pérdida de información.  Objetivo: Desarrollar y mantener una documentación completa que explique el proceso de creación de copias de seguridad, las políticas de retención de datos, los métodos de restauración y los procedimientos en caso de emergencia, asegurando una recuperación eficiente de datos. |
| Procedimientos a emplear |
| 1. Crear un esquema detallado de los procesos de respaldo 2. Documentar las rutas y ubicaciones de almacenamiento de los respaldos 3. Detallar el proceso de retención de copias de seguridad 4. Especificar las herramientas de restauración de datos 5. Incluir un plan de recuperación en caso de emergencia 6. Desarrollar un procedimiento para la verificación de las copias de seguridad 7. Registrar los cambios y actualizaciones en el proceso de respaldo 8. Revisión continua de la documentación |

Procedimiento para realizar un inventario del equipo, incluyendo su ubicación física, configuración actual y su software instalado.

|  |
| --- |
| Procedimiento para realizar un inventario del equipo, incluyendo su ubicación física, configuración actual y su software instalado. |
| Actividad: Realizar un inventario detallado del equipo, incluyendo su ubicación física, configuración actual y su software instalado.  Objetivo: Realizar un inventario detallado del equipo, su ubicación física, configuración actual y software instalado para asegurar que el Switch de Red 2 esté correctamente gestionado y seguro. Este inventario servirá como base para cualquier evaluación futura, actualización o auditoría de seguridad. |
| Procedimiento a emplear |
| 1. Registrar ubicación, área y acceso restringido al personal autorizado. 2. Documentar modelo, número de serie, puertos, y verificar funcionamiento sin daños. 3. Documentar direcciones IP, VLANs y políticas de seguridad, asegurando alineación con las mejores prácticas. 4. Documentar el software y firmware, verificando actualizaciones y ausencia de vulnerabilidades. 5. Registrar credenciales y asegurarse de que cumplan con políticas de seguridad, como contraseñas fuertes y autenticación de dos factores. 6. Elaborar un informe con todos los datos recopilados, identificando vulnerabilidades y proponiendo acciones correctivas. |

Procedimiento para implementar cerraduras con autenticación biométrica en puertas de acceso a las salas de servidores donde se encuentra el Switch de Red 2

|  |
| --- |
| Procedimiento para implementar cerraduras con autenticación biométrica en puertas de acceso a las salas de servidores donde se encuentra el Switch de Red 2 |
| Actividad: Implementar cerraduras con autenticación biométrica en puertas de acceso a las salas de servidores donde se encuentra el Switch de Red 2.  Objetivo: Asegurar que solo personal autorizado tenga acceso a las salas de servidores mediante un sistema de autenticación biométrica, reduciendo el riesgo de manipulaciones no autorizadas de los equipos. |
| Procedimiento a emplear |
| 1. Investigar y seleccionar un sistema biométrico compatible con la infraestructura de seguridad de Farmacorp, evaluando facilidad de uso, costo, fiabilidad y soporte. 2. Coordinar la instalación en las puertas de acceso, asegurando una correcta conexión y funcionalidad. 3. Configurar las cerraduras para acceso exclusivo al personal autorizado, registrando huellas dactilares y asociándolas a credenciales electrónicas. 4. Verificar el funcionamiento de las cerraduras y realizar pruebas de emergencia para asegurar el acceso en caso de fallo. 5. Implementar monitoreo para detectar fallos o accesos no autorizados y establecer mantenimiento periódico para asegurar su correcto funcionamiento. 6. Documentar la instalación, configuración y pruebas realizadas, generando un informe con los detalles de la implementación. |

Procedimiento para configurar autenticación de dos factores (2FA) para accesos remotos al switch

|  |
| --- |
| Procedimiento para configurar autenticación de dos factores (2FA) para accesos remotos al switch |
| Actividad: Configurar autenticación de dos factores (2FA) para accesos remotos al switch, asegurando que solo usuarios autorizados puedan operar el dispositivo.  Objetivo: Implementar un sistema de autenticación robusto que minimice los riesgos de accesos no autorizados al Switch de Red 2 mediante la autenticación de dos factores (2FA). |
| Procedimiento a emplear |
| 1. Elegir una solución 2FA compatible con el Switch de Red 2, considerando opciones como aplicaciones móviles, tokens o SMS, balanceando seguridad y facilidad de uso. 2. Configurar 2FA para accesos remotos, integrándolo con el sistema de gestión de usuarios para vincular cada usuario con su método de autenticación. 3. Registrar usuarios en el sistema 2FA y asegurarse de que puedan completar correctamente el proceso de autenticación. 4. Verificar que el sistema 2FA funcione correctamente y probar la recuperación de acceso en caso de pérdida del método de autenticación. 5. Habilitar logs detallados de accesos remotos y configurar alertas para intentos fallidos, notificando al equipo de seguridad. 6. Establecer un programa de mantenimiento periódico para actualizar el sistema y realizar auditorías de seguridad para detectar vulnerabilidades. |

