UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROPUESTA PARA LA GESTIÓN SEGURA DE ACTIVOS TECNOLÓGICOS Y CONTROL DE ACCESOS EN THERMOSOLUTIONS GROUP S.A., UBICADA EN SANTA ANA.

MODALIDAD PROYECTO PARA OPTAR POR EL GRADO DE BACHILLERATO INGENIERÍA EN SISTEMAS DE INFORMACIÓN

ESTUDIANTE

JOSEPH LAZO BADILLA

ENERO, 2025

DEDICATORIA

Este trabajo final de graduación, quiero dedicárselo primeramente a Dios ya que es quien me da la fuerza para seguir adelante, además me ha dado salud y paciencia para estar a punto de cumplir una meta más en mi camino de vida.

A mis padres, ya que siempre han sido un apoyo incondicional, han creído en mí y me dieron las bases de motivación para iniciar una formación académica permitiéndome llegar hasta aquí, ya que son darse cuenta han sido pilares fundamentales en mi vida.

AGRADECIMIENTOS

Agradecerle a mi mamá por su apoyo incondicional, y recordarme siempre lo que soy capaz de lograr y todo lo que representa para mí.

A mi papá por sus consejos de vida, por siempre estar ahí para escucharme y motivarme a seguir adelante y por guiarme a tomar las mejores decisiones.

A mis docentes, tutor y asesores, quienes con su guía, conocimientos y experiencia me ayudaron a construir una base sólida, no solo para este trabajo, sino para mi crecimiento como profesional.

Agradezco a la empresa ThermoSolutions Group, por brindarme el espacio y las facilidades necesarias para desarrollar este proyecto, así como por permitirme aplicar mis conocimientos en un entorno real.

Por último, a la universidad internacional de las Américas, compañeros y a todas las personas que, de una u otra forma, contribuyeron en este proceso.

CONTENIDO

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

La gestión de activos tecnológicos en las empresas representa un desafío, debido a su impacto directo en la seguridad de la información, desorden que afectan la continuidad operativa y el cumplimiento de normas reguladas como por ejemplo la ISO 27001, se propone integrar esta norma en ThermoSolutions Group al identificar múltiples carencias en los procesos relacionados con el control de estos activos.

El no contar con un procedimiento que asegure la devolución de activos de la empresa cuando un empleado finaliza su relación laboral, expone a la organización a incrementar pérdidas económicas y riesgos de fugas de información, esta problemática muestra que es importante adoptar las medidas según los lineamientos en la norma ISO 27001 sobre la gestión adecuada de los mismos.

Muchos empleados tienen acceso por medio de sus credenciales a los sistemas de la empresa, dando como punto crítico la ausencia de controles sobre esos accesos ya que no existen políticas claras para realizar la desactivación de aquellos usuarios que dejan la organización. Para evitar poner en peligro la confidencialidad de la información corporativa se deben colocar controles de acceso robustos, tal y como lo establece el control A.9 de la ISO 27001.

Actualmente los respaldos y recuperaciones de datos son situaciones de prioridad para la empresa que se pueden prevenir mediante la aplicación de las directrices según la norma ISO 27001, este punto debe planificarse para que la empresa cuente con un plan formal para garantizar la disponibilidad de la información en caso de desastres o fallos.

Existe un uso sin control para el manejo de los dispositivos USB, abriendo un fácil acceso al riesgo como lo son la introducción de programa maligno en los sistemas. Para poder disminuir el porcentaje de ingreso de estas amenazas se deben mitigar mediante las políticas restrictivas del manejo de los puertos USB, según las buenas prácticas de la ISO 27001.

Contar con un plan de mantenimiento preventivo de los activos tecnológicos afecta la vida útil de los dispositivos e incrementan los costos a las reparaciones inesperadas, según el control A.12

de la ISO 27001, este tipo de mantenimientos son esenciales para la continuidad y eficiencia de los recursos, y al identificar el problema en la organización se propone asignar la norma.

Finalmente, en la ISO 27001 en el control 7.1, indica que es de suma importancia mantener el control sobre los componentes de la red, es por eso por lo que contar con una representación gráfica de la red tanto física como lógica es importante para dar orden, identificar vulnerabilidades, proponer mejoras y tener una respuesta más rápida a incidentes.

Objetivos

Objetivo General

Elaborar una propuesta de medidas de control y seguridad, mediante la norma ISO 27001, enfocada en los activos tecnológicos, previniendo accesos no autorizados y mitigando riesgos asociados con robos de información y pérdida de datos.

Objetivos Específicos

Establecer un procedimiento para la devolución segura de activos tecnológicos que garantice el control y registro adecuado al momento de la salida de empleados.

Implementar un sistema de gestión de accesos que incluya la desactivación o modificación de credenciales de usuarios que dejan la empresa, asegurando así un control efectivo sobre los sistemas.

Desarrollar políticas de respaldo y recuperación de datos que aseguren la creación de copias periódicas y un plan de recuperación ante desastres, alineadas con los requisitos de la norma ISO 27001.

Establecer una política de control de dispositivos de almacenamiento USB en las computadoras que asegure la regulación de accesos según la norma ISO 27001.

Elaborar un procedimiento de mantenimiento preventivo y correctivo para los equipos tecnológicos, asegurando su operatividad y alineación con los estándares de seguridad de la norma

ISO 27001.

Documentar la topología de red de la empresa para la segmentación adecuada de los componentes y la protección de datos críticos, conforme a las directrices de la norma ISO 27001.

Justificación del proyecto

Como se mencionó previamente, ThermoSolutions Group es una empresa que no tiene una gestión adecuada de los activos tecnológicos, gestiona los inventarios sin seguir procedimientos o políticas adecuadas, el departamento no cuenta con un proceso para la gestión de estos activos, ni un seguimiento de las actividades o un control especifico.

Las deficiencias detectadas en la organización, tales como la ausencia de devolución de activos, la administración incorrecta de accesos a los sistemas, la ausencia de un plan de recuperación para su base de datos, la ausencia de control para la conexión de dispositivos de almacenamiento por USB, la ausencia de supervisión en el mantenimiento preventivo de los equipos y la estructura de red física y lógica sin documentar, son fallos que conducen a obtener riesgos en la seguridad de la información, productividad y una respuesta ineficiente ante algún incidente.

Con esta investigación se podrán diseñar e implementar las políticas y procedimientos con las mejoras practicas otorgadas por la norma ISO 27001, abordando una mejoría en los recursos existentes de la empresa y asegurando la protección de la información crítica para garantizar el cumplimiento de la norma y reducir el daño a cualquier riesgo de los sistemas.

Dentro de los beneficios que se esperan alcanzar se destacan la implementación de los controles para que se pueda proteger la confidencialidad, integridad y disponibilidad de los datos críticos de la empresa, asegurando la correcta utilización, mantenimiento y actualización de los activos pasa así prolongar su vida útil y reducir posibles costos.

Por otra parte, las interrupciones ante un incidente por falta de respaldos se minimizarán por medio de un plan y recuperación garantizando que todos los puntos se cumplan con los lineamientos de la norma ISO 27001, para ayudar a los empleados y al personal de TI trabajar de una manera más estructurada y eficiente.

Inspenet en su página Web hace énfasis a que una la mala gestión de los activos de TI puede elevar los costos de mantenimiento, reparación y reemplazos antes del vencimiento de la vida útil de los equipos, afectando la rentabilidad y operatividad de la organización.

Viabilidad técnica de la investigación

El desarrollo de la investigación es realizable, se basa en políticas y procedimientos establecidos por los estándares de la norma ISO 27001, es una norma que en el mercado es reconocida y que se aplica perfectamente en la gestión de los activos tecnológicos donde la infraestructura de TI actual y lo necesario para desarrollar capacitaciones de la empresa garantizan la posibilidad de implementar las medidas propuestas.

Las soluciones propuestas, pueden ser implementadas mediante herramientas disponibles en el mercado, diseñadas específicamente para satisfacer este tipo de requerimientos y además la organización cuenta con algunos recursos que se pueden aprovechar en el proyecto para complementarlos con elementos adicionales necesarios, como la compra de software especifico y certificados actualizados de la norma ISO 27001 a establecer.

Para garantizar la viabilidad técnica del proyecto, se requiere disponer de lo siguiente:

- **Hardware:** No será necesario adquirir hardware adicional ya que la empresa cuenta con dispositivos tecnológicos que ayudaran a realizar los procedimientos y procesos de control de activos, los cuales son:
    a) Router: Dispositivo modelo Dream Machi Ubiquiti el cual es administrable, permitiendo visualizar mediante un panel cuales son los dispositivos que están conectados a la red, la cual será una herramienta útil para el desarrollo de la topología física y lógica.
    b) Computadora: La empresa brindará una computadora Marca Dell, la cual servirá para realizar los procedimientos en Word y Excel.
    c) Servidore: La empresa cuenta con un servidor físico para hospedar la base de datos del ERP la cual nos va a servir para instalar el módulo de activos fijos.

d) Impresora: La empresa con varias impresoras en los departamentos, la cual servirá para imprimir documentos que se requieran en el proceso de investigación.
e) Switches: Dispositivos administrables y adoptados por el router, lo que permite tener visibilidad de toda la red por departamento, administrando dispositivos conectados como computadoras, puntos de acceso inalámbricos, impresoras y teléfonos.

- **Software:**
  a) La empresa cuenta con un sistema ERP el cual están conscientes y anuentes a adquirir con el proveedor la instalación y compra del módulo de activos fijos, esto con el fin de manejar un control e inventario de cada uno para mejorar el seguimiento y la trazabilidad.
  b) Administración del Office 365, Active directory y acceso remoto por medio de VPN, son herramientas activas con las que cuenta la empresa la cual serán útiles para establecer las políticas de control de accesos, desactivación de usuarios y credenciales.
  c) Para la recuperación de datos se utilizar la solución de Microsoft OneDrive en su última versión lanzada en octubre de 2024 que esta adquirida por la empresa y para la recuperación de la base de datos ante algún incidente se debe implementar el sistema llamado Veeam con su versión 8.1.305 liberada 23 enero 2025.
  d) Para la realización de la topología de la red se utilizará el dispositivo adquirido por la empresa llamado dream machine de la marca Unifi, con soporte de actualizaciones hasta el año 2029, el cual la empresa lo tiene disponible y no dará una imagen clara y detallada.
  e) Se deberán adquirir los certificados oficiales más recientes de la norma ISO 27001 por parte del estudiante, para garantizar que las políticas y procedimientos diseñados se cumplan adecuadamente.

- **Espacio Físico:** La empresa cuenta con instalaciones suficientes que no afectan las actividades del proyecto, tanto el área de servidores como las estaciones de trabajo por consiguiente no será necesario realizar adecuaciones físicas a gran escala.

Viabilidad operativa de la investigación

A nivel operativo la investigación es viable ya que se adapta con las actividades actuales de la empresa y está diseñado para integrarse de manera efectiva con los procesos actuales de la organización, por lo tanto, no se va a requerir reestructuraciones significativas en cuanto a la implementación de las políticas y procedimientos propuestos lo que resulta un impacto positivo a nivel organizacional sin embargo, para llevar a cabo este proyecto, se requiere conocimiento en las siguientes áreas :

- Para implementar políticas efectivas de monitoreo, registro y control de activos.
- Manejo del módulo de activos fijos del sistema ERP con el que cuenta la empresa.
- gestión en los accesos y seguridad de la información para poder establecer los estándares adecuados del control de los accesos y las contraseñas.

El personal de TI, proveedores de software y expertos en la norma ISO 27001 deberán llevar a cabo talleres sobre las políticas y procedimientos, en el uso del nuevo módulo de activos, así como la información básica al personal administrativo que en sus tareas laborales tenga alguna relación con el sistema y por último capacitar al personal en el cumplimiento de las nuevas regulaciones anteriormente mencionadas para garantizar el éxito de la investigación y el proyecto donde es importante recalcar que estos talleres y capacitaciones no forman parte del alcance de la investigación y deben organizarse de manera independiente por la organización.

El departamento de será uno de los principales responsables en gestionar y darle seguimiento a los activos tecnológicos para garantizar el cumplimiento de las políticas, sin embargo, el personal administrativo será el responsable de la entrega, recepción y asignación de activos tecnológicos a los colaboradores.

Por otra parte, existen usuarios indirectos que van a requerir supervisar el cumplimiento de las políticas y garantizar que los equipos estén cumpliendo con los objetivos operativos del departamento.

Impactos positivos en la forma de realizar las tareas:

- La mejora de los procesos cuando se trata del control de asignación y devolución de activos reducirá las pérdidas y mejorará la trazabilidad.

- Con la implementación de los procedimientos para realizar los respaldos de la información serán cambios que garanticen la recuperación ante desastres.
- Uso del ERP en el módulo de activos fijos, que ayudara a gestionar un inventario, tiempo de depreciación, control de mantenimiento, ubicación y agilizara las tareas administrativas relacionadas a estos.

Viabilidad económica de la investigación

Costos de Software

- La empresa cuenta con el ERP, y van a comprar el módulo de activos fijos para gestionar todos los dispositivos a registrar.

Costo: $1,500 dólares

- Para la gestión de respaldos de las bases de datos se debe contar con una licencia capaz de realizarlos, se opta por “Veeam Backup & replication” la cual es compatible con respaldos de máquinas virtuales y servidores físicos configurando otro servicio como repositorio.

Costo: $ 1,815 dólares anual.

Costo de hardware

No se necesitarán adquirir hardware adicional, la empresa cuenta con las herramientas y dispositivos tecnológicos adecuados para soportar el software solicitado.

Espacio físico

Se asignará un espacio físico exclusivo para poder mantener el inventario de manera segura, ya que como parte del procedimiento es cuidar los recursos de la organización y así cuidar los activos tecnológicos, cabe resaltar que no se requiere invertir en la ampliación del espacio físico, pero si en el mobiliario que asegura la organización y seguridad del inventario.

Costo: $350 dólares.

Otros costos

- Se debe considerar la capacitación del módulo de activos fijos, con una duración de dos horas donde participa el departamento de TI, contabilidad y el auditor interno de la compañía.

Costo: $160 dólares.

- Se deben comprar las certificaciones de la ISO 27001 con la versión más reciente para guiar el diseño e implementación de los controles.

Costo: $ 200 dólares.

- Para el registro de inventario, generación de políticas y capacitaciones se debe contemplar un gasto menor en papelería e impresiones.

Costo: $100 dólares.

Tabla1
Resumen de costo.

Tipo de costo	Precio
Software	$ 3,315.00
Hardware	$0.00
Mobiliario	$ 350.00
Otros (capacitaciones, certificaciones y materiales)	$ 460.00
Total	$ 4,125.00

Elaboración Propia

Justificación de costos

Como parte del compromiso por la mejora en activos tecnológicos y seguridad de la información la inversión será cubierta por la empresa pagando un total de $ 4125 dólares, considerando los beneficios que aportará es un costo razonable tomando en cuenta la reducción de los riesgos e incremento de orden administrativo aprovechando los recursos existentes que la organización tiene como la infraestructura y sistemas.

Esta inversión permitirá disminuir costos con relación a la pérdida de activos tecnológicos, posibles incidentes en la seguridad y muchos errores por falta de control de inventarios, lo que garantiza que el monto de dinero pagado sea de recuperación rápida.

Viabilidad legal

El cumplimiento a la normativa nacional debe estar ajustado a las leyes y los reglamentos de Costa Rica en lo que tiene que ver con la protección de los datos, como la ley (N°8968) la cual hace énfasis en la obligación de proteger los datos de los empleados, clientes y proveedores.

Esta investigación se diseñará balo los lineamientos de la norma ISO/IEC 27001 que estipula una seria de controles específicos para la protección de los activos tecnológicos (Sección A.8), la gestión de accesos (A.9) y el cumplimiento legal (A.18).

Como una limitante legal, todo software debe estar estrictamente con licencias originales para evitar problemas legales que alteren el orden a la propiedad intelectual o el uso inadecuado de software.

En la actualidad la empresa no cuenta con políticas formales para el control de los activos tecnológicos, ninguno es registrado en un sistema, solamente se monitorean de manera calculada por lo que no existe algún proceso estructurado cuando se trata de alguna devolución de los equipos ni para las desactivaciones de los accesos cuando algún empleado deja la empresa. Tampoco existe un protocolo de respaldos de la información de los accesos confidenciales.

Requisitos legales de la investigación

Manejo de los activos Tecnológicos: En la cláusula de (ISO/IEC 27001: A.8.1.1) es requisito identificar y registrar todos los activos tecnológicos, para asegurar que estén protegidos y gestionados adecuadamente.

Accesos a los sistemas: cuando un usuario se retira de la compañía ya sea por renuncia o despido se debe contar con un control de acceso basado en los privilegios mínimos y desactivaciones inmediatas de las credenciales de acceso, basándose en la norma (ISO/IEC 27001: A.9.2.1).

En la cláusula (ISO/IEC 27001: A.12.3.1), Se enfoca en el respaldo y recuperación de datos como un plan formal para la creación de copias de seguridad y prevención ante algún incidente.

topología de red: Crear un mapa detallado, tomando en cuenta la parte física como la lógica, para poder identificar los puntos de conexión, segmentos y dispositivos asociados basándose en la (ISO/IEC 27007: 8.9).

En términos legales la implementación de normas y políticas son viables, ya que las medidas que se incluyen para documentar y proteger la infraestructura de la red, controles formales para la gestión de activos, accesos y datos que permitirá a la organización operar de una manera más segura y eficiente basándose en los lineamientos de la norma ISO/IEC 27001, así como la implementación de los controles formales relacionados con la red.

Proyecciones

La investigación se proyecta mediante la norma ISO 27001 fortalecer en ThermoSolutions Group la gestión de todos los activos tecnológicos, reduciendo el riesgo a fugas de datos y accesos no autorizados donde con estas políticas y procedimientos claros realizara un orden y cumplimiento efectivo de la norma.

A través del módulo de activos fijos se llevará a cabo un inventario detallado, donde podremos registrar la fecha de compra, ubicación por departamento, responsable, se asignará la proyección de la vida útil en meses y un código único que diferenciará al activo para su registro, además, contando con un plan de respaldo de datos, la empresa minimizará el tiempo de inactividad en caso de desastres o fallos.

Se pretende mejorar el inventario y con ello disminuir los costos por perdidas y fallos en sistemas para que la organización tenga como finalidad operar más eficiente, ordenada, competitiva y segura, garantizando su uso correcto de los recursos tecnológicos y estableciendo una base sólida para el crecimiento de la organización.

Alcance funcional

En el inventario de los activos tecnológicos, se debe contar con la identificación, registro y clasificación de los activos como: servidores, computadoras, celulares, equipos de red, etc., todo se debe manejar en el sistema centralizado del módulo de activos fijos del ERP, y rastrear o monitorear el estado, ubicación, mantenimiento y uso para verificar que se esté realizando su correcta administración.

Además del inventario, la seguridad de activos, copias de seguridad y el orden en la topología representan una suma importante de valor a la organización con la ayuda de los protocolos y procedimientos que aseguran la protección y disponibilidad de los datos críticos.

Tabla 2

Procedimientos de la investigación.

Nombre del apartado	**Descripción del apartado**
Procedimiento de Seguridad de Activos de Cómputo.	Se establecerá una política de recolección de activos de cómputo, en la cual se elaborará un documento de la entrega y su verificación de inventario en el módulo del sistema de activos.
Control de acceso y gestión de contraseñas	Se implementará un protocolo para los exempleados, desactivando o cambiando credenciales de todos los sistemas, esta política incluirá eliminación de accesos remotos o herramientas de autenticación.
Seguridad de la información.	Se implementarán dos políticas relacionadas con el respaldo y recuperación de datos. Las políticas incluirán la realización de copias de seguridad periódicas y la creación de un plan de recuperación ante desastres de acuerdo con la norma ISO/27001:2022 ,17.1

Control de puertos USB	Se implementará una política de bloqueo de puertos USB en todos los equipos de la empresa, exceptuando aquellos que necesiten autorización para el uso de dispositivos.
Procedimiento de mantenimiento	Se implementará un plan de mantenimiento preventivo y correctivo para los equipos tecnológicos, conforme al Control A.12.1.2 de la norma ISO 27001 y así la documentación del historial de mantenimiento en el sistema de gestión de activos.
Control de la Topología de Red bajo ISO 27001	Se implementará una documentación detallada de la topología de la red, conforme al Control 8.9 de la norma ISO 27001, que permita visualizar y gestionar de manera efectiva los componentes de la red, asegurando la correcta segmentación y protección de los datos críticos. Esta documentación incluirá tanto la topología física como lógica, y se mantendrá actualizada para garantizar la seguridad en las comunicaciones, facilitar el mantenimiento de la infraestructura

Fuente: Lazo, 2025.

Alcance Metodológico

La investigación de adapta a la metodología Scrum la cual con el enfoque ágil garantiza la flexibilidad y una adaptación constante y continua a la entrega de los resultados, los trabajos se organizarán con los ciclos de desarrollos Sprints, lo que ayudara a realizar los ajustes a cada avance y cumplir porque los objetivos se alcancen conforme a las necesidades de la empresa.

Fases del Proceso

- Primera fase es clave del proyecto ya que inicia por la identificación de los activos a registrar, en analizar las áreas de mejora y los procedimientos que se van a implementar

evaluando los recursos necesarios como software, hardware, políticas y roles dentro del equipo.

- Sprints de implementación:
    - Lista de activos y desarrollo de las políticas de control de acceso
    - Implementar el sistema de respaldo y la recuperación de los datos.
    - Uso del USB y mantenimiento preventivo de los activos mediante el despliegue de las políticas de seguridad.
    - Elaboración de la topología física y lógica de la red.
- Como retroalimentación, después de cada sprint, se debe realizar la revisión con los involucrados del proyecto que son TI, administrativos y altos mandos como gerencias para verificar cada avance y gestionar los ajustes en caso de ser necesario con el fin de darle mayor forma a los objetivos de la organización.