Procedimiento para configurar el Sistema de Gestión de Información y Eventos de Seguridad (SIEM)

|  |
| --- |
| Procedimiento para configurar el Sistema de Gestión de Información y Eventos de Seguridad (SIEM) |
| Actividad: Configurar un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) que permita supervisar en tiempo real los eventos registrados en el switch.  Objetivo: Implementar un sistema SIEM que monitorice los eventos de seguridad del Switch de Red 2, permitiendo detectar y responder rápidamente a intentos de manipulación o acceso no autorizado. |
| Procedimiento a emplear |
| 1. Elegir un sistema SIEM compatible y configurarlo para recibir y procesar eventos del Switch de Red 2. 2. Configurar el Switch para enviar logs de seguridad al SIEM, asegurando su procesamiento en tiempo real. 3. Configurar alertas para eventos críticos como accesos no autorizados y cambios anómalos, ajustando umbrales específicos. 4. Configurar el SIEM para analizar logs y detectar patrones sospechosos, documentando las evidencias de intentos de manipulación. 5. Definir un proceso automatizado para bloquear accesos no autorizados, restaurar configuraciones y generar informes detallados. 6. Monitorear el rendimiento del SIEM y ajustar configuraciones según sea necesario, realizando auditorías periódicas. |

# Conclusiones

Se diseñó un Sistema de Gestión de Seguridad de la Información (SGSI) que cumple con los estándares de la norma ISO 27001:2013. Este sistema asegura la confidencialidad, integridad y disponibilidad de los datos críticos y sensibles de FarmaCorp. Durante el desarrollo del proyecto, se realizó un análisis exhaustivo de los activos de información, clasificándolos según su nivel de sensibilidad e impacto. También se identificaron amenazas y vulnerabilidades, priorizando los riesgos más significativos para aplicar controles efectivos.

Por otro lado, se evidenció que la infraestructura tecnológica robusta de FarmaCorp, junto con las estrategias de respaldo y recuperación, garantiza la continuidad operativa incluso frente a posibles fallos.

# Recomendaciones

* Es fundamental mantener el SGSI actualizado mediante revisiones periódicas que permitan adaptarlo a nuevos riesgos, cambios en la infraestructura tecnológica y normativas emergentes.
* Se recomienda fortalecer la gestión de incidentes implementando simulacros frecuentes y actualizando los protocolos de respuesta, lo que ayudará a reducir los tiempos de recuperación y a minimizar los impactos de los incidentes.
* La automatización de controles debe ser una prioridad, invirtiendo en herramientas que permitan monitorear actividades, realizar auditorías de acceso y detectar intrusiones de forma más eficiente.
* Se sugiere continuar con los programas de capacitación para el personal, enfocándose en roles clave y asegurando que todos los empleados conozcan las mejores prácticas de seguridad.
* Se recomienda ampliar la seguridad física y lógica, reforzando el control de acceso a instalaciones críticas y adoptando métodos de autenticación más robustos, como la autenticación multifactor. También es importante establecer métricas claras para evaluar la efectividad de las políticas implementadas, llevando a cabo auditorías internas regulares y analizando tendencias en los incidentes registrados.

Finalmente, FarmaCorp debe mantenerse al día con los avances en la norma ISO 27001 y otras regulaciones pertinentes, asegurando el cumplimiento continuo y fortaleciendo la confianza de clientes, socios y otras partes interesadas. Estas medidas garantizarán la sostenibilidad y mejora continua del SGSI.

# Referencias

BuenVivir. (2021). *BuenVivirDigital*. Obtenido de https://buenvivirdigital.com/buenvivir/farmacorp/escuela-de-regentes-de-farmacorp-promueve-el-desarrollo-profesional

GenteMotivandoGente. (2022). *GenteMotivandoGente*. Obtenido de https://gentemotivandogente.com/index.php/en/responsabilidad-social-2/267-123-abril-2022-e/3945-farmacorp-empresa-lider-del-sector-farmaceutico-boliviano-celebra-85-anos-de-servicio-a-la-comunidad

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

International Organization for Standardization. (2016). *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. Obtenido de https://www.iso.org/standard/64120.html

International Organization for Standardization. (2017). *ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance*. Obtenido de https://www.iso.org/standard/63417.html

International Organization for Standardization. (2019). *ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls*. Obtenido de https://www.iso.org/standard/67397.html

International Organization for Standardization. (2020). *ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*. Obtenido de https://www.iso.org/standard/77802.html

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. Obtenido de https://www.iso.org/standard/75652.html

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Obtenido de https://www.iso.org/standard/80585.html

International Organization for Standardization. (2024). *ISO/IEC 27006-1:2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems*. Obtenido de https://www.iso.org/standard/82908.html

Sydle. (2022). *Sydle*. Obtenido de https://www.sydle.com/es/blog/mejora-continua-6101a388b2503757979faf52