Con el enfoque ágil a presentar permite realizar ajustes cada vez que surgen nuevos desafíos y necesidades asegurando siempre que los controles y procedimientos sean mejorados de manera constante gracias a la implementación por fases, los beneficios del proyecto permitirán a la empresa aplicar los controles a medida que avanzan las etapas.

Alcance tecnológico

Como parte esencial de implementar los procedimientos es recalcar que se basa en uso de las tecnologías o herramientas enfocadas y alineadas en la ISO 27001 para garantizar que la seguridad y administración de la información y los recursos de la organización es la adecuada, utilizando el módulo de activos fijos el cual tiene la capacidad de registrar estos dispositivos el cual cada uno de ellos.

Como alcance tecnológico de los procesos contribuye en reducción de perdidas o mejora en los costos, fortaleciendo la seguridad ya que la información estará con políticas rigurosas asegurando que la empresa siempre cumpla con los estándares adecuados con el fin de garantizar continuidad del negocio y que su base sea sólida para ser competitiva y con posibilidades de crecimiento.

Este alcance es muy importante ya que es clave para el éxito de la investigación porque al optimizar los recursos evita gastos innecesarios o esfuerzos duplicados manteniendo un enfoque en los

objetivos claves para asegurar que cada etapa sea un cumplimiento requerido por la organización y así que todos trabajen enfocados en un mismo propósito.

CAPÍTULO II: MARCO REFERENCIAL

Antes de iniciar con el marco referencial, es importante definir y conocer los diferentes tipos de activos de TI, estas definiciones son de tipo especifico que según Vargas y Ollarves (2020) son:

- Hardware de infraestructura
- Convenios de alquiler o rentas de instalaciones e infraestructura de TI
- Software desarrollado internamente
- Licencias de software
- Equipos de usuario final (p.201).

Como un propósito para esta investigación es expresar el problema que enfrenta la organización al no contar con un buen manejo de los activos tecnológicos, pero gracias a la norma ISO/IEC 27001:2022, se puede asegurar que los procedimientos pueden mejorar y ser el canal óptimo para lo que la empresa necesita, así como lo expresa María, A. L. E (2021) menciona que "la información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización" (p.334), estoy de acuerdo con el autor ya que en la actualidad la falta de conocimiento o de buen manejo del proceso, genera una organización más vulnerable ante un ataque, riesgo de seguridad, robo de información y mal manejo de los recursos de la empresa , así también concuerda con el comentario de Watkins (2022) que indica que "el estándar ISO 27001:2022 es una norma internacional que establece los requisitos para la creación, implementación y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque radica en resguardar la información sensible de una organización, gestionando eficazmente los riesgos de seguridad. Esta norma ofrece un marco integral basado en un ciclo de vida, abarcando desde la planificación hasta la mejora de los controles de seguridad" (p.45).

Según Calder (2023) "mediante la implementación de controles de seguridad adecuados, como el cifrado de datos, el control de acceso y la segmentación de redes, las empresas de servicios tecnológicos pueden salvaguardar información confidencial, minimizando el riesgo de exposición a amenazas internas y externas" (p.35), es por eso por lo que la norma es aplicable para lo que la organización requiere y el manejo de los activos es adaptable al entorno seguro y eficiente por medio de los procedimientos.

Todo lo que este distinguido como un activo fijo tiene un ciclo de vida, y existen algunas características importantes que ayudan a conservar su funcionamiento y cumplir correctamente con su periodo de vida útil, por eso estoy de acuerdo con Víctor (2021) ya que clasifica este ciclo en "el mantenimiento preventivo es un tipo de intervención que se realiza antes que resulte el desperfecto, y tiene por fin minimizar los problemas técnicos y mitigar los costos de reparaciones o paradas. El mantenimiento correctivo, es un tipo de intervención que se realiza cuando ocurre una falla que implica una desmejora o paralización del proceso productivo. El mantenimiento predictivo es que, dado ciertos parámetros de funcionamiento, puede anticipar a las fallas esperadas de los equipos" (p.39), con esa mención nos aclara el panorama de que la investigación debe mitigar el mal manejo de los activos tecnológicos en la organización.

Amenazas de un activo tecnológico

Las amenazas de un activo se dividen en dos tipos las cuales según menciona Rodríguez (1995) "las internas corresponden a personas dentro de la organización, pueden ser mal intencionadas al tratar de dañar un sistema o robar la información o por desconocimiento de uso, puede llegar eliminar la información. En cambio, las amenazas externas, se refieren a problemas del entorno donde está el activo o sistema, por ejemplo: sismos, desastres naturales, inundaciones, entre otros" (p.38).

Las empresas hoy deben saber identificar los riesgos que pueden poner en peligro o afectación a los activos, por eso es importante analizar la posibilidad de cómo puede materializarse una vulnerabilidad y así evaluar las consecuencias que esto podría generar , ya que así como lo indica Rodríguez (1995) "la seguridad de la información tiene como meta proteger los activos o recursos de las organizaciones de pérdida y asegurar la viabilidad de las operaciones de la organización si ésta llegara a ocurrir" (p.12).

Dentro de las acciones a considerar Vargas y Ollarves (2020) citando a Valencia Duque y Orozco menciona que "las organizaciones se encuentran en el dilema de contar con una gran cantidad y variedad de activos tecnológicos, y tener que establecer y clasificar estos activos puede ser una tarea de grandes proporciones, sobre todo en aquellas grandes organizaciones" (p.197). En ese contexto, la seguridad de la información debe darse en el proceso de comprender, identificar y clasificar los activos.

Además, una identificación de riesgos es crucial para cualquier infraestructura de TI, así lo menciona Vargas y Ollarves (2020) que “la identificación de activos es crucial y debe iniciarse antes de que se identifique cualquier riesgo. Pretende identificar y priorizar los activos de acuerdo con sus niveles de criticidad en la organización” (p.203), me parece importante ya que antes de identificar una vulnerabilidad o evaluar una amenaza, primeramente, debemos iniciar por identificar los riesgos de acuerdo con la importancia de un activo con relación a su rango de criticidad.

Gestión de activos

La implementación de un sistema para gestionar los activos tecnológicos es un beneficio para la organización ya que contribuye a la buena gestión y ayuda a aplicar las normas de una manera más ágil y transparente, así se concuerda con Johan C (2021) al mencionar que “al querer avanzar con un sistema informático que no vaya según las necesidades de la organización, existirán inconvenientes en todas las aéreas que manejan el control de activos, y esto llevará a que surjan más complicaciones al instante de hacer las ocupaciones de recolección y actualización de información del inventario” (p.107), además de contar con un software para la gestión de los activos Mogollón E (2021) definen a la gestión de activos como “un modelo de negocio, basado en un enfoque de tipo estratégico; para ello, deben alinearse varias áreas esenciales que aporten un valor fundamental en la organización tales como: operaciones, mantenimiento y decisiones de inversión de capital” (p.34), es por eso por lo que la organización con ayuda de una buena gestión reduce la perdida de inventario y cuida la vida útil de los equipos o software.

Además de lo mencionado anteriormente, la investigación hará énfasis a los controles establecidos por la norma ISO/IEC 2007:2022, la cual en su clausula 8.0 es llamada “controles tecnológicos”, por ende, podemos decir que como parte de la gestión la norma en su clausula 8.2 indica que “Se restringirá y gestionará la asignación y el uso de derechos de acceso privilegiados.”, haciendo énfasis directo a los derechos de accesos privilegiados, además en su apartado 8.12 también hace énfasis a la restricción de accesos a la información, mencionando que “Se aplicarán medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible” (p.18).

Asimismo, la Norma ISO/IEC 27001 (2022) indica que “El sistema de gestión de seguridad informática preserva dichos pilares mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente” (p.4). Por consiguiente, las políticas y procedimientos son la guía para implementar en la organización de ThermoSolutions con el objetivo de establecer el manejo adecuado de los activos y por consiguiente de la información.

Ciclo de Vida de los activos de TI

Todo tipo de activo tiene su periodo de vida útil, en el caso de los activos de TI es comprendido por un conjunto de pasos o fases que según los autores Vargas y Ollarves (2020). Son:

- Plan: La estrategia y las decisiones sobre que activos se necesitan dentro de la organización.
- Adquisición: Se adquiere mediante la compra, construcción, arrendamiento o concesión de las licencias.
- Asignación: Comprende la instalación, integración con otros componentes.
- Mantenimiento: Puede ser necesario realizar mantenimiento para maximizar el valor para los usuarios, extender la vida útil del activo y mitigar riesgos.
- Retiro: Incluye la transición de usuarios a otros recursos, cancelación de acuerdos, renovación de licencias y el inicio de la planificación de reemplazo. (p.202)

De acuerdo con el texto anterior, una gestión eficiente es garantizada mediante un control de los activos tecnológicos de acuerdo con su ciclo de vida, además esto permite tener un control total para optimizar los recursos, reducir riesgos y cumplir con los estándares de la norma ISO ya que según menciona Rodríguez (1995), “Clasificar la información de acuerdo a su importancia para la empresa para saber qué tanta seguridad se necesita para cada tipo de información, cuánto tiempo necesita ser retenida, a quién se le dará acceso, si se requieren duplicados de la información o no,

etc.” (p.14), según lo expuesto por Rodríguez, asegurar la información ante posibles amenazas es indispensable darle trazabilidad.

A continuación, para comprender el orden del ciclo, se muestra la figura que grafica los procedimientos mencionados

Figura 1.

Ciclo operativo de los activos

Fuente: https://www.e-dea.co/blog/gestion-activos-ti

Beneficios de la gestión del ciclo de vida de los activos

Gestionar los activos de TI por medio del ciclo de vida aporta valor, así lo menciona cobit en su versión 5 que “los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia”, esta mención esta enfatizada en la matriz de “practicas clave de gestión” la cual está compuesta por cinco claves que son: “Identificar y registrar activos actuales, Gestionar activos críticos, gestionar el ciclo de vida de los activos , optimizar el costo de los activos y administrar licencias” (p.163).

Una buena gestión del ciclo de vida de los activos ayuda a tener algunos beneficios valiosos para las organizaciones después de contar con una implementación con estrategia efectiva, IBM (2024) menciona estos beneficios:

- Vida útil prolongada: Con la información recopilada de un activo a través de sensores (IoT), los operadores ahora pueden medir el rendimiento de los activos en tiempo real. Con esta información, pueden reparar los activos antes de que se averíen, sustituir piezas clave cuando sea necesario y programar el mantenimiento cuando sea óptimo para su organización.
- Reducción del costo y el tiempo de inactividad: Cuando las organizaciones asumen un papel proactivo tanto en el monitoreo como en la mejora del rendimiento de sus activos a través del mantenimiento programado regularmente en lugar de esperar una avería, reducen la probabilidad de costosas reparaciones y tiempo de inactividad.
- Mayor eficiencia: Según una encuesta reciente de IDC (1), aumentar la eficiencia operativa fue la principal prioridad para las organizaciones en 2022 (51 %). Para conseguirlo, muchas están invirtiendo en estrategias de gestión del ciclo de vida de los activos que utilizan las capacidades del IoT y la inteligencia artificial para realizar el mantenimiento preventivo.

Además de los beneficios mencionados por IBM, cobit v5 enfatiza que “gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente” (p.165). Estoy de acuerdo ya que una organización con el proceso del ciclo de vida activo y en ejecución, promueve desde un inicio el cuido y mitiga el riesgo de los dispositivos.

CAPÍTULO III: MARCO METODOLÓGICO

Enfoques de investigación

Para conocer el método de cómo se lleva a cabo la recolección y análisis de los datos, es importante detallar los diferentes enfoques disponibles los cuales se presentan como métodos cualitativos, cuantitativos y mixtos. Según Hernández R; Fernández C; Baptista P. (2014) citando a Grinell (1997) los enfoques:

- Llevan a cabo la observación y evaluación de fenómenos.
- Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.
- Demuestran el grado en que las suposiciones o ideas tienen fundamento.
- Revisan tales suposiciones o ideas sobre la base de las pruebas o del análisis.
- Proponen nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones e ideas o incluso para generar otras. (p.4)

Enfoque cuantitativo

Uno de los enfoques utilizados para recolección y análisis de datos numéricos es el enfoque cuantitativo, se característica por la medición y cuantificación de las variables lo que permite realizar relaciones y las estadísticas, según Romero et al., (2023). Indica que "Se utiliza para medir y cuantificar variables, establecer relaciones y realizar generalizaciones estadísticas" (p.15) , además de lo mencionado, el método o enfoque cuantitativo tiene cuatro características claves que según Romero et al., (2023) son "La objetividad y replicabilidad, muestra grande y representativa, análisis estadístico y el enfoque deductivo" (p.15), estas características son valiosas para lograr que el enfoque sea una herramienta confiable para medir los fenómenos y realizar la toma de decisiones basadas en los datos objetivos.

Enfoque Cualitativo

Tal y como su nombre lo indica podríamos comprender que el enfoque mixto es la combinación de ambos métodos cuantitativo y cualitativo , integrando el análisis numérico y estadístico del método cuantitativo pero la compresión de significados del método cualitativo, y Romero et al., (2023) expresa que “al combinar los métodos cuantitativos, que se centran en la recopilación y análisis de datos numéricos para identificar patrones, relaciones y tendencias, con los métodos cualitativos, que se enfocan en la comprensión y explicación de significados, experiencias y contextos sociales, la investigación mixta permite capturar la complejidad y multidimensionalidad de los fenómenos investigados” (p.18). Estoy de acuerdo ya que integrar estos dos enfoques se obtiene una comprensión más completa de las problemáticas estudiadas.

Enfoque Mixto

Tal y como su nombre lo indica podríamos comprender que el enfoque mixto es la combinación de ambos métodos, y Romero et al. (2023) expresa que “al combinar los métodos cuantitativos, que se centran en la recopilación y análisis de datos numéricos para identificar patrones, relaciones y tendencias, con los métodos cualitativos, que se enfocan en la comprensión y explicación de significados, experiencias y contextos sociales, la investigación mixta permite capturar la complejidad y multidimensionalidad de los fenómenos investigados” (p.18).

Enfoque de investigación seleccionado

Por lo tanto, esta investigación se realiza mediante un enfoque cualitativo, ya que este proceso es inductivo, recurrente, analiza diferentes realidades subjetivas y no tiene secuencia lineal, por lo tanto, este enfoque resulta adecuado para el estudio ya que uno de los objetivos principales del proyecto es comprender y considerar las experiencias, criterios y puntos de vista del departamento de TI y demás involucrados, de acuerdo con su administración de los activos tecnológicos. Según Hernández, C. (2014) “este tipo de investigación no tiene en un principio un concepto claro de lo que se estudia ni una hipótesis que después se pueda validar. Los conceptos y las hipótesis se van formulando a lo largo de la propia investigación” (p.189).

Tipos de investigación

La investigación cualitativa ofrece mayor flexibilidad y profundidad en comprender los fenómenos estudiados, brindando una visión más clara y detallada de la realidad, comenzando desde la interacción con los involucrados de estudio e interpretación de sus experiencias; este enfoque tiene variedad de métodos y técnicas que están diseñadas para explorar, comprender e interpretar los diferentes tipos de resultados que se generan, las cuales dependen del tipo de problema de investigación, del análisis de datos utilizado y el objeto del estudio. El método o diseño de investigación según Hernández et al., (2014), "es el plan o estrategia que se desarrolla para obtener la información que se requiere en una investigación y responder al planteamiento" (p.128). De acuerdo con lo mencionado anteriormente, los tipos de investigación son:

Investigación descriptiva

La investigación descriptiva puede elaborarse en un enfoque cuantitativo o cualitativo, sin embargo, en esta descripción abordamos solamente hacia el enfoque cualitativo, donde Según Valle A; Manrique L; Revilla D. (2022). Citando a Guevara et al. Menciona que "El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas" (p.14). Tomando la cita de los autores, este tipo de investigación no busca explicar porque ocurren las cosas ni modificar ninguna variable, sino en presentar un panorama claro y fiel de la realidad observada.

Investigación exploratoria

Esta investigación busca principalmente identificar varios aspectos del comportamiento humano tales como las motivaciones, actitudes, intenciones, creencias, gustos y preferencias. Según Hernández et al., (2014) expresa que "Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien,

si deseamos indagar sobre temas y áreas desde nuevas perspectivas". (Hernández, 2014, p.91) En otras palabras, el enfoque busca conocer un fenómeno de acuerdo con como sucedió en el contexto, utilizándola para el problema que no está claramente definido.

Tipo de investigación utilizado

En este proyecto, para el manejo de activos tecnológicos, se emplea una investigación descriptiva, que facilita la identificación y el detalle de la administración de estos activos en la compañía. Además, con esta metodología se pueden registrar los procesos de forma exacta, las herramientas empleadas y las acciones vinculadas a estos controles. Además, este tipo de estudio resulta beneficioso ya que permite detallar el funcionamiento, los procesos que incluye y la organización de la administración de activos, simplificando la recopilación de datos esenciales a través de los métodos apropiados.

Fuentes de información

Las fuentes de información se refieren a diversos orígenes de los cuales se extrae la información para desarrollar un estudio, siendo importantes para cualquier tipo de investigación o proyecto. Según Braun (2016) "las fuentes de información son los recursos de los cuales se extrae información relevante para la investigación" (p.45). Estas fuentes se clasifican en primarias, secundarias y terciarias.

Fuente de información primaria

Las fuentes de información primaria son aquellas que contienen la información original, sin alterar y sin interpretar, es la información en su estado original y que se mantiene como tal, sin cambios, en el tiempo. En este contexto, se emplean encuestas y cuestionarios diseñados específicamente para almacenar las opiniones y necesidades de los empleados respecto a las herramientas de recursos humanos, las encuestas son herramientas importantes para obtener las opiniones directas de los empleados sobre la implementación de tecnologías de recursos humanos. Además, las entrevistas con los jefes de recursos humanos y observaciones directas en el entorno

laboral son importantes para comprender las dinámicas organizativas y las necesidades reales de los empleados. (Patton, 2015, p. 67)

Tabla 3

Fuentes de información primarias

Recurso	**Descripción**
Repositorios de trabajos finales de graduación	Se examinan los estudios centrados en la administración de los activos tecnológicos de TI para obtener antecedentes y puntos de vista relevantes.
Consultas a responsables del departamento	Se realizan las entrevistas con los encargados de cada área para comprender los requisitos del sistema de control de activos a implementar.
Asesoría de experto	La empresa cuenta con opción de consultar al proveedor del servicio del módulo de activos fijos para obtener el mejor modelado del proceso.
Libros	Se utiliza como un marco referencia para la encontrar definiciones, algunos métodos y bases teóricas.

Fuente: Lazo, 2025.

Fuente de información secundaria

Las fuentes secundarias de información son aquellas en las que se interpreta, analiza o modifica de alguna forma la información de fuentes primarias, así mismo Álvaro B (2019) expresa que las fuentes secundarias "Interpreta y analizan fuentes primarias. Las fuentes secundarias son textos basados en fuentes primarias e implican generalización, análisis, síntesis, interpretación o evaluación" (p.15). Por consiguiente, la investigación se pretende realizar con apoyo de:

Tabla 4

Fuentes de información secundarias.

Recurso	**Descripción**
Normativas y estándares	Normativas ISO27001 y COBIT ITL

artículos, Libros y revistas digitales	búsqueda de herramientas y definiciones
Páginas web	Para buscar información herramientas, métodos y normas.

Fuente: Lazo, 2025.

Fuente de información terciaria

Las fuentes de información terciarias "contienen información extraída de fuentes primarias y secundarias, permitiendo guiar definiciones de los conceptos claves de la investigación. Dando énfasis a las fuentes terciarias Molina y Méndez (2019), expresan que "una fuente de información terciaria es aquella que contiene información recopilada de una fuente secundaria, contiene, por ende, y a la vez, información primaria" (p.10).

Tabla 5

Fuentes de información terciarias

Recurso	**Descripción**
Directorios y portales de investigación	Para ubicar fuentes primarias y secundarias
Normas y estándares compilados	Colecciones de la norma en bibliotecas especializadas o sitios de página web oficiales.
Páginas web	Para buscar información herramientas, métodos y normas.
Repositorios de información gubernamental	Informes y regulaciones sobre la gestión de activos de TI en sitios como el NIST e ISO

Fuente: Lazo, 2025.

Variables de investigación

Las variables de investigación según pueden ser evaluadas con un solo elemento o con varios, Freire (2019) expresa que "Las variables intervienen como causa o como efecto en el proceso investigativo. Las variables que se van a investigar quedan identificadas desde el momento en que se define el problema" (p.172). Esto nos ayuda a comprender que la investigación sin las variables no tendría una línea lógica y óptima para obtener los objetivos expuestos.

Variable conceptual

La variable conceptual según Hernández et al., (2014) indica que “Se tratan de definiciones de diccionarios o de libros especializados y cuando describen la esencia o las características de una variable, objeto o fenómeno se les denomina definiciones reales” (p.119), es decir, el autor explica la variable conceptual usado otros términos que provienen de diccionarios, libros o definiciones.

Esta variable amplia la definición de conceptos que según Freire (2019) “Definición conceptual de la variable: Básicamente, constituye una abstracción articulada en palabras conceptualmente, para facilitar su comprensión y su adecuación a los requerimientos prácticos de la investigación. Es definirla. Representa la expresión del significado que el investigador le atribuye, y con ese sentido se debe entender durante toda la investigación. También es conocida como la función nominal de la variable a medir”. (p.172)

Variable operacional

Una variable operacional según Hernández et al., (2014) son las que “constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado” (p.120), en otras palabras, según el autor esta variable describe de forma detallada como se va a medir en la práctica, especificando las herramientas e instrumentos que se utilizaran para ejecutarlo.

Variable Instrumental

Los métodos utilizados para medir y analizar las variables establecidas en la investigación se definen como variable instrumental, ya que según Rodo (2020), “La función principal de VI es detectar la presencia de una variable explicativa en el término de error” (párr.1).

Cuadro de Variables

Para este proyecto de investigación se toman en cuenta los tres tipos de variables mencionados anteriormente, ayudando a establecer el uso.

A continuación, se muestran el cuadro de variables con detalles al respecto.

Tabla 6

Variables del proyecto

Objetivo Específico	Variable	Variable Conceptual	Variable Operacional	Variable Instrumental	Instrumento de Recolección de Datos
Establecer un procedimiento para la devolución segura de activos tecnológicos	Devolución de activos	Según López A (s.f.) "Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizada el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo".	Guía de procedimiento de devolución	Guía de formulario de registro de activos, Checklist de devolución	Observación, entrevistas
Desactivación o modificación de credenciales	Gestión de accesos	"Se especifica el rol de cada usuario que deben tener únicamente acceso a los servicios de red que han sido permitidos. Se puede controlar el acceso por procesos restringidos para controlar un inicio eficaz de acuerdo con las políticas de	Procedimiento de gestión de accesos	Guía de procedimiento, Guía de listado de accesos	Cuestionarios, revisión documental

		accesos" ISO 27001 (2022).			
Desarrollar políticas de respaldo, seguridad y recuperación de datos	Respaldo de seguridad	Según Maliza S (2023) "Los respaldos de seguridad se refieren a la práctica de crear copias de seguridad de datos para prevenir la pérdida de información en caso de algún evento catastrófico".	Plan de respaldo	Veeam Backup & Replication, Guía de procedimiento de restauración de datos	Observación, entrevistas, revisión documental
Establecer una política de control de dispositivos de almacenamiento USB en las computadoras	Dispositivos USB	Según Porto y Merino (2022) "Se conoce como memoria USB. Esta es un dispositivo de pequeño tamaño que se utiliza para guardar una gran cantidad de información mediante lo que se conoce sistema Flash".	Software de control de USB	ESET Complete, Guía de informe de usuarios con permisos autorizados	Encuestas, observación
Elaborar un procedimiento de mantenimiento preventivo y correctivo para los equipos tecnológicos	Mantenimiento de equipos tecnológicos	IBM (2023) menciona que "El mantenimiento de los equipos comprende tanto el mantenimiento que se realiza regularmente, incluido el mantenimiento proactivo, como cualquier tarea de mantenimiento necesaria".	Plan de mantenimiento	Softland, Guía de informe de intervención	Observación, entrevistas, revisión documental

Documentar la topología de red de la empresa	Topología de red	IBM (2024) define la topología de red como "La forma en que los nodos y las conexiones se organizan física y lógicamente en una red".	Diagramas de topología	Dream Machine	Revisión documental, entrevistas

Elaboración propia

Instrumentos de recolección de datos

Entrevistas

El primer instrumento es las entrevistas que según Hernández C. (2014) indica que "la entrevista tiene la finalidad de mejorar el conocimiento, siendo en cierto modo un tipo de interacción conversacional con rasgos particulares que necesitan ser bien entendido, es un tipo de interacción conversacional cara a cara" (p.204).Concuerdo con el autor ya que no solo se trata de realizar preguntas a la persona encargada o quien posea conocimiento, sino también se debe pedir procesamiento y elaboración de las respuestas.

Para analizar y comprender mejor el proceso actual de la gestión de activos tecnológicos de la empresa, se utiliza la entrevista de manera estructurada utilizando una guía de entrevista, la cual cuenta con 12 preguntas de manera abierta y optando por entrevistar al encargado del departamento de TI.

Observación investigativa

Para describir mejor los propósitos esenciales del instrumento de observación cualitativa, Hernández et al., (2014) menciona lo siguiente:

- Explorar y describir ambientes, comunidades, subculturas y los aspectos de la vida social, analizando sus significados y a los actores que la generan.

- Comprender procesos, vinculaciones entre personas y sus situaciones, experiencias o circunstancias, los eventos que suceden al paso del tiempo y los patrones que se desarrollan.
- Identificar problemas sociales.
- Generar hipótesis para futuros estudios. (p.398)

Para esta investigación, y de acuerdo con lo mencionado por Hernández se debe realizar la observación para analizar directamente como se manejan los activos en la empresa y no depender solamente de la entrevista ya que se puede escribir con mayor precisión los procesos en tiempo real, identificar patrones y detectar posibles problemas.

Mediante una guía de observación se pretende comprender los procesos de la gestión de activos, así como lo indica la revista Urbano G (2016), citando a Nogales menciona que "La observación cualitativa es un proceso semiestructurado o nada estructurado de captación de información general sobre la conducta o el comportamiento de las unidades muéstrales con el fin de realizar un análisis cualitativo de la información resultante" , concuerdo con el texto anterior ya que uno de los propósitos principales de la observación es con el fin de evaluar el flujo y manejo de los activos en las áreas de la empresa donde el proceso sea involucrado, analizando el rol de los encargados de TI e identificar las debilidades y oportunidades de mejora en los procesos del control y seguridad para poder comprender el impacto de la gestión actual en la protección de los datos e incumplimiento de la normativa.

CAPITULO IV: ANÁLISIS DE RESULTADOS

En este capítulo se analizan los resultados obtenidos mediante la aplicación de dos técnicas cualitativas con una entrevista al encargado del departamento de TI y observación directa en las instalaciones permitiendo identificar debilidades en el control de activos tecnológicos con el fin de determinar la situación actual de la empresa y procesos actuales del departamento de TI, se ejecutó una entrevista a su encargado y se efectuó una observación elaborando las técnicas con una guía de entrevista y una guía de observación adjuntas en el apéndice de este documento.

Estos instrumentos de recolección de datos brindaron datos muy interesantes que a continuación, se presentan los resultados obtenidos tras la aplicación de la entrevista y la observación.

Resultados de la entrevista

El propósito de la entrevista llevada a cabo fue examinar el procedimiento de gestión de activos tecnológicos en el departamento de tecnología de la información, identificando a los encargados y su nivel de implicación en las diferentes fases, además, se examinaron elementos fundamentales como la rastreabilidad, el uso eficaz de los recursos y el nivel de automatización del proceso actual dando énfasis en el dialogo en donde se abordaron los desafíos y posibilidades de optimización en la administración de activos, además de las aspiraciones del departamento para consolidar el control y la organización de estos recursos a futuro.

Al entrevistar al encargado del departamento, se confirmó que, si existe un procedimiento informal para la administración de activos, este se centra únicamente en la adquisición de hardware, sin abarcar otros aspectos clave como el mantenimiento o la baja de equipos, según su descripción, el flujo actual del proceso incluye los siguientes pasos:

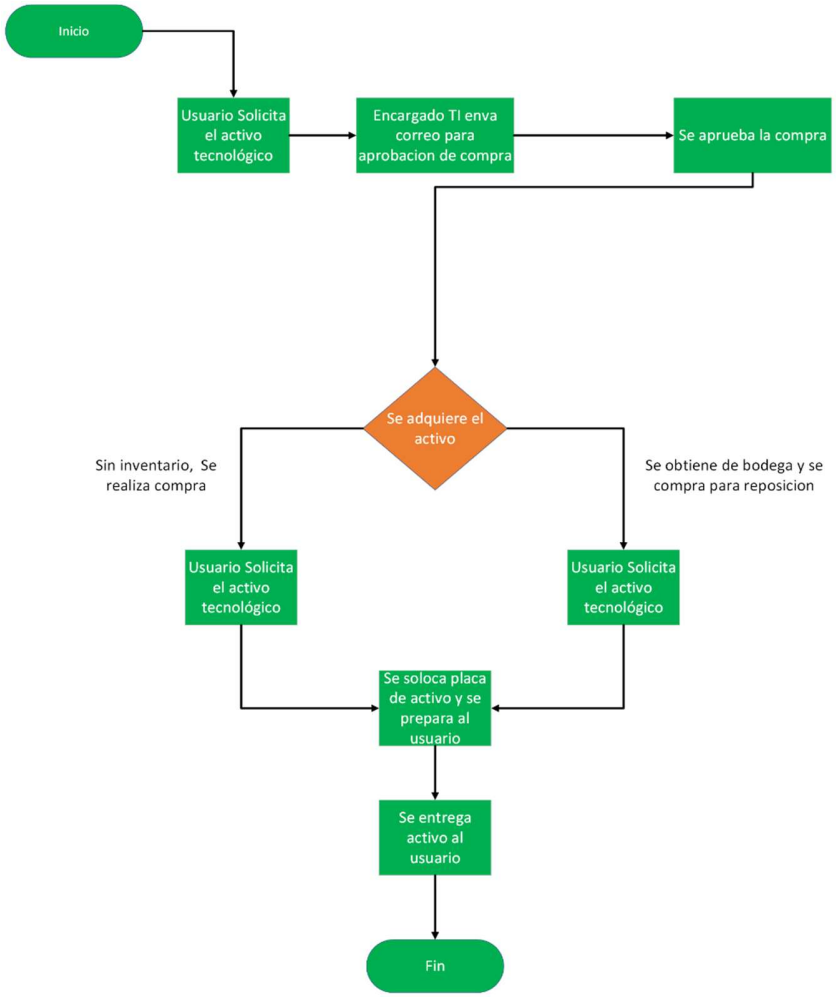
- Un usuario solicita nuevo hardware o equipo.
- Se envía a gerencia administrativa y general para su aprobación.
- Se obtiene la aprobación por parte de finanzas y gerencia.

- Se obtiene la aprobación por parte de finanzas y gerencia.
- Después de la aprobación, se selecciona la máquina y se adapta al usuario.
- Se agrega placa de consecutivo de activos, se entrega al usuario y no se registra en sistema.
- Se almacena la factura para términos de garantía o revisión de compra.

A continuación de muestra un diagrama para visualizar el proceso actual de la empresa al momento de realizar la solicitud de un activo tecnológico.

Figura 2.

Ciclo actual de activos



Elaboración propia

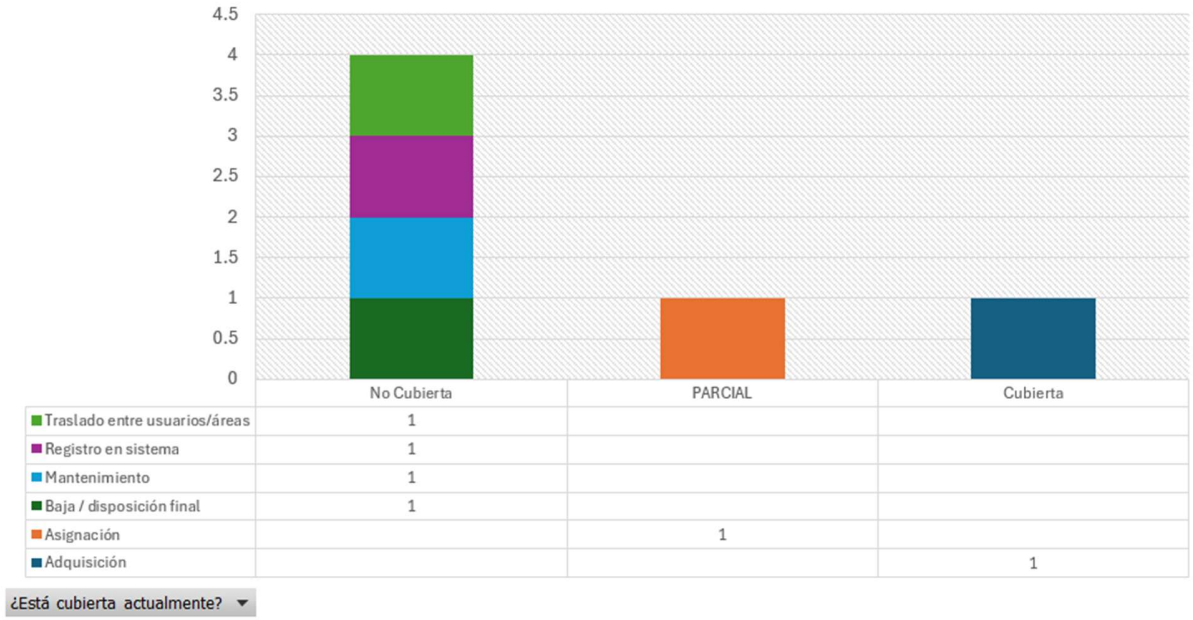
La entrevista realizada demuestra que la organización no cuenta con el procedimiento formal para el manejo de activos tecnológicos, registrándose solamente a nivel contable, pero con muchas manualidades como el cálculo de la depreciación y sin contemplar el mantenimiento, ni la vida útil de los activos, el procedimiento de adquisición tiene buena trazabilidad sin embargo no basta solo con terminar el ciclo colocándole una placa con un consecutivo, ya que esto elimina el seguimiento estructurado y control del inventario.

Tampoco existe una política clara para la recolección de activos cuando un empleado abandona la empresa, lo que ha generado perdidas por devoluciones incompletas y también las bajas de los dispositivos se envían por correo sin embargo no se realiza ninguna documentación formal, es por eso que el entrevistado hace énfasis en considerar la implementación de un sistema de control, capacitación del personal y la creación de políticas y procedimientos para establecer una cultura que distribuya la responsabilidad del control de activos entre todas las áreas y no solo de TI.

Se identificó que el procedimiento actual solo cubre parcialmente el ciclo de vida de los activos tecnológicos, en la siguiente figura se muestra un gráfico con las etapas cubiertas y no cubiertas:

Figura 3.

Gráfico de cobertura de procesos.



Elaboración propia

Es necesario señalar que la transcripción de la entrevista puede ser consultada en los apéndices de este documento.

Resultados de la observación

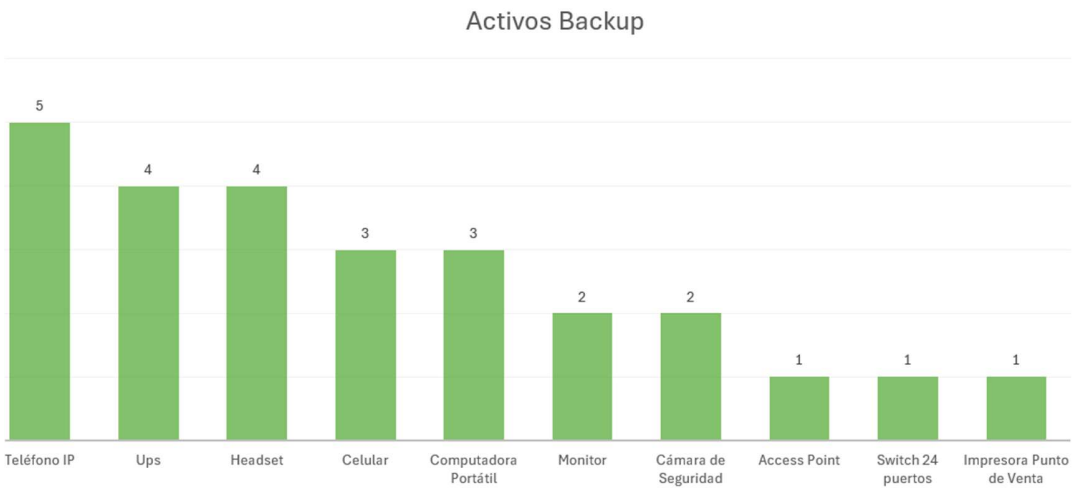
En la observación, se abordaron temas que fueron conversados en la entrevista para darle mayor detalle y complementarlos con el objetivo de profundizar el proceso de registro y manejos de los activos, en donde se confirma visiblemente la falta de controles sobre los activos de TI, donde se aprecia que existía una hoja en formato Excel que llevaban controles, sin embargo no está actualizada y no se cuenta con el inventario completo ya que muchas personas no entienden o desconocen el procedimiento de los activos.

Con la observación realizada se lograron extraer puntos importantes a considerar:

1- Se contabilizan 21 activos tecnológicos nuevos dentro del cuarto de servidores, los mismos se encuentran bien protegidos y solo el encargado de TI tiene la llave de acceso, a continuación, se muestra una gráfica para observar la cantidad por tipo de activo:

Figura 4.

activos TI.

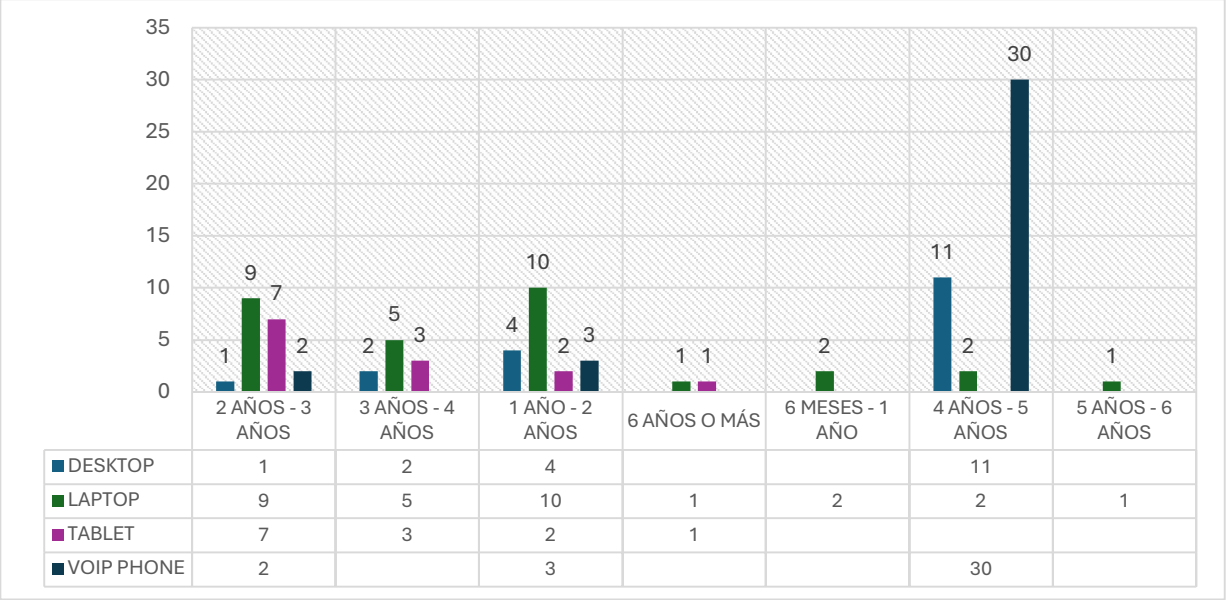


Elaboración propia

2- Al realizar la entrega de un activo, no existe documento que haga responsable al usuario que está recibiendo el equipo.
3- Se observa que hubo cambios de puestos por ascensos y los activos en estas situaciones generan problemas con el inventario al no contar con un sistema que permita hacer los traslados entre departamentos.
4- La empresa al tener como actividad comercial la producción, generan mucha materia de desecho como chatarra, una vez a la semana llega el camión a recolectarlo para su debido proceso, en este basurero se observan dos computadores de escritorio, un monitor y una UPS que fueron depositados sin control e incluso algunos tenían la placa colocada.
5- Se realiza el registro en una hoja de cálculo, pero con inventario desactualizado y contiene información incompleta, pero como el registro contable se encuentra contabilizado se logran extraer la cantidad de activos y su fecha de compra lo que servirá para realizar un inventario inicial con cada departamento, a continuación, se muestra el hallazgo sobre los activos vigentes y su periodo de compra el cual servirá para toma de decisiones de acuerdo con la vida útil de cada uno de los equipos.

Figura 5.

activos en puestos de trabajo.



	2 AÑOS - 3 AÑOS	3 AÑOS - 4 AÑOS	1 AÑO - 2 AÑOS	6 AÑOS O MÁS	6 MESES - 1 AÑO	4 AÑOS - 5 AÑOS	5 AÑOS - 6 AÑOS
DESKTOP	1	2	4			11	
LAPTOP	9	5	10	1	2	2	1
TABLET	7	3	2	1			
VOIP PHONE	2		3			30	

Elaboración propia

6- Se detectan credenciales de acceso que no son definidos mediante el perfil del puesto.
7- Se observa que algunos usuarios dejan contraseñas visibles o las comparten entre ellos.

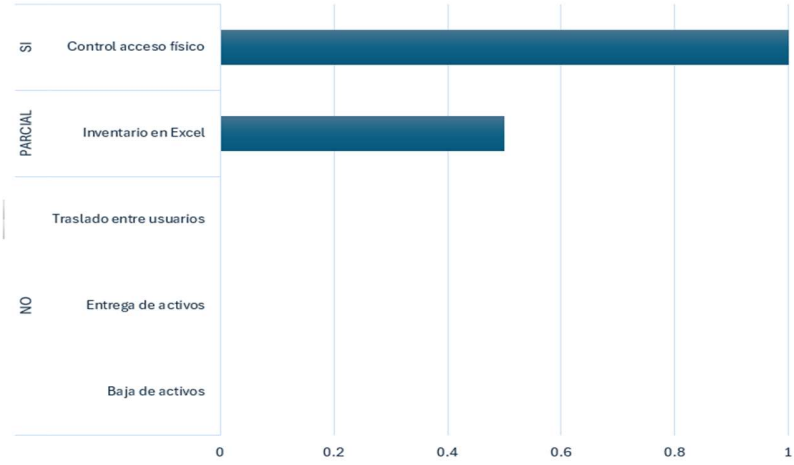
Mediante la observación realizada se logran identificar algunas oportunidades de mejora en el control de los activos, ya que la falta de documentación en la entrega de equipos, la ausencia de un sistema de traslado entre departamentos y la desprotección de los equipos de respaldo exponen a la empresa a riesgos de pérdida, robo o descontrol del inventario, comprometiendo la seguridad de la información y trazabilidad de los bienes tecnológicos.

En cuanto a las auditorias sobre los activos de TI, se comprueba que no se ejecutan de manera periódica, no se analiza el valor de los activos y tampoco se realiza una limpieza de información o datos cuando se decide retirar un activo, este proceso se ha solicitado hacer sin embargo no existe un proceso definido, dando como resultado que ThermoSolutions Group debe implementar políticas, procedimientos y herramientas formales orientadas y alineadas con la gestión de activos con los requisitos de la norma ISO/27001 para fortalecer la seguridad de la empresa.

A continuación, se muestra la gráfica donde podemos observar el nivel de cumplimiento de la documentación de los procesos actuales, donde tres de cisco procesos no se ejecutan de manera correcta, uno de forma parcial y el último si se cumple.

Figura 6.

Nivel de documentación de procesos.



Elaboración propia

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capitulo presenta las conclusiones y recomendaciones tras la investigación y desarrollo de los objetivos establecidos en este documento para la empresa Thermosolutions Group, con el fin de evidenciar el proceso actual de la gestión de activos de TI utilizando como metodología descriptiva con el fin de facilitar la identificación y detalle de la administración de los activos, obteniendo como herramienta la entrevista y método de observación para análisis de resultados del personal involucrado en los procesos.

Conclusiones

Un Procedimiento de devolución de activos tecnológicos permite establecer un control formal sobre la recuperación de los dispositivos cuando un colaborador finaliza su relación laboral, ya sea por despido o renuncia, asegurando que los dispositivos sean devueltos de buena forma, registrados correctamente y que se actualice el inventario institucional con el propósito principal en reducir pérdidas económicas, mejorar la trazabilidad de los recursos y proteger la información contenida en los equipos.

Es fundamenta contar con una política para el control de accesos y gestión de contraseñas que aplique para los empleados que dejaron de pertenecer a la organización, la gestión adecuada de credenciales es esencial para evitar accesos no autorizados a los sistemas corporativos, es por eso que esta política se enfoca en establecer un protocolo claro para la desactivación o modificación de accesos cuando un colaborador se retira, lo que garantiza la confidencialidad de la información y el cumplimiento de los controles de seguridad exigidos por la norma ISO/IEC 27001.

La información es uno de los activos más valiosos de la empresa, y al carecer de procedimientos que garanticen la información de la organización, se debe realizar el documento que defina cómo realizar respaldos periódicos y cómo actuar ante desastres tecnológicos, esta implementación asegura la disponibilidad de los datos, minimiza el tiempo de inactividad y fortalece la continuidad operativa, alineándose con los principios de protección de la norma ISO.

La empresa cuenta con un software administrado por consola que permite el bloqueo de los puertos USB sin embargo no existe una política para el uso medido de estos dispositivos, lo que es de gran importancia mediante una política establecer el bloqueo por defecto de los puertos USB y permitir las excepciones controladas para reducir el riesgo de malware y fuga de datos.

La empresa no cuera con un plan para el mantenimiento preventivo y correctivo de los activos tecnológicos, lo que deja como resultado el desconocimiento de su vida útil, incremento en costos por fallos inesperados e incidentes que pueden interrumpir la operatividad de los recursos, con un procedimiento se logra asegurar que cada intervención técnica esté documentada, programada y alineada con los estándares de seguridad establecidos por la norma ISO/IEC 27001.

La documentación de la topología física y lógica de la red es clave para la administración eficiente de la infraestructura tecnológica y gracias a la herramienta Dream Machine, la empresa puede visualizar en tiempo real los dispositivos conectados, sus ubicaciones y segmentaciones sin embargo el aprovechamiento de esta funcionalidad no cubre un buen manejo de los dispositivos de la red, sin embargo se puede implementar la política con el fin de mantener un inventario gráfico actualizado, facilitar la respuesta ante incidentes y asegurar el cumplimiento de los controles relacionados con la gestión de activos y la protección de la infraestructura.

Recomendaciones

Uno de los puntos que la empresa debería considerar es optar por la herramienta de software para la gestión de inventarios tecnológicos que permita dar trazabilidad y actualizaciones en tiempo real, sin brincarse el proceso contable de su depreciación, brindando todo tipo de actualizaciones a tiempo real para los usuarios.

La empresa debe tomar la decisión en adquirir el procedimiento devolución de activos mediante su inclusión en el reglamento interno de la empresa y capacitar al personal de recursos humanos y TI sobre su aplicación para lograr permitir mantener un control riguroso sobre los activos asignados, reducir pérdidas materiales y proteger la información contenida en los dispositivos.

Documentar un proceso integral que complete el proceso actual de la adquisición de los activos, mostrando desde la adquisición, registro, asignación, traslado, mantenimiento, baja y eliminación segura de datos, alineado con la ISO 27001.

Hay que asegurar que los equipos en bodega estén almacenados de manera correcta y segura, limitando accesos a personal no autorizado, así mismo limitar los accesos de acuerdo con los roles definidos.

Capacitar a los colaboradores de las responsabilidades en la gestión y protección de los activos, incluyendo el uso adecuado de contraseñas, entregas, traslados y devoluciones, teniendo en cuenta que todo va documentado con firmas obligatorias el momento de asignar o mover activos entre usuarios o áreas.

Cumplir con un cronograma de mantenimiento preventivo y correctivo, ejecutando controles regulares de inventario para que el procedimiento de recolección de equipos, desactivación de cuentas o accesos y limpieza de datos sea de acuerdo con la norma y cumpla con la seguridad que la empresa necesita para la protección de la información, donde el proceso sea claro para la baja de los dispositivos.

Realizar la topología de la red por departamentos, sucursales y los dispositivos conectados (servidores, switches, routers, puntos de acceso, impresoras y estaciones de trabajo), ilustrando la segmentación actual que pueda ser analizada para futuras mejoras.

En la siguiente tabla, se definen los tiempos estimados y responsables:

Procedimiento / Política	**Tiempo estimado**	**Responsables**
Devolución de activos tecnológicos	1 mes	Departamento de TI y Recursos Humanos

Procedimiento / Política	**Tiempo estimado**	**Responsables**
Gestión de accesos y contraseñas	2 meses	Departamento de TI
Respaldo y recuperación de datos	1 mes	Departamento de TI
Control de puertos USB	3 semanas	Departamento de TI
Mantenimiento de equipos tecnológicos	Inicio en el próximo trimestre	Departamento de TI y proveedores autorizados
Control de la topología de red	Revisión semestral + actualizaciones inmediatas	Departamento de TI
Asignación de activos tecnológicos	2 semanas	Departamento de TI y Recursos Humanos

CAPÍTULO VI: PROPUESTA

Introducción

Las amenazas en los recursos de información de las empresas se incrementan constantemente, debido a la necesidad e importancia de contar con los sistemas funcionando de manera operativa y eficiente, además cada vez estos recursos se vuelven más atractivos para las personas malintencionadas, con el propósito de adquirir información delicada y confidencial de los datos, esto puede abarcar desde perjudicar la reputación de la compañía hasta extraer posiblemente dinero. La tecnología progresa y con ella se presentan diversas formas de fraude o necesidades, ya sean internos o externos, por lo que es necesario tomar conciencia acerca de cómo proteger de manera integral la seguridad de la información en el ámbito empresarial.

La compañía, al administrar de manera eficiente los activos tecnológicos, previene las inversiones incorrectas o excesivas que surgen de neutralizar amenazas sin una evaluación previa, desestimar riesgos, ausencia de contramedidas, establecer controles excesivos y de un costo superior al requerido, falta de claridad en la distribución de funciones, responsabilidades sobre los activos de información, y la falta de procedimientos que aseguren una respuesta oportuna y apropiada ante cualquier incidencia.

De acuerdo con lo mencionado anteriormente, resulta crucial tener procedimientos claros y obligatorios en la organización en base al sistema de gestión, con el fin de detectar los riesgos, amenazas y vulnerabilidades a los que puedan estar sujetos los recursos de información de la entidad, para garantizar un nivel de madurez apropiado en términos de seguridad y control de los dispositivos, dando como respuesta a las brechas identificadas en el diagnóstico realizado, que evidencia debilidades en trazabilidad de activos, control de accesos, respaldo de información, mantenimiento preventivo y correctivo documentado.

Objetivos

Objetivo general

Elaborar un conjunto de acciones correctivas, preventivas y regulaciones que faciliten la eliminación de las brechas de seguridad identificadas en los procesos tecnológicos de ThermoSolutions Group S.A. y que estén vinculadas a los activos tecnológicos, implicando la implementación de políticas, procedimientos, herramientas tecnológicas y sistemas de seguimiento que garanticen la privacidad de acuerdo con los lineamiento de la norma ISO/IEC 27001:2022 para enfatizar en aspectos de amenazas, riesgos y vulnerabilidades que pongan en peligro la confidencialidad, integridad y disponibilidad de la información asegurando de forma razonable la protección de los activos tecnológicos del negocio.

Objetivos específicos

- Reducción de riesgos y fuga de datos: Al ejecutar los controles de acceso implementados, creación de copias de seguridad y normativas de uso de dispositivos, se reduce la posibilidad de que datos delicados sean presentados o suprimidos de formas no autorizadas.
- Control y trazabilidad de activos tecnológicos: La puesta en marcha del módulo de activos fijos sugerido para incorporarlo al ERP de la empresa, facilitará el registro, seguimiento y auditoría de cada activo registrado desde su compra hasta su finalización, lo que potenciará la eficiencia en sus seguimientos y controles.
- Cumplimiento conforme a la regulación que según la conformidad con la norma ISO/IEC 270001:2022 permitirá que ThermoSolutions este alineada con la ley 8968 de protección de datos personales y otras normativas.
- Optimización de procesos de mantenimiento y respaldo: Se establecerán planes de mantenimiento preventivo y políticas de respaldo que reducirán el tiempo de inactividad y los costos por fallos inesperados.
- Disminución de gastos por pérdidas o sustitución innecesaria para conseguir un inventario al día y regulado que prevendrá adquisiciones duplicadas y facilitará una planificación financiera más eficiente.

- Incremento en la administración de accesos: La automatización del proceso de desactivación de credenciales disminuirá la posibilidad de accesos no permitidos y optimizará la reacción frente a cambios en el personal.

Normativas aplicadas

Normativa	Alcance	Objetivo	Propósito	Indicadores de Progreso y Logro
Control A.8 - Gestión de activos	Todos los activos tecnológicos de la empresa	Identificar, clasificar y proteger los activos	Evitar pérdidas, fugas de información y descontrol del inventario	% de activos registrados en el sistema ERP % de activos con trazabilidad completa.
Control A.9 - Control de accesos	Usuarios con credenciales en sistemas internos	Garantizar que solo usuarios autorizados accedan a la información	Evitar accesos no autorizados tras la salida de empleados	Tiempo promedio de desactivación de credenciales N° de accesos no autorizados detectados
Control A.12 - Mantenimiento de equipos	Equipos tecnológicos (PCs, servidores, impresoras)	Asegurar la operatividad y prolongar la vida útil	Reducir fallos inesperados y costos por reparaciones	cumplimiento del cronograma de mantenimiento
Control A.13 - Protección contra software malicioso	Dispositivos con puertos USB y acceso a red	Prevenir la introducción de malware por medios extraíbles	Evitar infecciones y fugas de datos por USB	N° de dispositivos con puertos USB bloqueados cumplimiento de auditorías USB

Normativa	Alcance	Objetivo	Propósito	Indicadores de Progreso y Logro
Control A.17 - Continuidad del negocio	Sistemas críticos y bases de datos	Garantizar disponibilidad de la información ante desastres	Evitar pérdida de datos y tiempo de inactividad	% de respaldos realizados según cronograma de éxito en simulacros de recuperación.
Control A.7.1 - Inventario de componentes de red	Infraestructura de red física y lógica	Documentar y controlar la topología de red	Mejorar respuesta ante incidentes y segmentación segura	Tiempo de respuesta ante fallos de red

Procedimiento de devolución de activos

El documento “Procedimiento de Seguridad de Activos de Cómputo”, adjunto como apéndice C, tiene como propósito establecer un función principal contar con un proceso formal para la devolución de activos tecnológicos en ThermoSolutions Group S.A., garantizando la protección de la información y la trazabilidad de los dispositivos al finalizar la relación laboral de un colaborador. El procedimiento responde a la necesidad de minimizar riesgos que puedan haber ante una mala gestión de los activos tecnológicos, en el uso indebido de recursos y la fuga de información, además cumple con los controles establecidos por la norma ISO/IEC 27001, aplicándose a todos los colaboradores que hayan recibido activos tecnológicos como parte de sus funciones, y contempla la devolución obligatoria de estos recursos al momento de su salida de la organización, ya sea por renuncia, despido o finalización de contrato.

Se busca asegurar la recuperación física de los equipos, la actualización del inventario institucional y la eliminación de accesos a sistemas críticos, contribuyendo así a la seguridad operativa y administrativa de la empresa dentro de los controles normativos aplicados, y con énfasis en las norma en los siguientes controles: el control 5.9 sobre inventario de activos, que exige mantener un registro actualizado y documentado; el control 5.11 sobre retiro de activos, que establece la necesidad de evidencia formal de devolución; el control 6.1 sobre responsabilidades del personal, que asigna al usuario la obligación de devolver los activos en condiciones adecuadas; y el control 8.1, que exige la revocación de accesos a redes al devolver dispositivos con credenciales activas.

El procedimiento está elaborado por cinco etapas fundamentales iniciando con la notificación de salida del colaborador por parte de recursos humanos con al menos 48 horas de anticipación; revisión del inventario y preparación de documentos por parte del área de TI; entrega y verificación física de los activos; firma de la constancia de devolución y actualización del sistema; por último, validación final del proceso por parte de recursos humanos para proceder con el cierre administrativo.

Como parte de las evidencias que se requieren, se incluye la notificación formal de salida, el inventario de activos asignados, la constancia de devolución firmada por ambas partes, y el informe final de cierre del proceso emitido por el área de TI, pero en casos donde el colaborador se encuentre fuera de la organización, se contempla una logística especial para la devolución, incluyendo envíos a puntos autorizados y diagnósticos remotos.

El plan propuesto representa un enfoque sistemático y alineado con buenas prácticas internacionales para la gestión segura de activos tecnológicos. Asegura la trazabilidad, la protección de la información y el cumplimiento normativo, reduciendo riesgos operativos y fortaleciendo la seguridad de los activos tecnológicos en la organización.

Política de control de accesos y contraseñas

El documento “Política de control de accesos y gestión de contraseñas”, que se adjunta como apéndice D, tiene como función principal, establecer un procedimiento operativo que cumpla con la gestión segura de credenciales de acceso en ThermoSolutions Group S.A., en especial durante el proceso de finalización de contrato laboral, respondiendo a la necesidad de proteger los dispositivos tecnológicos de la organización frente a accesos no autorizados para garantizar la integridad, confidencialidad y disponibilidad de la información.

La política está basada en los principios de la norma ISO/IEC 27001, y establece controles específicos para la desactivación o modificación inmediata de todas las credenciales asociadas a colaboradores que finalizan su relación laboral, ya sea por renuncia, despido o término de contrato, además es importante destacar que en esta solución se contemplan la gestión de accesos a plataformas internas, servicios en la nube, VPN, ERP, correos electrónicos, tokens y sistemas con autenticación multifactor (2FA).

El procedimiento aplica de forma obligatoria a todos los colaboradores con accesos a sistemas informáticos o accesos digitales de la organización para buscar prevenir accesos no autorizados posteriores a la salida del personal, evitar la fuga de información y cumplir con los controles

A.9.2.1, A.9.2.6 y A.9.4.1 de la norma ISO/IEC 27001, los cuales regulan el ciclo de vida de las credenciales de usuario, la revocación de derechos de acceso y la restricción basada en el principio de necesidad de conocimiento.

Se estructura en cinco etapas, iniciando con notificación de salida del colaborador por parte del departamento de recursos humanos; seguidamente se debe realizar un levantamiento de accesos utilizados por el colaborador; desactivación o modificación de credenciales por parte del área de TI; registro del proceso en el sistema de control interno; y generación del informe de cierre del procedimiento, validado por recursos rumanos, además cada etapa cuenta con responsables definidos y documentación de respaldo.

Como parte de las evidencias requeridas, de elaboran los documentos de notificación formal de salida, el formulario de registro de desactivación de credenciales, la bitácora de acciones realizadas y el informe de cierre del procedimiento con el fin de fortalecer la seguridad de la infraestructura tecnológica, reducir riesgos operativos y promover una cultura organizacional basada en la responsabilidad y la prevención. La coordinación efectiva entre recursos humanos, el área de TI y las jefaturas de departamento es clave para garantizar la continuidad operativa y la protección de los activos digitales de la empresa.

Seguridad de la información

El documento “Seguridad de la Información”, adjunto como apéndice E, se establece con el objetivo establecer un procedimiento formal para la protección de los datos críticos de ThermoSolutions Group S.A., mediante la implementación de respaldos periódicos y un plan de recuperación ante desastres, además con el procedimiento pretende garantizar la disponibilidad, integridad y recuperación de la información ante incidentes como fallos técnicos, errores humanos, ataques cibernéticos o desastres naturales, alineándose con los controles de la norma ISO/IEC 27001:2022.

El procedimiento establece directrices claras para la realización de copias de seguridad de bases de datos, servidores y archivos críticos, así como la definición de roles, frecuencias de respaldo,

medios de almacenamiento y procesos de restauración además, se contempla la verificación periódica de la integridad de los respaldos y la conservación de versiones históricas, asegurando trazabilidad y cumplimiento normativo.

El procedimiento se compone en dos componentes principales:

Componente	Descripción
Copias de seguridad	Se realizan respaldos periódicos de la información crítica: • **Diarios** para bases de datos. • **Semanales** para carpetas compartidas. • **Mensuales** para servidores completos. Los respaldos se almacenan en la nube con autenticación segura, conservando al menos tres versiones históricas. Su integridad se verifica mensualmente y se documenta detalladamente.
Plan de recuperación ante desastres	Define cómo restaurar la funcionalidad de los sistemas tras un incidente. Incluye: • Objetivos y alcance del plan. • Listado de sistemas prioritarios. • Procedimientos de restauración paso a paso. • Roles y responsabilidades asignadas. • Contactos clave internos y externos. El plan debe actualizarse anualmente o tras cambios en la infraestructura.

El procedimiento propuesto representa un enfoque integral para la gestión de la seguridad de la información, asegurando la continuidad operativa de ThermoSolutions Group S.A. y fortaleciendo la seguridad frente a amenazas tecnológicas y operativas.

Control de puertos USB

El documento “Política de Control de Puertos USB” la cual se encuentra adjunto como Anexo F, y se representa como un conjunto de directrices para prevenir riesgos de seguridad asociados al uso no autorizado de dispositivos de almacenamiento extraíbles en ThermoSolutions Group S.A., para responder a la posible amenaza de infiltración de software malicioso o fuga de información sensible a través de estos dispositivos de almacenamiento USB.

El procedimiento establece el bloqueo por defecto de todos los puertos USB en equipos conectados a la red corporativa que son entregados a los usuarios finales por primera vez, permitiendo únicamente su habilitación mediante solicitud formal y justificada, además esta medida busca proteger la integridad, confidencialidad y disponibilidad de los activos de información, así como fomentar una cultura organizacional basada en la prevención y el uso responsable de los recursos tecnológicos.

El alcance de esta política es obligatorio para todos los dispositivos de cómputo de la organización, incluyendo computadoras de escritorio, portátiles, estaciones de trabajo y cualquier otro equipo conectado a la red. Aplica a todo el personal, sin distinción de cargo o tipo de contrato, incluyendo consultores y contratistas.

La implementación del procedimiento se compone en cuatro etapas iniciando con un bloqueo inicial de puertos USB mediante la administración de la consola ESET, además de una solicitud formal de excepciones por parte de jefaturas, un registro en una bitácora centralizada de excepciones autorizadas; y auditorías periódicas para verificar el cumplimiento de la política, estas excepciones se otorgan únicamente para casos justificados, como actualizaciones de firmware o procesos de impresión especializada, y deben ser aprobadas por el jefe inmediato y el área de TI.

Como parte de las evidencias requeridas, se incluyen: el registro de excepciones de puertos USB, el registro de configuración de bloqueo, la bitácora de excepciones autorizadas y el informe de auditoría. Estos documentos permiten mantener trazabilidad, facilitar auditorías y asegurar que las excepciones se gestionen de forma controlada y documentada, la cual representa una medida preventiva clave para reducir la superficie de ataque en la infraestructura tecnológica de la

organización, reforzando el cumplimiento normativo, mejorando la administración de TI y la protección de los activos digitales frente a amenazas internas y externas.

Procedimiento de mantenimiento de equipos de computo

El documento “Procedimiento de Mantenimiento de Equipos Tecnológicos” se encuentra adjunto como apéndice G y tiene como función principal establecer un protocolo estructurado para la ejecución de mantenimientos preventivos y correctivos en los activos tecnológicos de ThermoSolutions Group S.A., buscando garantizar la disponibilidad, funcionalidad y seguridad de los equipos y alineándose con los controles de la norma ISO/IEC 27001, particularmente en lo referente a la gestión de activos, protección contra fallos y administración de cambios.

La normativa está fundamentada en los controles 5.9 de inventario de activos, 8.14 contra la protección de fallos y 8.32 en gestión de modificaciones, los cuales obligan a mantener un inventario actualizado, ejecutar acciones preventivas y documentar toda intervención técnica para cumplir con extender la vida útil de los equipos, mejorar la planificación de recursos técnicos y asegurar la trazabilidad de las acciones realizadas.

El procedimiento se divide en dos componentes principales:

Componente	Descripción
Mantenimiento preventivo	Se realiza de forma periódica para asegurar el buen estado de los equipos: • **Cada 6 meses** para computadoras e impresoras. • **Cada 3 meses** para servidores. Incluye limpieza interna, verificación de ventiladores y temperatura, actualización de software, revisión de cableado y registro de actividades en el sistema de gestión de activos.
Mantenimiento correctivo	Se ejecuta ante fallas reportadas por los usuarios. Puede realizarse internamente o con proveedores externos. Cada intervención debe documentarse con fecha, tipo de falla, solución aplicada y técnico responsable. Se registra en el módulo de activos fijos y debe estar disponible para auditorías.

Estos documentos permiten demostrar cumplimiento, facilitar auditorías y tomar decisiones informadas sobre la gestión de activos tecnológicos.

Control de la topología de red bajo ISO 27001

El documento “Control de la Topología de Red bajo ISO 27001”, se encuentra adjunto como apéndice H, el cual tiene como punto principal establecer una política transparente para la administración y mantenimiento de la topología de red física y lógica en la organización, además busca asegurar la integridad, disponibilidad y confidencialidad de la infraestructura de TI mediante una documentación detallada y controlada de todos los componentes de red activos.

El procedimiento aplica a todos los dispositivos y enlaces de red que se encuentra conectados a la red y que son parte fundamental para el servicio o el buen funcionamiento entre las conexiones, incluyendo routers, switches, firewalls, servidores, estaciones de trabajo, puntos de acceso inalámbrico y conexiones externas como VPNs y enlaces con las tres sucursales fuera de las oficinas centrales, fundamentándolo en los controles 7.1 y 8.9 de la norma ISO/IEC 27001, que exigen la identificación de activos y la implementación de medidas para restringir accesos no autorizados a la infraestructura.

La responsabilidad principal recae en el departamento de tecnologías de la información, encargado de documentar y mantener los diagramas de red. El jefe de TI supervisa, autoriza cambios y garantiza su almacenamiento seguro con control de versiones. Se establece que los diagramas deben revisarse al menos cada seis meses o tras cualquier modificación significativa.

El procedimiento distingue entre dos tipos de topología:

Tipo de Topología	**Descripción**

Topología Lógica	Representa la estructura de comunicación de la red, incluyendo subredes, VLANs, rutas y políticas de tráfico. En ThermoSolutions, la red lógica está segmentada por VLANs (como VLAN_USER, VLAN_SECURITY, VLAN_VOIP), con una arquitectura centralizada desde la sede en Santa Ana y conexiones VPN hacia sucursales. Esta segmentación mejora la seguridad, el rendimiento y la administración del tráfico.
Topología Física	Muestra la disposición y conexión física de los dispositivos de red (switches, routers, access points, etc.). Cada departamento cuenta con su propio switch, lo que mejora la segmentación y tiempos de respuesta. Se identifican riesgos físicos como gabinetes abiertos, que deben corregirse para cumplir con los controles de seguridad. El firewall permite visualizar en tiempo real la estructura física y el estado de los dispositivos conectados.

El procedimiento propuesto fortalece la administración de la infraestructura de red, mejora la capacidad de respuesta ante incidentes, y asegura el cumplimiento con los estándares de seguridad de la información establecidos por la norma ISO/IEC 27001.

REFERENCIAS

Ático, G. (2024, 25 noviembre). Fuentes de información: Qué son, cuántos tipos existen y ejemplos. Grupo Atico34. https://protecciondatos-lopd.com/empresas/fuentes-informacion/

Calle Mollo, S. E. (2023). Diseños de investigación cualitativa y cuantitativa. Ciencia Latina Revista Científica Multidisciplinar, 7(4), 1865-1879. https://doi.org/10.37811/cl_rcm.v7i4.7016

Córdoba-Mercado, M. M., de Lima, C. M., & Pérez-Córdoba, A. L. (2025). Grounded Theory constructivista: investigación sobre prácticas con tecnologías digitales en educación superior. Educación Y Educadores, 26(3), e2633. https://doi.org/10.5294/edu.2023.26.3.3

Cruz-Adame, J. (2021). ACTIVOS FIJOS. Revista Científica Saberes 5.0, 1(1), 103–110. Recuperado a partir de https://revistas.saberescincopuntocero.com/index.php/rcs50/article/view/141

De Admin, V. T. L. E. (2020, 22 septiembre). ITIL 4: PRÁCTICAS DE GESTIÓN DE ITIL: GESTIÓN DE ACTIVOS DE TI. Interpolados. https://interpolados.wordpress.com/2020/09/22/itil-4-practicas-de-gestion-de-itil-gestion-de-activos-de-ti/

Edwards, M. (s/f). ISO 27001:2013 – annex A.8: Asset management | ISMS.Online. Recuperado de https://www.isms.online/iso-27001/annex-a-8-asset-management/

Herrera Pereda, E. C. (2021). Implementación de la norma ISO/IEC 27001 para la mejora de la seguridad de la información en la empresa Corporación Suyo S.A.C., Lima, 2021.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security Management Systems – Requirements. ISO. Disponible en https://www.iso.org/standard/82875.html

Iso/iec 27001:2022. (2022). ISO. https://www.iso.org/standard/27001

Kempwad, A. (2024, junio 4). COBIT BAI09.02 - manage critical assets. ITSM Docs - ITSM Documents & Templates. https://www.itsm-docs.com/blogs/cobit-framework/cobit-bai09-02-manage-critical-assets

López, A. (s. f.). Anexo 8. https://www.iso27000.es/iso27002_8.html

Marisol, M. S. J. (2023, 1 septiembre). Sistema de respaldo de datos utilizando cloud computing para el mejoramiento de la seguridad de la plataforma virtual moodle en la Unidad Educativa del Milenio Intercultural Bilingüe “Chibuleo”. https://repositorio.uta.edu.ec/items/31bab8a9-269b-4bc6-9905-90350c506fdf

Martínez, V. (2024, 17 julio). Cómo auditar la gestión de activos de TI. https://www.auditool.org/blog/auditoria-de-ti/como-auditar-la-gestion-de-activos-de-ti

María, A. L. E. (2021). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia Et Technica, 1(47), 334–339. https://doi.org/10.22517/23447214.1177

Norma ISO 27001. (s.f.). A.8 Gestión de activos en ISO 27001. Obtenido de https://www.normaiso27001.es/a8-gestion-de-activos/

Pila Toalombo, C. M. (2023). Análisis de riesgos para la implementación de la norma ISO 27001 en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Porto, J. P., & Merino, M. (2022, 28 abril). USB - Qué es, clasificación, definición y concepto. Definición.de. https://definicion.de/usb/

¿Qué es la gestión del ciclo de vida de los activos? (2024, enero 16). Ibm.com. https://www.ibm.com/mx-es/topics/asset-lifecycle-management

¿Qué es la Topología de red? (2024, octubre 24). Ibm.com. https://www.ibm.com/mx-es/topics/network-topology

Rodó, P (2020). *Estimación con variables instrumentales (VI)* web: economipedia.com. Recuperado de: https://economipedia.com/definiciones/estimacion-con-variables-instrumentales-vi.html

Rojas-Gutiérrez, W. J. . (2022). La relevancia de la investigación cualitativa. Studium Veritatis, 20(26), 79–97. https://doi.org/10.35626/sv.26.2022.353

Romero et al. (2023). Método mixto de investigación: Cuantitativo y cualitativo. En Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú eBooks. https://doi.org/10.35622/inudi.b.105

Saint Leo University. (s.f.). ¿Qué es la arquitectura de seguridad informática y por qué es importante la arquitectura de seguridad?

Santolaria, D. (s. f.). ISOWin. https://isowin.org/blog/activos-ISO-27001/

Software de diagramación y creación de diagramas de flujo. (s/f). Microsoft.com. Recuperado el 28 de enero de 2025, de https://www.microsoft.com/es-es/microsoft-365/visio/flowchart-software

Suscriptor. (2023, 14 junio). Gestión de activos según la ISO 27002. Software ISO. https://www.isotools.us/2023/02/09/gestion-de-activos-segun-la-iso-27002/

Tique Rodríguez, J. R. (2021). Modelo de seguridad de la información basado en la norma ISO/IEC 27001 para mejorar la gestión en una empresa del sector salud.

Torres, C. (2020). Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A. (pp. 1-61).

Valencia Estacio, E. C. (2023). Modelo de seguridad de la información basado en la norma ISO/IEC 27001 para la gestión de riesgos en la empresa Cooperativa de Ahorro y Crédito Parroquia San Lorenzo, Sullana, 2023.

Valle, A., Manrique, L., & Revilla, D. (2022, 1 marzo). La Investigación descriptiva con enfoque cualitativo en educación. https://repositorio.pucp.edu.pe/items/b5d6a4d5-9f3f-4e26-89da-1531725f3931

Vargas, A. M. C., & Ollarves, J. J. T. (2020). Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI. INNOVA Research Journal, 5(3.2), 196-213. https://doi.org/10.33890/innova.v5.n3.2.2020.1608

Veeam: Data portability and resilience. (s/f). Veeam Software. Recuperado de https://www.veeam.com/

Victor, H. N. W. (2021). La administración de los activos fijos y la gestión de la empresa Unique S.A., Lima – 2020. https://hdl.handle.net/20.500.12952/6351

Watkins, S. (2022). ISO/IEC 27001:2022 - An introduction to information security and the ISMS standard. New York. Obtenido de https://www.google.com.ec/books/edition/ISO_IEC_27001_2022_An_introductio

APÉNDICE

APÉNDICE A Guía de entrevista

Organización: ThermoSolutions

Nombre del Entrevistado:

Cargo: Encargado del departamento de TI

Preguntas:

1- ¿Actualmente la organización cuenta con un procedimiento para el registro y control de activos? Indique como es el proceso actual.
2- ¿Quiénes son los responsables para la gestión y manejo de los activos?
3- ¿Existe alguna medida para prevenir la perdida, robo o mal manejo de los dispositivos tecnológicos?
4- ¿Existe un plan de mantenimiento preventivo y correctivo para los activos tecnológicos?
5- ¿Se actualizan los softwares de los equipos? En caso de responder si, como es el proceso.
6- ¿Qué mejoras considera necesarias para optimizar el control de los activos tecnológicos?
7- ¿Cómo manejan los activos cuando un empleado deja la empresa o cambia de puesto?
8- ¿Qué mejoras han identificado en el proceso actual para la gestión de los activos?
9- ¿Cómo considera usted que la empresa podría fortalecer la protección y control de los activos?
10- ¿Actualmente como identifica un dispositivo en la red y como está estructurada la topología?
11- ¿Se documentan los cambios, transferencias o bajas de los activos dentro de la empresa?
12- ¿Cómo se realiza el control de dispositivos de almacenamiento externo con conexiones por medio de USB?

APÉNDICE B Guía de observación

Nombre de la Empresa: ThermoSolutions

Actividad de la Empresa: Productora y comercializadora de calentadores domésticos, industriales y comerciales.

OBJETIVO: Observar y evaluar las actividades relacionadas con el proyecto de gestión segura de activos tecnológicos y control de accesos.

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
1	¿Se observa un registro formal de los activos tecnológicos?				
2	¿Dónde y cómo se almacenan los activos tecnológicos? (Ubicación, medidas de seguridad)				
3	¿Se documentan los cambios de activos entre empleados o áreas?				
4	¿Cómo se asignan los activos a los empleados? (Procedimiento, registro, firma de entrega)				
5	¿Qué sucede con los activos cuando dejan de ser utilizados o son dados de baja?				

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
6	¿Existen medidas de seguridad para prevenir el acceso no autorizado a los equipos?				
7	¿Se detectan prácticas que pongan en riesgo la seguridad de la información en los activos tecnológicos?				
8	¿Se observa algún procedimiento de mantenimiento preventivo o correctivo?				
9	¿Cómo manejan los empleados los activos tecnológicos?				
10	¿Se observa alguna práctica de respaldo de datos en los activos tecnológicos?				
11	¿Se evidencian prácticas alineadas con normas de seguridad como ISO 27001?				

APÉNDICE C Procedimiento de devolución de activos

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROCEDIMIENTO DE DEVOLUCIÓN DE ACTIVOS

JOSEPH LAZO BADILLA

JUNIO, 2025

INTRODUCCIÓN

En toda organización la entrega de recursos tecnológicos a los empleados es una práctica fundamental para ejercer las tareas o funciones del día a día, pero cuando se trata de la devolución regulada de estos recursos al concluir la relación de trabajo es un aspecto crucial en la administración de la seguridad de la información y la salvaguarda de los dispositivos tecnológicos, la ausencia de procedimientos formales en esta fase puede originar riesgos relacionados con la pérdida de dispositivos, uso inapropiado, fuga de información.

Con el fin de mitigar estos riesgos de devolución de los activos tecnológicos, se establece el presente procedimiento, el cual tiene como objetivo principal asegurar que todos los activos tecnológicos asignados a un colaborador sean devueltos de forma ordenada, verificada y registrada, al momento de su salida de la empresa, ya sea por renuncia, despido o término de contrato, además esta acción permite no solo la recuperación física de los equipos, sino también la actualización precisa del inventario en el sistema, garantizando trazabilidad, control y reducción de posibles brechas de seguridad.

Además de la devolución física de los activos, se debe incluir el seguimiento y entrega del inventario actualizado en donde el responsable del área de TI debe verificar que todos los activos asignados al colaborador estén registrados en el sistema, validar su estado, y completar el formulario de entrega de inventario, además este documento debe ser firmado por el colaborador y archivado junto con la constancia de devolución, asegurando así una trazabilidad completa del proceso.

Este procedimiento debe ser aplicado en coordinación con el departamento de Recursos Humanos, quien notificará la salida del colaborador y coordinará la entrega formal de los activos e inventario. La documentación generada debe ser almacenada en el sistema ERP y respaldada digitalmente para fines de auditoría y control interno.

Objetivo

Debe existir una política clara y formal que este documentada para asegurar que todos los activos tecnológicos asignados a empleado sean regresados o devueltos de forma controlada y se pueda verificar al momento de la salida de la empresa para garantizar la protección de los activos de TI, actualizar el inventario en el módulo del sistema y reducir los riesgos relacionados con la pérdida o uso indebido de los dispositivos, logrando cumplir con los controles establecidos por la norma ISO/IEC 27001 en el apartado de control y seguimiento de activos.

El control busca reducir los riesgos en:

- Perdida de dispositivos que pertenecen a la organización.
- Fuga de información confidencial o acceso no autorizado después de la salida de un empleado.
- Inconsistencias en el inventario de activos tecnológicos.
- Responsabilidad legal y administrativa por activos que no son devueltos.

Alcance

Este procedimiento es aplicable para todos los colaboradores de la organización, de manera obligatoria que hayan recibido activos tecnológicos para el cumplimiento de sus funciones y que deberán devolverlos cuando este finaliza su relación laboral garantizando la trazabilidad y actualización del inventario de la organización.

El procedimiento pretende garantizar un inventario actualizado con trazabilidad, seguridad de la información, reduciendo los riesgos de pérdida o mal uso de los activos, en cumplimiento con la norma ISO/IEC 27001.

El cumplimiento de este procedimiento permitirá cumplir con:

- Evitar la permanencia de activos fuera de la institución.
- Proteger la información que esta almacenada en dispositivos móviles y portátiles.

- Lograr mantener el inventario actualizado con evidencia documentada.
- Cumplir con las auditorías internas y externas relacionadas con la gestión de los activos y seguridad de la información.
- Contribuir con la reducción de riesgos operativos, financieros y perdidas asociadas a los equipos.

Definiciones

- **Activo tecnológico:** Todo recurso informático asignado a un colaborador para el desempeño de sus funciones, incluyendo computadoras, laptops, celulares, tabletas, periféricos, dispositivos de red, tokens, licencias de software y cualquier equipo electrónico relacionado.
- **Inventario de activos:** Registro formal y actualizado que contiene la lista de los activos tecnológicos de la organización, con detalles como número de serie, responsable asignado, estado, ubicación y fecha de entrega.
- **Devolución de activos:** Proceso mediante el cual un colaborador que deja de laborar en la organización, o que ya no requiere un activo específico, entrega los recursos tecnológicos asignados a su cargo al departamento correspondiente.
- **Constancia de devolución:** Documento oficial firmado por el colaborador y el área de TI que certifica la entrega de los activos asignados, incluyendo el estado en que se encuentran.
- **Colaborador saliente:** Persona que finaliza su relación laboral con la organización, ya sea por renuncia, despido, finalización de contrato o cualquier otro motivo válido.
- **Evidencia documental:** Archivos físicos o digitales que respaldan cada etapa del procedimiento (notificación, inventario, constancia e informe final).

Abreviaturas

- **TI:** Tecnologías de la Información.
- **RH:** Recursos Humanos.
- **ISO/IEC 27001:** Norma internacional para la gestión de la seguridad de la información.
- **ERP:** Sistema de Planificación de Recursos Empresariales.

- **ID:** Identificador único de un activo tecnológico dentro del inventario.

Normativa

El procedimiento se fundamenta en la norma ISO/IEC:27001 en los siguientes controles:

- Control 5.9 Inventario de activos de información hace énfasis en que se debe mantener un inventario preciso, actualizado y documentado de todos los activos tecnológicos, identificando claramente su responsable, ubicación, estado y uso, la devolución de activos permite cerrar el ciclo de vida del recurso en manos del usuario saliente.
- Control 5.11 Retiro de activos el cual especifica que todos los activos deben devolverse a la organización cuando ya no se requieran o al terminar la relación laboral con el colaborador y debe existir evidencia formal de la devolución y verificación del estado del activo.
- Control 6.1 Responsabilidades y deberes del personal establece que los usuarios son responsables del uso seguro y adecuado de los activos asignados, incluyendo su devolución oportuna en las condiciones acordadas.
- Control 8.1 Seguridad de los servicios de red, este control, aunque no es específico a devoluciones, se relaciona en casos donde activos devueltos tengan credenciales o configuraciones que permitan acceso a sistemas de red, la devolución debe ir acompañada de la revocación de accesos.

Matriz de roles

- El departamento de tecnologías de la información es quien debe recibir los equipos devueltos por el colaborador, revisar su estado físico y funcional, y asegurarse de que todo quede debidamente registrado y actualizado en el inventario del sistema
- En el departamento de recursos humanos, tiene la responsabilidad de coordinar el proceso de salida del colaborador, esto incluye informar con antelación al equipo de TI

sobre la salida para que puedan preparar el proceso de devolución y validación de los activos tecnológicos.

- Cada colaborador debe entregar todos los activos tecnológicos que le fueron asignados durante su tiempo de trabajo, como computadoras, celulares, cargadores, tokens, entre otros. Esta entrega debe hacerse de manera ordenada, en el momento establecido, y en buenas condiciones, siempre que sea posible.

Matriz de responsabilidades entrega de activos

Actividad	**Ejecuta**	**Aprueba**	**Supervisa**	**Informado**
Solicitud de asignación de activos	RRHH	Gerencia	Auditoría Interna	TI
Preparación de activos y documentación	TI	Jefatura TI	RRHH	Auditoría
Entrega física de activos al colaborador	TI, Colaborador	RRHH	Auditoría	Gerencia
Registro de asignación en el sistema ERP	TI	Jefatura TI	RRHH	Auditoría
Validación final y firma de recepción	Colaborador, RRHH	Gerencia	Auditoría	TI

Matriz de responsabilidades devolución de activos

Actividad	Ejecuta	Aprueba	Supervisa	Informado
Notificación de salida del colaborador	RRHH	Gerencia	Auditoría Interna	TI
Preparación de inventario y documentos	TI	Jefatura TI	RRHH	Auditoría
Entrega y verificación de activos	TI Colaborador	RRHH	Auditoría	Gerencia
Actualización del inventario en ERP	TI	Jefatura TI	RRHH	Auditoría
Validación final y cierre	RRHH	Gerencia	Auditoría	TI

Recomendaciones

Para la implementación de este procedimiento, se recomiendan cinco etapas fundamentales las cuales se dividen de la siguiente manera:

Etapa	Descripción	Responsable
N°1: Notificación de salida	Recursos Humanos informa formalmente al área de TI sobre la salida del colaborador con al menos 48 horas de anticipación.	Recursos Humanos
N°2: Revisión de inventario y preparación	El área de TI consulta el inventario de activos asignados y prepara el documento de devolución correspondiente.	Departamento de TI
N°3: Entrega y verificación de activos	El colaborador entrega los activos. El personal de TI inspecciona el estado físico y actualiza la información en el sistema de activos fijos.	Colaborador / Departamento de TI
N°4: Firma de constancia y actualización	Ambas partes firman la constancia de devolución y se actualiza el	Colaborador / Departamento de TI

	inventario. Se guarda una copia del documento como respaldo.	
N°5: Validación final del proceso	Recursos Humanos confirma que el procedimiento de devolución fue completado para continuar con el cierre administrativo o liquidación del colaborador.	Recursos Humanos

Para documentar y revisar el cumplimiento de estos procedimientos se debe generar y conservar las siguientes evidencias:

- **Notificación de salida del colaborador:** Documento emitido por el departamento de recursos humanos que notifica oficialmente al departamento de Tecnología de la Información acerca de la salida de un empleado, y comienza el proceso de recuperación de activos y desactivación de accesos para facilitar la programación de la devolución de equipos y la preparación de los documentos requeridos.
- **Inventario de activos asignados:** Es un inventario actualizado que especifica todos los dispositivos tecnológicos proporcionados al empleado, ya sea para uso cotidiano o temporal y actúa como orientación para determinar qué equipos deben ser restituidos, bajo qué circunstancias se entregaron y si falta algún elemento, además, evita pérdidas o irregularidades.
- **Constancia de devolución de activos:** Formulario que se firma en el momento en que el colaborador entrega los equipos, es la evidencia formal de que la devolución se realizó, garantiza la responsabilidad de ambas partes y deja registro de los activos devueltos, su estado físico y la conformidad de entrega, si durante la devolución se detectan con daños, el departamento de TI deberá documentar el estado del equipo en la constancia de la devolución, además debe realizar la evaluación técnica para determinar si el daño es por mal uso o desgaste natura. En caso de negligencia comprobada, la empresa podrá aplicar las políticas internas correspondientes ya sea con la reposición del equipo, deducción proporcional o acciones administrativas de acuerdo con el reglamento interno de la compañía.

En el caso de los colaboradores que desempeñan sus funciones fuera de la organización, el proceso de devolución se coordina mediante una logística previamente definida entre el departamento de TI y recursos humanos, esto podría incluir él envió de los activos a puntos autorizados, mensajería y algunas revisiones de diagnósticos de forma remota.

- **Informe final de cierre de proceso:** Es el informe que emite el departamento de Tecnología de la Información al concluir todo el proceso, certificando que el proceso de devolución se ha finalizado adecuadamente y confirmando que no existe ningún compromiso con el colaborador destacado en relación con los activos tecnológico.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción	Elaborado por:

NOTIFICACIÓN DE SALIDA DEL COLABORADOR

ThermoSolutions Group S.A

Notificación Formal de Salida de Colaborador

Nombre del colaborador: _____

Departamento: _____

Fecha de salida: ___ / ___ / ____

Tipo de salida: ☐ Renuncia ☐ Despido ☐ Fin de contrato

Notificado por: _____

Fecha de notificación a TI: ___ / ___ / ____

Firma recursos Humanos: _____

INVENTARIO DE ACTIVOS ASIGNADOS

ThermoSolutions Group

Listado de Activos Asignado

N° placa Activo	Tipo Activo	Serie	Fecha asignación	Observaciones

Responsable de TI: _____ **Firma:** _____

CONSTANCIA DE DEVOLUCIÓN DE ACTIVOS

ThermoSolutions Group

Nombre del colaborador:	
Departamento:	
Fecha de salida:	

Detalle de activos devueltos

#	Tipo de activo	Consecutivo	Estado del equipo	Observaciones
1			Bueno ☐ Regular ☐ Dañado ☐	
2			Bueno ☐ Regular ☐ Dañado ☐	
3			Bueno ☐ Regular ☐ Dañado ☐	
4			Bueno ☐ Regular ☐ Dañado ☐	
5			Bueno ☐ Regular ☐ Dañado ☐	

Verificado en sistema de activos: ☐ Sí ☐ No

Fecha de verificación: _____

En fe de lo anterior, firmo conforme en San José, el día **xx** del mes de **xx** del año **xxxx.**

Firma TI: _____ **Firma RH: _____**

INFORME FINAL DE CIERRE DE PROCESO

ThermoSolutions Group S.A

Informe Final de Devolución de Activos

Colaborador: _____

Departamento: _____

Fecha de salida: ___ / ___ / ____

Fecha de devolución: ___ / ___ / ____

Todos los activos devueltos: ☐ Sí ☐ No

Observaciones:

☐ Activos verificados y registrados en sistema.

☐ Constancia firmada por ambas partes.

☐ Copia entregada a recursos humanos.

Responsable TI: _____ **Firma:** _____

Recursos Humanos: _____ **Firma:** _____

APÉNDICE D Política de control de accesos y gestión de contraseñas

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

POLÍTICA DE CONTROL DE ACCESOS Y GESTIÓN DE CONTRASEÑAS

JOSEPH LAZO BADILLA

JUNIO, 2025

ThermoSolutions Group S. A	PL-CAGC-INF-001	Fecha: 15/06/2025
Política de control de accesos y gestión de contraseñas	Rev. 01	Proceso: Tecnologías de la información / Recursos Humanos / Jefaturas de área

INTRODUCCIÓN

Los datos de las empresas son muy valiosos para las organizaciones, garantizar la seguridad de los accesos a los sistemas y plataformas digitales se vuelve cada vez más una prioridad, es por eso que en este documento se establece la política para ThermoSolutions Group S.A enfocándose principalmente sobre el control de accesos y gestión de contraseñas, con el fin de definir un marco normativo y operativo que asegure la protección de los recursos tecnológicos frente a accesos no autorizados, especialmente durante el proceso de desvinculación de personal.

Esta política contribuye a la necesidad de aplicar controles robustos para la gestión de credenciales de usuarios, alineándose con los principios y directrices establecidos por la norma internacional ISO/IEC 27001, que promueve buenas prácticas en la gestión de la seguridad de la información, buscando fortalecer los mecanismos internos de control, reducir riesgos de datos sensibles y asegurar que las cuentas de acceso sean gestionadas de forma adecuada, especialmente cuando un colaborador deja de formar parte de la organización, la implementación de esta política permitirá no solo cumplir con estándares internacionales, sino también fomentar una cultura de responsabilidad y prevención en el uso y administración de los sistemas de información corporativos.

Objetivo

Es fundamental establecer un protocolo de seguridad claro, estructurado y obligatorio que regule la modificación o desactivación inmediata de todas las credenciales de acceso asociadas a los usuarios que finalizan su relación laboral con la empresa, ya sea por motivos de despido, renuncia voluntaria, terminación de contrato u otras circunstancias, para que este protocolo sea cumplido se deben contemplar cada una de las plataformas, sistemas internos, accesos remotos, servicios en la nube y cualquier otro recurso digital que haya sido asignado al colaborador durante su permanencia en la empresa.

El objetivo principal de esta medida es prevenir cualquier posibilidad de acceso no autorizado en la organización que pueda comprometer la integridad, confidencialidad o disponibilidad de la información y evitar mala gestión de la información, fuga o mal uso de los datos y recursos tecnológicos pertenecientes a la empresa, además, este control contribuye al cumplimiento de estándares internacionales de seguridad de la información, como los establecidos por la norma ISO/IEC 27001, promoviendo una gestión responsable y segura de los accesos a los activos tecnológicos de ThermoSolutions Group S.A.

Alcance

Es aplicable y de manera obligatoria para todos los colaboradores que cuenten con accesos a los sistemas de informática o aquellas herramientas que requieran autenticación, ya sean accesos remotos o plataformas de uso organizacional que fueron asignadas a los colaboradores de ThermoSolutions Group S.A, es aplicable para el proceso de salida de personal por renuncia o despido, con el objetivo de garantizar el control de accesos, proteger la información crítica y cumplir con los controles por la norma ISO/IEC 27001.

Definiciones

- **Credenciales de acceso:** Combinación de usuario, contraseña y/o mecanismos adicionales de autenticación (como tokens o códigos de verificación en dos pasos) que permiten a un colaborador acceder a los sistemas, plataformas o recursos digitales de la organización.
- **Gestión de accesos:** Conjunto de políticas, procesos y controles implementados para regular la creación, modificación, uso y desactivación de las credenciales de los usuarios dentro de los sistemas de la empresa.
- **Desactivación de credenciales:** Acción de anular o modificar los accesos de un colaborador a los sistemas informáticos de la organización, con el fin de prevenir el uso no autorizado de los recursos tecnológicos.
- **Autenticación de doble factor (2FA):** Método de seguridad que requiere dos formas de verificación (por ejemplo, contraseña y código enviado al celular) para conceder acceso a un sistema.
- **Bitácora de acciones:** Registro formal y ordenado de las actividades técnicas realizadas por el área de TI durante la gestión de desactivación de credenciales, que garantiza trazabilidad y soporte en auditorías.
- **Colaborador saliente:** Persona que finaliza su relación laboral con la organización y que debe tener todos sus accesos digitales revocados o modificados de inmediato.
- **Evidencia documental:** Conjunto de documentos (notificación, formulario de registro, bitácora e informe final) que respalda la correcta ejecución del procedimiento.

Abreviaturas

- **TI:** Tecnologías de la Información.
- **RH:** Recursos Humanos.
- **ISO/IEC 27001:** Norma internacional para la gestión de la seguridad de la información.
- **VPN:** Red Privada Virtual.
- **ERP:** Sistema de Planificación de Recursos Empresariales.
- **2FA:** Autenticación de Doble Factor.
- **ID:** Identificador único de usuario o cuenta dentro de los sistemas.

Normativa

Para garantizar la trazabilidad de las credenciales y accesos no autorizados, el procedimiento es basado bajo las prácticas de seguridad internacionales de la norma ISO/IEC 27001 en los siguientes controles:

- El control A.9.2.1 establece que para el registro de usuarios deben asignarse cuentas de forma controlada para el alta y baja de sus credenciales o accesos, exigiendo establecer la eliminación periódica de usuarios redundantes y desactivación automática o de forma inmediata cuando el empleado abandona la organización.
- El control A.9.2.6 especifica que los derechos de acceso deben retirarse cuando ya no requiera acceso, controlando los ingresos al colaborador cuando este finaliza el empleo o cambia de puesto dentro de la organización.
- El control A.9.4.1 se fundamenta en la restricción de acceso a la información indicando que debe estar controlado con base a la necesidad de conocimiento, restringiendo y ocultando las funciones de administración a usuarios finales y restringiendo de forma selectiva derechos de lectura, escritura o eliminación.

Matriz de roles

- Departamento de TI el cual es responsable de ejecutar el protocolo de desactivación de credenciales y documentar el proceso.
- Recursos humanos será la persona encargada de coordinar el proceso de salida del colaborador y notificar al área de TI.
- Jefaturas o gerencias del departamento son los encargados de validar con el departamento de TI cuales sistemas fueron utilizados por el colaborador.

Matriz de responsabilidades

Actividad	Ejecuta	Aprueba	Supervisa	Informado
Notificación de salida	RRHH	Gerencia General	Auditoría	TI
Levantamiento de accesos	TI	Jefatura TI	RRHH	Auditoría
Desactivación/modificación de credenciales	TI	Jefatura TI	RRHH	Auditoría
Registro en sistema de control	TI	Jefatura TI	Auditoría	RRHH
Informe de cierre	RRHH TI	Gerencia General	Auditoría	Gerencia

Recomendaciones

Para la implementación de este procedimiento, se recomiendan cinco etapas fundamentales las cuales se dividen de la siguiente manera:

Procedimiento	Descripción	Responsable
N°1: Notificación de salida	Recursos Humanos notifica al departamento de TI la salida del colaborador con al menos 48 horas de anticipación.	Recursos Humanos
N°2: Levantamiento de accesos	Se elabora un listado detallado de todos los sistemas y plataformas a los que el usuario tenía acceso.	Departamento de TI
N°3: Desactivación de accesos	Se desactivan o modifican contraseñas del correo, accesos remotos (VPN), ERP, sistemas internos, tokens y 2FA.	Departamento de TI
N°4: Registro del proceso	El proceso es registrado en el sistema de control interno y se archivan las evidencias.	Departamento de TI

N°5: Informe de cierre	Se genera un informe de cierre del procedimiento que es archivado por Recursos Humanos.	Recursos Humanos

La ejecución ordenada de este procedimiento permite asegurar que, ante la salida de un colaborador, todos los accesos a la infraestructura tecnológica sean controlados de forma correcta, esto nos ayuda a reducir significativamente el riesgo de accesos no autorizados y posibles fugas de información, sino que también fortalece el cumplimiento de políticas de seguridad, mejora la trazabilidad de acciones y mantiene protegidos los activos críticos de la organización. Una correcta coordinación entre Recursos Humanos y TI es clave para garantizar la continuidad operativa y la integridad de los datos empresariales.

Para evidenciar el cumplimiento de este procedimiento, se deberán llevar a cabo y conservar los siguientes documentos:

- **Notificación de salida del colaborador:** Documento ejecutado por el departamento de recursos humanos con el fin de comunicar de manera formal al área de TI la salida de un colaborador, con el objetivo de activar el proceso de desactivación de accesos, el área de TI puede tomar acción inmediata para proteger los sistemas de accesos no autorizados.
- **Formulario de registro de desactivación de credenciales**: Registra los accesos que fueron desactivados o modificados, el cual permite dejar auditoria clara de que las credenciales fueron gestionadas adecuadamente una vez ejecutada la salida del colaborador.
- **Bitácora de acciones realizadas:** Es un registro secuencial que detalla todas las acciones técnicas realizadas durante el proceso, desde que se recibió la notificación hasta que se completó la desactivación, permitiendo mantener trazabilidad del proceso, facilitar auditorías, y dar seguimiento a posibles errores, omisiones o tiempos de respuesta.
- **Informe de cierre del procedimiento:** Documento de cierre firmado por el área de tecnologías de la información en conjunto con la persona encargada de recursos humanos

que hace afirmar que todas las acciones fueron completadas satisfactoriamente permitiendo continuar con el proceso administrativo para el pago de la liquidación.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción	Elaborado por:

NOTIFICACIÓN DE SALIDA DEL COLABORADOR

ThermoSolutions Group S.A

Notificación Formal de Salida de Colaborador

Nombre del colaborador: _____

Departamento: _____

Fecha de salida: ___ / ___ / ____

Tipo de salida: ☐ Renuncia ☐ Despido ☐ Fin de contrato

Notificado por: _____

Fecha de notificación a TI: ___ / ___ / ____

Firma recursos Humanos: _____

FORMULARIO DE REGISTRO DE DESACTIVACIÓN DE CREDENCIALES

ThermoSolutions Group

Nombre del colaborador:	
Departamento:	
Fecha de salida:	

Detalle de sistemas desactivados

#	Sistema/Herramienta	Acción tomada	Fecha de acción
1		Desactivar ☐ Cambiar ☐ Eliminar ☐	
2		Desactivar ☐ Cambiar ☐ Eliminar ☐	
3		Desactivar ☐ Cambiar ☐ Eliminar ☐	
4		Desactivar ☐ Cambiar ☐ Eliminar ☐	
5		Desactivar ☐ Cambiar ☐ Eliminar ☐	

Actualizado en sistema de registros de accesos de control interno: ☐ Sí ☐ No

Fecha de actualización: _____

En fe de lo anterior, firmo conforme en San José, el día **xx** del mes de **xx** del año **xxxx**

Firma TI: _____ **Firma RH: _____**

BITÁCORA DE ACCIONES REALIZADAS

ThermoSolutions Group S.A

Sistema	Acción Realizada	Fecha	Responsable TI

INFORME DE CIERRE DEL PROCEDIMIENTO

ThermoSolutions Group S.A

Informe de Cierre de Proceso de Control de Accesos

Colaborador: _____

Departamento: _____

Fecha de salida: ___ / ___ / ____

Fecha de ejecución de desactivaciones: ___ / ___ / ____

Responsable técnico (TI): _____

Observaciones:

Confirmación:

☐ Todos los accesos fueron desactivados/modificados

☐ Bitácora completada y evidencia adjunta

☐ RH validó el cierre del proceso

Firma TI: _____ **Firma RH: _____**

APÉNDICE E Seguridad de la información

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

SEGURIDAD DE LA INFORMACIÓN

JOSEPH LAZO BADILLA

JUNIO, 2025

ThermoSolutions Group S. A	PRD-CTDR-INF-001	Fecha: 15/06/2025
Seguridad de la información	Rev. 01	Proceso: Tecnologías de la información

INTRODUCCIÓN

Las empresas son cada vez más vulnerables a errores técnicos en cuanto a tecnología, ataques a la información, fallos humanos o catástrofes naturales, por eso es crucial disponer de mecanismos eficaces que aseguren la disponibilidad, integridad y recuperación de la información vital de la organización, ya que la pérdida de datos importantes no solo puede poner en riesgo el funcionamiento cotidiano, sino también la continuidad del negocio, la confianza de los clientes y el cumplimiento normativo y por esta razón el presente procedimiento de respaldos periódicos y recuperación ante desastres, tiene como objetivo proteger la información esencial almacenada en sistemas, servidores y medios digitales, asegurando que, en caso de un incidente, los datos puedan restaurarse de forma rápida, segura y confiable.

Mediante este plan, se busca respaldar la información de forma periódica y definir roles, responsabilidades, activos críticos, frecuencias de copia y procesos de restauración, bajo criterios de seguridad, trazabilidad y mejora continua, reforzando así el compromiso institucional con la protección de sus activos de información y la continuidad operativa.

Objetivo

Estipular las directrices para proteger la información importante de la organización mediante la elaboración de respaldos periódicos y que se establezca un plan de recuperación ante desastres, con el propósito de garantizar la continuidad de la empresa frente a incidentes que comprometan la disponibilidad de los datos.

Uno de los activos más importantes de la organización es la información, por lo tanto, su pérdida puede causar grandes consecuencias graves, incumplimientos legales, daños o pérdidas económicas, este procedimiento tiene como propósito prevenir los riesgos en base a:

- respaldo de bases de datos, servidores y archivos críticos.
- reglas que estipulen el almacenamiento seguro de los respaldos ya sea en medios físicos o en la nube.
- revisión periódica de la integridad de los respaldos y mantenimiento de los registros detallados.
- establecer un plan de recuperación definiendo sistemas críticos o prioritarios.

Alcance

Este procedimiento será de aplicación obligatoria para todos los sistemas de información, servidores, bases de datos, archivos compartidos, dispositivos de almacenamiento y cualquier otro medio que contenga información esencial o crítica para la operación de ThermoSolutions Group S.A y debe ser aplicado tanto para los procesos de rutinas de respaldo como para la ejecución del plan de recuperación ante desastres, asegurando la continuidad del negocio frente a eventos inesperados que comprometan la disponibilidad, integridad o confidencialidad de los datos.

Este procedimiento se fundamente según la norma ISO/IEC:27001 en el control 17.1 el cual establece que las organizaciones deben garantizar la disponibilidad de la información mediante la implementación de planes de respaldo y recuperación, es por eso que esta ejecución del control mencionado permite asegurar que los datos puedan ser restaurados de manera oportuna y segura,

minimizando el impacto en las operaciones y saber responder antes cualquier incidente que comprometa la infraestructura o los sistemas de información.

Definiciones

- **Respaldo** Copia de seguridad de datos, archivos, bases de datos o sistemas que permite restaurar la información en caso de pérdida, corrupción o incidente.
- **Plan de recuperación ante desastres:** Conjunto de procedimientos documentados que permiten restaurar los sistemas y servicios tecnológicos de la organización tras un incidente grave, garantizando la continuidad del negocio.
- **Disponibilidad de la información:** Principio de seguridad que asegura que los datos estén accesibles cuando sean necesarios por los usuarios autorizados.
- **Integridad de la información:** Garantía de que los datos no han sido alterados o modificados de manera no autorizada.
- **Continuidad del negocio:** Capacidad de la organización para mantener operaciones esenciales durante y después de un evento que interrumpa sus procesos normales.
- **Medios de almacenamiento:** Dispositivos físicos o digitales donde se guardan los respaldos, como discos duros externos, servidores, almacenamiento en la nube u otros sistemas de almacenamiento seguro.
- **Simulacro de recuperación:** Ejercicio controlado en el que se pone a prueba el plan de recuperación ante desastres para validar su efectividad y preparar al personal responsable.
- **Activos críticos:** Sistemas, servidores, bases de datos o servicios tecnológicos considerados indispensables para la operación diaria de la empresa.

Abreviaturas

- **Backup:** Copia de seguridad de información.
- **Veeam:** Software de respaldo de servidores.
- **OneDrive:** Plataforma de respaldo en la nube.
- **DRP:** Plan de Recuperación ante Desastres.

Normativa

Este procedimiento responde conforme a la norma ISO/IEC 27001:2022, la cual establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información, específicamente, se fundamenta en los siguientes controles:

- Control 8.13 Copias de seguridad de la información: Este control hace énfasis en que se deben realizar copias de seguridad a intervalos regulares, conforme a una política y procedimientos documentados, asegurando su protección contra pérdida, alteración o destrucción, las copias deben ser verificadas y probadas regularmente.
- Control 5.29 Planificación de la continuidad del negocio de la información: Este apartado explica que las organizaciones deben establecer y ejecutar procedimientos que aseguren el funcionamiento continuo de los servicios y sistemas que manejan información más crítica o fundamental de la empresa e incluyendo procesos de recuperación ante desastres.
- Control 5.30 Implementación de la continuidad del negocio de la información: Se debe asegurar que los procedimientos de recuperación estén actualizados, sean conocidos por los responsables y se prueben regularmente para garantizar su eficacia en caso de incidentes.

Matriz de roles

- Departamento de TI se encargará de administrar respaldos, verificar su integridad y ejecutar plan de recuperación ante desastres**.**
- Usuarios finales deben de reportar necesidades de respaldo adicional y colaborar con los simulacros de recuperación.

Matriz de responsabilidades

Actividad	Ejecuta	Aprueba	Supervisa	Informado
Planificación de respaldos	TI	Jefatura TI	Auditoría	Gerencia
Ejecución del respaldo	TI	Jefatura TI	Auditoría	Gerencia
Validación de recuperación	TI Proveedor	Jefatura TI	Auditoría	Gerencia
Almacenamiento seguro	TI	Jefatura TI	Auditoría	Gerencia
Informe de respaldo	TI	Jefatura TI	Auditoría	Gerencia

Recomendación

Para facilitar la implementación de este procedimiento es recomendable desarrollarlo en las siguientes etapas:

Copias de seguridad

Se deben realizar copias de seguridad periódicas de la información esencial para la empresa de acuerdo con la siguiente frecuencia:

- Realizar una copia exacta de las bases de datos utilizadas por la empresa diariamente, para recuperar la información actualizada en caso de pérdida de datos, errores de sistema, corrupción de archivos o ataques informáticos.
- verificar, actualizar y respaldar semanalmente las carpetas compartidas en red o en la nube, que contienen archivos sensibles, de uso común o estratégicos para la operación, este tipo

de copia asegura que la documentación importante esté protegida contra modificaciones no autorizadas, pérdidas accidentales o daños.

- Backup completo de servidores se debe realizar mensualmente, con el fin de permitir recuperar por completo un servidor en caso de fallos mayores, ataques o daños físicos.

Los respaldos se deben almacenar en medios seguros de almacenamiento en la nube con autenticación, conservando al menos tres versiones históricas de cada respaldo, verificando la integridad de los respaldos mensualmente por el equipo de TI, documentando cada revisión detalladamente con fecha, tipo de respaldo, ubicación de almacenamiento y responsable.

Plan de recuperación ante desastres

Se deberá contar con un plan de recuperación ante desastres que permita restaurar la funcionalidad de los sistemas en el menor tiempo posible definiendo los activos prioritarios incluyendo en el plan:

- Introducción y objetivos del plan, como la la sección inicial del documento donde se describe el propósito del plan, su alcance y la razón por la que se implementa.
- Sistemas prioritarios, este compuesto de un listado de los sistemas, plataformas o servicios más importantes para la operación de la empresa, ordenados según su nivel de criticidad.
- Procedimiento de restauración de los sistemas son las instrucciones paso a paso para recuperar cada sistema, incluyendo los respaldos utilizados, las herramientas, y el orden en que deben restaurarse.
- Roles y responsable de cada etapa se refiere a la distribución de funciones entre los distintos participantes del plan, indicando quién hace qué, en qué momento y con qué nivel de autoridad.
- Contactos claves ya sean internos o externos el cual está definido por la lista de personas o empresas que deben ser notificadas o involucradas en el proceso de recuperación, ya sea dentro o fuera de la organización.

Se debe tomar en cuenta que cualquier modificación de sistemas o infraestructura tecnológica, se debe revisar el plan actual, actualizándolo cada doce meses como parte del ciclo de la mejora continua.

Para demostrar el cumplimiento del procedimiento se debe registrar y documentar los siguientes documentos:

Evidencia	Descripción	Propósito / Importancia
Control de respaldos realizados	Registro detallado de todas las copias de seguridad efectuadas (diarias, semanales, mensuales), incluyendo fechas, tipo de respaldo y responsable.	Asegura trazabilidad, permite verificar cumplimiento de frecuencias y sirve como respaldo ante auditorías o incidentes de pérdida de datos.
Actas de simulacros de recuperación	Documento que registra la ejecución y resultados de una prueba del plan de recuperación, simulando un incidente real de pérdida de datos o sistemas.	Evalúa la efectividad del plan de recuperación, permite detectar fallos, mejorar tiempos de respuesta y evidencia que el plan es funcional y no solo teórico.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción	Elaborado por:

CONTROL DE RESPALDOS REALIZADOS

ThermoSolutions Group

Registro de ejecución de respaldos

Fecha	Sistema	Tipo de Respaldo	Medio de almacenamiento	Responsable
		☐ Diario ☐ Semanal ☐ Mensual	☐ Nube ☐ Nas local	
		☐ Diario ☐ Semanal ☐ Mensual	☐ Nube ☐ Nas local	
		☐ Diario ☐ Semanal ☐ Mensual	☐ Nube ☐ Nas local	

APÉNDICE F política de control de puertos USB

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

POLITICA DE CONTROL DE PUERTOS USB

JOSEPH LAZO BADILLA

JUNIO, 2025

ThermoSolutions Group S. A	PRD-CTDR-INF-001	Fecha: 15/06/2025
Política de control de puertos USB	Rev. 01	Proceso: Tecnologías de la información

INTRODUCCIÓN

Cada día se detectan más vulnerabilidades a amenazas informáticas internas y externas, el uso indebido o no controlado de dispositivos de almacenamiento extraíbles USB se define en las empresas como un peligro significativo para la protección de los datos y la infraestructura tecnológica de las organizaciones, este tipo de dispositivos, si no se manejan correctamente, pueden propiciar la infiltración de software malintencionado, además de la fuga no autorizada de información sensible, poniendo en riesgo la integridad, disponibilidad y confidencialidad de los activos de información.

Con el objetivo de cerrar esta brecha de seguridad, se establece el presente procedimiento como parte de sus políticas de control de acceso y protección de activos tecnológicos, alineado con los estándares internacionales de seguridad de la información definidos en la norma ISO/IEC 27001:2022, específicamente en los controles 13.2.1 (protección contra software malicioso) y A.9.4.5 (uso restringido de servicios).

Esta política busca concretar directrices claras para el bloqueo, monitoreo y gestión de excepciones del uso de puertos USB en todos los equipos conectados a la red corporativa, para garantizar buen manejo de la seguridad ante estos dispositivos y buscando que este control de medios extraíbles no solo prevenga posibles incidentes de seguridad, sino que también refuerza el cumplimiento de los requisitos legales y normativos, promoviendo una cultura organizacional basada en la responsabilidad y la prevención de riesgos tecnológicos.

La implementación efectiva de este procedimiento implica la colaboración activa del departamento de Tecnologías de la Información, los jefes de área y los usuarios autorizados, así como el mantenimiento de un sistema de registros, auditorías y documentación que permita evidenciar el cumplimiento de los controles establecidos.

Objetivo

El propósito de este procedimiento es cerrar una brecha crítica de seguridad informática mediante el establecimiento de directrices claras y controladas que permitan prevenir la introducción de software malicioso y evitar la fuga no autorizada de información sensible a través del uso indebido de dispositivos de almacenamiento USB en los equipos corporativos.

Mediante esta política se busca reforzar la protección del entorno informático al controlar el acceso físico y lógico a los puertos USB de computadoras de escritorio, portátiles, estaciones de trabajo y cualquier otro equipo conectado a la red interna de la empresa, con la implementación de este control tiene como objetivo mitigar riesgos de seguridad que podrían comprometer la integridad, confidencialidad y disponibilidad de los datos, asegurar el cumplimiento de normativas internacionales como la ISO/IEC 27001, y fomentar una cultura de uso responsable y seguro de los activos tecnológicos dentro de la organización.

Alcance

Este procedimiento será de aplicación obligatoria para todos los equipos de cómputo, estaciones de trabajo, portátiles, computadoras de escritorio y cualquier otro dispositivo que se conecte a la red corporativa de ThermoSolutions Group S.A.

También aplica a todos los usuarios de la organización, sin excepción, independientemente de su cargo, área o nivel de acceso, incluyendo personal administrativo, operativo, técnico, consultores externos y contratistas que utilicen recursos tecnológicos propiedad de la empresa. Este procedimiento tiene como objetivo prevenir la utilización no autorizada de dispositivos de almacenamiento USB y similares (como discos externos, memorias portátiles, adaptadores inalámbricos, etc.), que puedan ser usados como vectores para la introducción de software malicioso, extracción de información sensible o alteración del entorno informático corporativo.

Se incluyen en este alcance todas las situaciones en las que:

- Se entrega un equipo nuevo o se reasigna uno existente.
- Se requiere el uso de un puerto USB con fines justificados.

- Se detecta el uso de dispositivos extraíbles sin previa autorización.
- Se realiza una auditoría interna o revisión de cumplimiento.

Definiciones

- **Dispositivo USB:** Unidad de almacenamiento extraíble como memorias portátiles, discos duros externos, adaptadores inalámbricos u otros periféricos que pueden conectarse a los equipos corporativos a través del puerto USB.
- **Bloqueo de puertos USB:** Configuración técnica aplicada a los equipos de la organización que deshabilita por defecto el uso de dispositivos USB no autorizados, con el fin de prevenir accesos no controlados o instalación de software malicioso.
- **Excepción autorizada:** Permiso formal otorgado por el jefe inmediato y aprobado por el departamento de TI que permite el uso controlado de puertos USB en un equipo específico y por un periodo definido.
- **Bitácora de excepciones:** Registro oficial y centralizado donde se documentan todas las solicitudes aprobadas de uso de dispositivos USB, incluyendo usuario, equipo, motivo y vigencia.
- **Auditoría de cumplimiento:** Proceso de verificación periódica realizado por el área de TI para asegurar que las políticas de bloqueo y control de dispositivos USB se estén cumpliendo adecuadamente.
- **Software malicioso (Malware):** Programas diseñados para dañar, alterar o robar información de los sistemas, los cuales pueden propagarse a través de dispositivos USB no controlados.
- **Registro de configuración:** Documento técnico que evidencia la aplicación de bloqueos de puertos USB en cada equipo entregado o reasignado, como parte del control preventivo.

Abreviaturas

- **USB**: Unidad de almacenamiento portátil.
- **Excepción autorizada**: Permiso especial para uso de USB en casos justificados.
- **ESET**: Software de control de dispositivos.
- **TI:** Tecnologías de la Información.
- **RH:** Recursos Humanos.

Normativa

El procedimiento se basa en fundamentos estipulados con las mejores prácticas internacionales bajo la norma ISO/IEC:27001, específicamente en los controles:

- 13.2.1 sobre la protección contra software malicioso establece que se debe implementar medidas de protección y recuperación ante amenazas causadas por software malicioso, es por eso por lo que el bloqueo de los dispositivos USB es una medida preventiva fundamental para evitar infecciones a través de los medios extraíbles no autorizados.

- A.9.4.5 En el uso restringido de servicios se enfoca en bloquear aquellos servicios o funcionalidades que no sean necesarios para el desempeño del trabajo del usuario

Estos controles contribuyen a limitar y controlar el acceso físico y lógico de los medios extraíbles dando como parte clave el cumplimiento del propósito que garantiza una mejor protección en los activos de la información

Matriz de roles

- El departamento de TI es el principal encargado de configurar, administrar y monitorear los controles de los puertos USB en todos los equipos conectados a la red corporativa, entre sus funciones está aplicar bloqueos por defecto, gestionar las herramientas de seguridad de ESET y las soluciones de administración de endpoints, además debe de registrar las excepciones aprobadas, mantener actualizada la bitácora de uso autorizado, y realizar auditorías periódicas para verificar el cumplimiento de la política.

- Jefe de departamento de cada área
  Son responsables de identificar, justificar y solicitar formalmente las excepciones al bloqueo de puertos USB para los casos en que el uso sea estrictamente necesario por razones operativas, estas solicitudes deben incluir el nombre del usuario, el equipo, el motivo de la excepción y serán evaluadas por el departamento de TI antes de su aprobación.

- Aquellos colaboradores que hayan recibido una excepción formal aprobada por su jefe inmediato y el Departamento de TI, estos usuarios deben utilizar los dispositivos de almacenamiento USB exclusivamente bajo las condiciones autorizadas, cumplir con las restricciones indicadas, y estar conscientes de que el uso inadecuado podrá conllevar sanciones administrativas y técnicas, además del retiro inmediato del permiso.

Matriz de responsabilidades

Actividad	**Ejecuta**	**Aprueba**	**Supervisa**	**Informado**
Solicitud de autorización	Usuario	Jefatura	TI	RRHH
Evaluación de solicitud	TI	Jefatura TI	Auditoría	Gerencia
Autorización/bloqueo	TI	Jefatura TI	Auditoría	Gerencia
Registro en bitácora	TI	Auditoría	Jefatura TI	Gerencia
Informe de excepciones	TI	Gerencia TI	Auditoría	RRHH

Recomendaciones

El procedimiento se basa en las mejores prácticas de control de la norma, en relación con la norma ISO/IEC 27001:2022, particularmente en los controles 13.2.1 sobre el apartado de protección contra software malicioso y A.9.4.5 sobre el control de acceso a sistemas y funciones.

La regulación del uso de puertos USB contribuye a prevenir incidentes de seguridad relacionados con amenazas internas o externas y refuerza el cumplimiento de las políticas de protección de activos tecnológicos, además mencionan que se deben incluir requisitos para la protección contra la intercepción, copia o modificación de la información, respaldado por políticas de uso aceptable.

Para la implementación se recomienda dividirla en las siguientes etapas:

Etapa	Descripción	Observaciones / Requisitos clave
N°1: Bloqueo de dispositivos USB	Se bloquean todos los puertos USB de los equipos nuevos o reasignados utilizando la herramienta de administración ESET.	Debe documentarse en un registro de configuración técnica.
N°2: Solicitud de excepciones	Los jefes de departamento deben realizar una solicitud formal de excepción para casos justificados.	TI debe revisar y aprobar, registrando usuario, equipo y justificación.
N°3: Registro en bitácora de excepciones	Se mantiene una bitácora actualizada que incluye todos los usuarios con permisos excepcionales.	La bitácora debe contener: nombre de usuario, motivo, fecha de solicitud y firma del responsable de TI.
N°4: Auditorías periódicas	Se ejecutan revisiones al menos cada 6 meses para verificar cumplimiento.	Cualquier uso indebido debe ser documentado y tratado según política de incidentes.

Excepciones permitidas

Se permitirán los usos de los puertos USB mediante una solicitud formal aprobada por el jefe inmediato del área y autorizada por el departamento de TI, estas excepciones de otorgarán a equipos dedicados a procesos específicos como impresiones especializadas, actualizaciones del firmware de las máquinas de producción.

Se mantendrá un registro detallado con usuario autorizado, equipo, motivo de la excepción y vigencia, realizando auditorias trimestrales para validar el uso correcto de los dispositivos autorizados.

Evidencias requeridas

Para evidenciar el cumplimiento de este procedimiento, se deberán llevar a cabo y conservar los siguientes documentos:

- **Registro de excepciones de puertos USB:** Formulario en el que se registran las solicitudes formales realizadas por los jefes de cada departamento el cual tiene como fin habilitar temporal o permanente los puertos USB en casos justificados, permitiendo controlar y justificar los equipos que requieren el uso de dispositivos USB y evitar habilitaciones informales, para evidenciar la trazabilidad en la aprobación.
- **Registro de configuración de bloqueo USB:** Documento técnico que evidencia que el bloqueo de puertos USB fue aplicado correctamente en cada dispositivo entregado, evidenciando que el control preventivo ha sido ejecutado en todos los equipos de la empresa y garantizando que la restricción de puertos USB están aplicados por defecto.
- **bitácora de excepciones autorizadas:** Es un registro centralizado que detalla todas las excepciones aprobadas para el uso de puertos USB en los dispositivos que son propiedad de la compañía, consolidando la información de los formularios recibidos y facilita el control y seguimiento de los equipos con puertos USB habilitados, permitiendo hacer auditorías o revocaciones según se requiera.
- **informe de auditoría:** Es un documento técnico elaborado por el área de TI que resume los resultados de las auditorías periódicas y que permite evaluar si los dispositivos USB se están utilizando conforme a las políticas establecidas, y si existen desviaciones que deban corregirse.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción	Elaborado por:
01	28/05/2025	Creación de documento inicial	Joseph Lazo Badilla

REGISTRO DE EXCEPCIONES DE PUERTOS USB

ThermoSolutions Group

Fecha	
Departamento:	
Nombre del solicitante	
Nombre del colaborador:	
Equipo (Código / Serie)	
Aprobado por:	

Motivo de la solicitud

☐ Actualización firmware

☐ Impresión especializada

☐ Otro: _____

En fe de lo anterior, firmo conforme en San José, el día **xx** del mes de **xx** del año **xxxx.**

REGISTRO DE EXCEPCIONES DE PUERTOS USB

Empresa: ThermoSolutions Group

N° activo	Colaborador	Departamento	Equipo (Serie)	Fecha de bloqueo	Realizado por (TI)	Observaciones

Firma TI: _____ **Firma RH: _____**

BITÁCORA DE EXCEPCIONES AUTORIZADAS

Empresa: ThermoSolutions Group

N° activo	**Colaborador**	**Departamento**	**Equipo (Serie)**	**Motivo**	**Observaciones**

INFORME DE AUDITORÍA

Empresa: ThermoSolutions

Informe de auditoría de control de puertos USB

Fecha: ___ / ___ / ____

Auditor responsable: _____

Resumen de resultados

Equipo	Usuario	Estado de puertos	Observaciones	Cumple Política
		☐ Bloqueado ☐ Excepción activa ☐ Desbloqueado		☐ No ☐ Sí
		☐ Bloqueado ☐ Excepción activa ☐ Desbloqueado		☐ No ☐ Sí

Medidas correctivas tomadas

ACTA DE SIMULACRO REALIZADO

ThermoSolutions Group S. A
Acta de Simulacro de Recuperación de Datos

Fecha del simulacro: ___ / ___ / ____

Tipo de incidente simulado: ☐ Falla técnica ☐ Ataque cibernético ☐ Otro: _____

Sistemas involucrados: _____

Duración total del simulacro: _____

Resumen del proceso:

Resultado final:

☐ Exitoso ☐ Parcialmente exitoso ☐ Fallido

Recomendaciones

Firma:

Responsable de TI: _____

APÉNDICE G Procedimiento de mantenimiento de equipos tecnológicos

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS TECNOLÓGICOS

JOSEPH LAZO BADILLA

JUNIO, 2025

ThermoSolutions Group S. A	PRD-CTDR-INF-001	Fecha: 15/06/2025
Procedimiento de mantenimiento de equipos tecnológicos	Rev. 01	Proceso: Tecnologías de la información

INTRODUCCIÓN

En el contexto de una infraestructura tecnológica empresarial, la disponibilidad, confiabilidad y seguridad de los activos tecnológicos son elementos esenciales para garantizar la continuidad operativa y la protección de la información, los equipos y sistemas informáticos que no reciben un mantenimiento adecuado están más expuestos a fallos, vulnerabilidades de seguridad y disminución en su rendimiento, lo que puede comprometer los procesos críticos de la organización.

En base a esta necesidad, se establece la normativa internacional ISO:27001 para definir los lineamientos técnicos y administrativos del mantenimiento preventivo y correctivo de los activos tecnológicos, con el objetivo de mantener el buen funcionamiento a lo largo del tiempo, minimizar interrupciones no planificadas y extender la vida útil de los equipos.

Esta normativa se fundamenta en los principios de gestión de activos y seguridad de la información establecidos particularmente en los controles relacionados con el inventario de activos, la protección contra fallos y la gestión de cambios. A través de su aplicación, se garantiza no solo la eficiencia operativa, sino también el cumplimiento de estándares internacionales que respaldan la integridad, disponibilidad y confidencialidad de los sistemas de información de la empresa.

Objetivo

Establecer un procedimiento estándar, estructurado y sistemático para el cumplimiento de mantenimiento correctivo y preventivo de los activos tecnológicos, con el fin de asegurar el tiempo de vida útil de los dispositivos, brindando disponibilidad, funcionalidad y alineación con los controles de seguridad establecidos en la norma ISO/IEC 27001, buscando garantizar el adecuado funcionamiento de los equipos y reducir el riesgo de fallos imprevistos, prolongando la vida útil de los dispositivos, mejorar la planificación de los recursos técnicos y manteniendo la continuidad operativa de la organización.

Alcance

Es aplicable a todos los activos tecnológicos que son utilizados en las áreas de trabajo de ThermoSolutions Group el cual debe realizarse de manera obligatoria para las áreas administrativas y operativas, se incluyen computadoras de escritorios y portátiles, servidores, impresoras, switches, routers y otros equipos de infraestructura tecnológica, aplicándose tanto para mantenimientos preventivos como para acciones por fallas para garantizas la mejora continua de los servicios.

Este procedimiento se fundamenta según la norma ISO/IEC:27001 en el control A.12.1.2 que establece que el mantenimiento debe realizarse de manera planificada y controlada para reducir los riesgos que puedan comprometer la seguridad de los sistemas de la información, por lo tanto, este procedimiento asegura que estos activos estén disponibles y funcionando de manera operativa bajo las condiciones óptimas y seguras con registros que respalden cada intervención técnica.

Definiciones

- **Mantenimiento preventivo:** Conjunto de actividades planificadas orientadas a garantizar la operatividad de los equipos tecnológicos mediante revisiones periódicas, limpieza, actualización de software y verificación de rendimiento.
- **Mantenimiento correctivo:** Acciones realizadas sobre los equipos cuando presentan fallas o incidentes, orientadas a restablecer su funcionamiento normal, incluyendo reparaciones, reinstalaciones y sustitución de componentes.

- **Cronograma de mantenimiento:** Documento que establece las fechas programadas para la ejecución de mantenimientos preventivos de acuerdo con el tipo de equipo y su criticidad.
- **Registro de mantenimiento:** Evidencia documental que respalda las acciones de mantenimiento realizadas, detallando fecha, equipo, técnico responsable, tipo de intervención y observaciones.
- **Proveedor autorizado:** Empresa externa certificada que presta servicios técnicos cuando el mantenimiento no puede ser resuelto de manera interna por el departamento de TI.
- **Sistema de gestión de activos (Softland):** Herramienta corporativa utilizada para registrar todas las actividades relacionadas con mantenimientos preventivos y correctivos de los activos tecnológicos

Normativa

Esta normativa aplica a todos los activos tecnológicos que están dentro del inventario de TI de los cuales se detallan:

- Computadoras de escritorio y portátiles.
- Servidores físicos y virtuales.
- Switches, routers y firewalls.
- Equipos de almacenamiento.
- Sistemas de videovigilancia.
- Estaciones de trabajo administrativas.

Se requiere mantener un inventario actualizado de todos los activos vinculado cada uno a su responsable, y establecer medidas proactivas que permitan minimizar el impacto de posibles fallos, es por eso que se tomara como base los controles de la norma 5.9, 8.14 y 8.32 , especialmente para cumplir con los mantenimientos preventivos y correctivos ya que estos apartados detallan que toda intervención técnica, reinstalaciones, configuraciones o mantenimientos deben estar documentados y autorizados bajo un proceso de control.

Controles de la normativa aplicados

- Control 5.9 Inventario de activos de información: Este control se centra en la importancia de mantener un inventario al día de todos los activos tecnológicos, asignándoles a cada uno su encargado, localización, estado y programación de mantenimiento.
- Control 8.14 Protección contra fallos: Es necesario implementar acciones proactivas para reducir el efecto de eventuales fallos, y los controles preventivos regulares disminuyen la posibilidad de sucesos tecnológicos no previstos.
- Control 8.32 Administración de modificaciones: Cualquier acción técnica, en particular los mantenimientos correctivos que conlleven modificaciones de hardware, reinstalaciones o configuraciones, deben ser documentadas bajo un procedimiento de control de modificaciones.

Matriz de roles

- Departamento de TI es la persona encargada de elaborar y mantener actualizados los planes de mantenimiento, coordinando los mantenimientos preventivos y correctivos para registrarlos en la actividad realizada al sistema de gestión de activos.
- Jefes de departamento deben notificar al departamento de TI sobre fallas o necesidades, además apoyar con la disponibilidad para los posibles periodos asignados en la agenda de mantenimientos.

Matriz de responsabilidades

Actividad	**Ejecuta**	**Aprueba**	**Supervisa**	**Informado**
Planificación de cronograma	TI	Jefatura TI	Auditoría	RRHH
Ejecución del mantenimiento preventivo	TI/Proveedor	Jefatura TI	Auditoría	Usuario
Registro de actividades	TI	Jefatura TI	Auditoría	Gerencia
Mantenimiento correctivo	TI/Proveedor	Jefatura TI	Auditoría	Gerencia

Actividad	Ejecuta	Aprueba	Supervisa	Informado
Informe final	TI	Jefatura TI	Auditoría	Gerencia

Recomendaciones

Para asegurar el correcto funcionamiento del procedimiento, se recomienda ejecutarlo de acuerdo con las siguientes etapas:

Mantenimiento preventivo

Para las computadoras de escritorio, portátiles e impresoras se realizarán mantenimientos con una frecuencia periódica de seis meses, mientras que para servidores se deberá realizar cada tres meses, realizando para todos los casos su limpieza interna, revisión de ventiladores, temperatura, actualizaciones de software, verificación de los dispositivos y pruebas de rendimiento.

Dentro de las actividades a realizar son:

- Limpieza interna: Eliminación de polvo, suciedad y residuos acumulados dentro del equipo para prevenir sobrecalentamiento, fallos eléctricos y deterioro de componentes internos como ventiladores, placas base o memorias.
- verificación de ventiladores, temperatura, y rendimiento: Consiste en comprobar que los ventiladores estén funcionando correctamente, que la temperatura del equipo se mantenga dentro de los rangos normales, y que el sistema no presente lentitud o sobrecargas, para obtener como objetivo principal de este punto evitar daños por sobrecalentamiento, mejora la eficiencia del equipo y detectar posibles fallos antes de que se conviertan en incidentes críticos.
- Actualización de software y parches de seguridad: Repara vulnerabilidades, mejora el rendimiento del sistema y aumenta la protección contra amenazas o fallos del sistema.
- revisión de conexiones y cableado: Inspección física y funcional de los cables de poder, red, periféricos, así como conectores internos en servidores o computadoras.

- Registro de actividad en el sistema de los activos: Documentación de todas las ejecuciones realizadas durante el proceso de cada mantenimiento y estas acciones deben ser ingresadas en el módulo de control de activos fijos de softland con el fin de llevar un historial técnico por equipo.
- Agendar el mantenimiento periódico nuevamente según corresponda: Programar la próxima fecha de mantenimiento del equipo según su tipo, uso o estado actual (cada 3 o 6 meses, según corresponda).

Mantenimiento correctivo

Se realizará solamente en caso de incidentes o reportes por parte del usuario, estos casos se podrán ejecutar internamente o dependiendo de la complicidad con un proveedor autorizado, cada acción correctiva se deberá documentar indicando la fecha, falla, solución implementada y técnico responsable, y toda intervención será registrada en el módulo de activos fijos de softland, y deberán estar disponibles para auditorías internas y externas.

Para asegurar el cumplimiento del procedimiento y trazabilidad se deben almacenar y generar los siguientes documentos:

- Cronograma semestral de mantenimiento preventivo: Documento de planificación que indica las fechas programadas para realizar mantenimientos preventivos a los equipos tecnológicos durante un período de seis meses, además permite organizar con anticipación las intervenciones técnicas, coordinar con los departamentos involucrados, y garantizar que todos los equipos reciban mantenimiento dentro del plazo establecido.
- Formulario de mantenimiento preventivo realizado: Registro que se completa cada vez que se lleva a cabo un mantenimiento preventivo a un dispositivo, proporcionando pruebas de las labores efectuadas en cada equipo, proporcionando seguimiento acerca de qué equipos fueron atendidos, qué revisiones se llevaron a cabo, en qué condiciones se encontraban y quién las llevó a cabo.
- Registro de mantenimiento correctivo: Documento que se llena cada vez que un equipo presenta una falla o necesita una reparación no programada, permite llevar un control de los

incidentes técnicos ocurridos, el historial de reparaciones, la frecuencia de fallos por equipo, y tomar decisiones sobre reposición o mejora.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción	Elaborado por:
01	30/05/2025	Creación de documento inicial	Joseph Lazo Badilla

CRONOGRAMA SEMESTRAL DE MANTENIMIENTO PREVENTIVO

Organización: ThermoSolutions Group

Cronograma semestral

Numero de activo	Equipo	Ubicación	Responsable del equipo	Fecha programada	Responsable de TI

FORMULARIO DE MANTENIMIENTO PREVENTIVO REALIZADO

ThermoSolutions Group S.A

Registro de Mantenimiento Preventivo

Fecha: ___ / ___ / ____

Código del equipo: _____

Tipo de equipo: _____

Ubicación: _____

Tareas realizadas:

☑ Limpieza interna ☑ Verificación ventiladores ☑ Actualizaciones ☑ Revisión de rendimiento

Otros: _____

Observaciones:

Firma del técnico _____

Firma del usuario _____

REGISTRO DE MANTENIMIENTO CORRECTIVO

Organización: ThermoSolutions Group

Registro de Mantenimiento Correctivo

Numero de activo	Equipo	Falla reportada	Solución aplicada	Técnico responsable	Proveedor externo
					☐ No ☐ Sí

APÉNDICE H Procedimiento de control de la topología de red

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROCEDIMIENTO DE CONTROL DE LA TOPOLOGÍA DE RED

JOSEPH LAZO BADILLA

JUNIO, 2025

ThermoSolutions Group S. A	PRD-CTDR-INF-001	Fecha: 15/06/2025
Procedimiento de control de la topología de red	Rev. 01	Proceso: Tecnologías de la información

INTRODUCCIÓN

La infraestructura de la red en una compañía se destaca como uno de los cimientos esenciales para el funcionamiento constante y seguro de los sistemas tecnológicos, bajo esta definición, la adecuada documentación y continuo mantenimiento de la topología de red, tanto en su aspecto físico como lógico, resulta crucial para asegurar la integridad, disponibilidad y privacidad de los datos y servicios esenciales.

Este documento tiene como propósito establecer los lineamientos para la elaboración, gestión y conservación de los diagramas de red que representen gráficamente la arquitectura tecnológica de la organización, a través de la gestión estructurada de la topología, se busca facilitar la administración de los dispositivos conectados, fortalecer la seguridad mediante una segmentación adecuada y mejorar la capacidad de respuesta ante incidentes o cambios en la infraestructura.La política abarca todos los componentes de red, incluyendo routers, switches, firewalls, servidores, estaciones de trabajo, conexiones inalámbricas y accesos externos, estableciendo claramente los roles y responsabilidades del equipo de TI en cuanto al diseño, actualización y resguardo de los diagramas de red, en este documento se define la metodología para su elaboración.

Objetivo

El propósito de este documento es establecer una política clara y estructurada para la creación, gestión y mantenimiento actualizado de la topología de red a nivel físico y lógico, así como la correcta representación y documentación de la infraestructura de red no solo permite una visión integral de los componentes tecnológicos de la organización, sino que también facilita la administración, diagnóstico, planificación de crecimiento y respuesta ante incidentes de seguridad.

Por medio de esta política, se busca garantizar que todos los elementos de red incluyendo dispositivos, enlaces, configuraciones y segmentaciones estén organizados, documentados y protegidos conforme a los principios de seguridad de la información, esta administración de la

topología también es clave para asegurar el cumplimiento de los controles de seguridad exigidos por normativas como la ISO/IEC 27001, especialmente aquellos relacionados con la gestión de activos, la protección de la infraestructura y la planificación de continuidad operativa.

Mantener actualizada la topología de red permite al área de TI identificar problemas en la red de manera más eficiente, prevenir riesgos, optimizar recursos y segmentar adecuadamente los entornos según niveles de prioridad.

Alcance

Esta normativa es de cumplimiento obligatorio para todos los componentes de la infraestructura tecnológica de ThermoSolutions Group S.A, incluyendo tanto la red de cables como la inalámbrica, además de los sistemas internos y conexiones externas, Incluyendo todos los dispositivos de red, tanto activos como pasivos, que están directa o indirectamente vinculados a la red empresarial, como routers, switches, cortafuegos, puntos de acceso inalámbrico y servidores físicos.

Asimismo, este alcance contempla las interconexiones con redes externas, como accesos VPN, enlaces con las sucursales de los canales de venta en Liberia, Heredia y Curridabat, proveedores tecnológicos y cualquier otro punto de integración que tenga implicaciones en la seguridad, disponibilidad o funcionamiento de la red interna.

Problema que resuelve

La empresa actualmente cuenta con una infraestructura de red que le permite administrar todos sus dispositivos de manera lógica e identificar mediante un diagrama actualizado a tiempo real los equipos físicos identificados y adoptados dentro de la red, logrando identificar de manera automática los dispositivos conectados, visualización de puertos, segmentos, Vlan, estados operativos, monitoreo centralizado por departamento y un control de energía y tráfico por dispositivo, sin embargo a pesar de contar con la herramienta, la misma no es utilizada, la falta de una política clara genera desorganización, vulnerabilidades de seguridad, dificultades en la gestión de cambios y una respuesta lenta ante incidentes, es por eso que se debe contar con una

documentación actualizada para lograr identificar rápidamente los dispositivos conectados de manera correcta con sus ubicaciones, segmentaciones y relaciones para no comprometer la eficiencia operativa y la protección de la información.

Con el objetivo de cumplir la problemática actual se debe de completar un documento llamada “Registro de actualización de topología” y en caso de que se agregue, se modifique o elimine un dispositivo, se debe incluir la identificación de su ubicación por departamento, responsable, fecha y motivo del cambio, además si es un nuevo dispositivo en la red es importante identificarlo con un nombre adecuado para en caso de algún incidente, se pueda detectar físicamente de manera rápida y así cumplir con una revisión de manera rápida.

Acción	Descripción del manejo documental	Objetivo del cumplimiento
Registro de actualización de topología	Documento que se completa cada vez que se agrega, modifica o elimina un dispositivo. Incluye ubicación, responsable, fecha y motivo del cambio.	Evita pérdida de trazabilidad y permite identificar cambios en la infraestructura.
Diagrama físico de red	Generado automáticamente por la Dream Machine y complementado manualmente si hay dispositivos no detectados.	Mejora la visibilidad de la infraestructura y facilita la respuesta ante fallos físicos.
Diagrama lógico de red	Incluye segmentación por VLANs, rutas de comunicación, accesos VPN.	Permite una administración eficiente del tráfico y mejora

Acción	Descripción del manejo documental	Objetivo del cumplimiento
	Validado por el departamento de TI y archivado con control de versiones.	la seguridad por segmentación.
Acta de revisión semestral	Documento firmado por el jefe de TI que valida la revisión y actualización de los diagramas físicos y lógicos.	Garantiza cumplimiento normativo y evita obsolescencia de la documentación.
Control de versiones	Cada modificación en los diagramas se archiva con su versión, fecha y responsable técnico.	Evita confusión entre versiones, facilita auditorías y mantiene historial de cambios.
Integración con ERP	Los cambios documentados se registran también en el sistema ERP en el módulo de activos, para trazabilidad cruzada.	Asegura consistencia entre sistemas y mejora la gestión de activos tecnológicos.

Definiciones

- **Topología de red física:** Representación gráfica que indica la ubicación física de los dispositivos de red y cómo están conectados entre sí, incluyendo routers, switches, firewalls, servidores y puntos de acceso.
- **Topología de red lógica:** Representación de la estructura de la red desde el punto de vista de comunicación y segmentación, mostrando subredes, VLANs, rutas y jerarquía de accesos.
- **Diagramas de red:** Esquemas gráficos que representan la infraestructura tecnológica de la organización, tanto física como lógica, para facilitar la administración, control y auditoría de la red.
- **Segmentación de red:** Proceso de dividir la red en segmentos o subredes para mejorar la seguridad, el rendimiento y la administración de los recursos tecnológicos.

- **Cambio significativo en infraestructura:** Modificación que impacta la conectividad, la seguridad o la configuración de la red, como instalación de nuevos switches, routers, enlaces VPN o actualización de firewalls.
- **Dream Machine:** Dispositivo firewall y de gestión de red que permite visualizar en tiempo real la topología física y lógica de la red.

Abreviaturas

- **TI:** Tecnologías de la Información
- **VPN:** Virtual Private Network
- **VLAN:** Virtual Local Area Network
- **ISO/IEC 27001:** Norma internacional de gestión de seguridad de la información
- **FW:** Firewall

La presente política aplica tanto para el diseño inicial de la topología como para cualquier modificación, reestructuración o expansión que afecte la infraestructura de red, su cumplimiento es obligatorio para el personal del departamento de TI y para cualquier proveedor externo autorizado que intervenga en la infraestructura tecnológica de la organización, asegurando así un control uniforme y seguro de los recursos tecnológicos en toda la empresa.

Normativa

Un estándar internacional para la gestión de la seguridad de la información lo brinda la ISO:27001 ayudando a cumplir con los requisitos legales y regulatorios mejorando la confianza el cliente, para este procedimiento el control de la norma 8.9 se enfoca en que las empresas establezcan procedimientos internos en configuraciones claves en seguridad, este apartado de la norma busca establecer medidas para restringir el acceso no autorizado a la infraestructura de la red, es por eso que una correcta segmentación lógica y su documentación en la topología contribuyen a uno de los cumplimientos de este requisito.

En el control de la norma 7.1 hace énfasis en identificar y controlar todos los activos, incluyendo dispositivos de red, router, switches, firewalls, servidores, los cuales deben estar documentados en los diagramas de red ayudando a mantener de una manera visual un inventario gráfico y actualizado.

Matriz de roles

La adecuada administración de la topología de red necesita una asignación precisa de responsabilidades dentro del equipo técnico de ThermoSolutions Group S.A., para garantizar que los esquemas representen con exactitud la infraestructura existente, se mantengan al día y se administren bajo los estándares de seguridad.

El departamento de Tecnologías de la Información es el principal responsable de diseñar, documentar y mantener actualizadas tanto la topología física como la topología lógica de la red, esta labor implica la elaboración de los diagramas y la verificación de su alineación con la arquitectura real de la infraestructura, así como la implementación de segmentaciones de red que cumplan con los controles y políticas de seguridad establecidas por la organización, especialmente aquellos que buscan limitar el alcance de incidentes, proteger los datos sensibles y facilitar el monitoreo eficiente.

El jefe del departamento de TI tiene la responsabilidad de supervisar la integridad, confidencialidad y disponibilidad de los diagramas de red, siendo la única persona en autorizar cualquier modificación en los diagramas, revisar de manera periódica la consistencia de los esquemas con respecto a la infraestructura real y garantizar que los diagramas sean almacenados de forma segura, con acceso controlado y registro de versiones anteriores para fines de auditoría o recuperación.

Actividad	**Ejecuta**	**Aprueba**	**Supervisa**	**Informado**
Levantamiento de información	TI	Jefatura TI	Auditoría	Gerencia
Diagramación de topología	TI	Gerencia TI	Auditoría	Gerencia
Validación de la topología	TI Proveedor	Gerencia TI	Auditoría	Gerencia
Actualización periódica	TI	Jefatura TI	Auditoría	Gerencia

Actividad	Ejecuta	Aprueba	Supervisa	Informado
Archivo y resguardo	TI	Jefatura TI	Auditoría	Gerencia

Desarrollo

Se presentan dos tipos de diagramas:

- Topologías físicas: muestra ubicación y las conexiones especificas entre dispositivos.
- topología lógica: Muestra la estructura lógica de la comunicación, subredes, Vlans y rutas.

El diagrama se podrá visualizar a tiempo real en el dispositivo firewall llamada dream machine, con el cual a la empresa ya cuenta y será útil tanto para las topologías como para detectar posibles fallos en la red, permitiendo identificar los puntos de conexión de una manera rápida y eficiente.

Actualización de los diagramas

Toda modificación que deba realizarse a los diagramas debe ser documentada y autorizada por el jefe de TI, revisándose al menos una vez cada seis meses o durante cualquier cambio significativo en la infraestructura, guardando las versiones anteriores como copias para un control de cambios.

Historial de revisiones de este documento

Rev.	Fecha de edición	Descripción
01	02/06/2025	Creación de documento inicial

Topología Lógica

El diseño lógico de la red nos muestra que la red de ThermoSolutions utiliza una arquitectura centralizada y segmentada, lo cual fortalece el control y rendimiento, las oficinas centrales ubicadas en santa Ana ofrece el control y la seguridad de los datos donde se establece la conexión segura hacia las distintas sucursales mediante una VPN site-to-site con las ubicaciones en Heredia, Liberia y Curridabat, por otra parte la red lógica se encuentra segmentada por medio de VLANs lo cual permite una adecuada segregación del tráfico según el tipo de servicio o área lo que refuerza los principios de confidencialidad, integridad y disponibilidad de la información.

A continuación, se presenta una tabla que muestra la configuración actual de las VLANs.

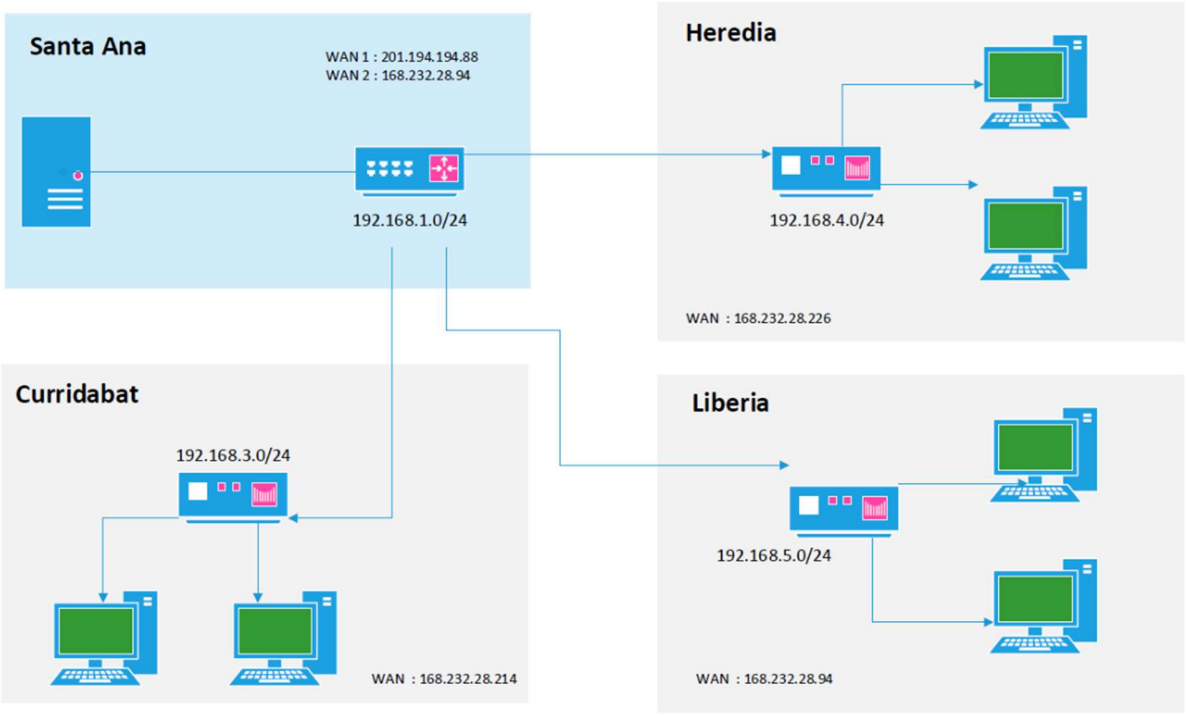
Tabla1

Resumen de vlans.

VLAN	Propósito	Rango de red
VLAN_DEFAULT	Administración general	192.168.1.0/24
VLAN_USER	Dispositivos de usuarios	192.168.20.0/24
VLAN_SECURITY	Equipos de seguridad (cámaras, control de acceso)	192.168.15.0/24
VLAN_VOIP	Telefonía IP	192.168.25.0/24

Elaboración Propia

Topología lógica, Vlan’s sucursales



Elaboración Propia

En cuanto a la topología lógica el firewall ofrece funcionalidades en cuanto a segmentación de la red por medio de VLANS, asignación de puertos específicos, políticas de control de tráfico hacia/desde internet, reglas direccionamiento IP, protocolos de puertos y aplicaciones, además permite aislar los dispositivos en una misma red o VLAN.

Con respecto a los dispositivos de red, mediante el sistema actual del firewall podemos observar a tiempo real el comportamiento y direccionamiento de cada uno de los dispositivos conectados a la red, como los access point que brindan señal inalámbrica a los distintos departamentos de la organización, para un total de once unidades que se detallan en la siguiente imagen capturada desde el dispositivo dream machine obteniendo como resultado el nombre, estado actual, dirección IP y dispositivo principal al cual están conectados.

Tipo	Nombre	Estado	Versi...	Dirección IP	Dispositivo principal
	SALA CAPACITACION- UAP-AC-Lite	Actualizado	6.6.77	192.168.1.56	USW-48-PoE #21
	PISO 1 - UAP-AC-Lite	Actualizado	6.6.77	192.168.1.78	USW-16-PoE-SSA #6
	PRODUCCION - UAP-AC-Lite	Actualizado	6.6.77	192.168.1.71	THERMOSOLUTIONS_SANTA_ANA-... #2
	BODEGA - UAP-AC-LR	Actualizado	6.6.77	192.168.1.60	USW-16-PoE-MP #8
	SALA JUNTAS - UAP-AC-Pro	Actualizado	6.6.77	192.168.1.59	USW-16-PoE-SSA #8
	AC Pro_2do Piso Presidencia	Actualizado	6.6.77	192.168.1.95	USW-24-PoE #12
	U6 Lite Comedor	Actualizado	6.7.17	192.168.1.121	USW-24-PoE #14
	SEGURIDAD-U6-LR	Actualizado	6.7.17	192.168.15.253	USW-24-PoE #8
	PISO 2 -U6-LR	Actualizado	6.7.17	192.168.1.237	THERMOSOLUTIONS_SANTA_ANA-... #6
	U6 Pro_1er Piso Anexo	Actualizado	6.6.77	192.168.1.247	USW-16-PoE_1er Piso Anexo #1
	U6 Pro_2do Piso Anexo	Actualizado	6.6.77	192.168.1.92	USW-16-PoE_2do Piso Anexo #1

Conmutadores conectados y administrados en la red

Topología	Nombre	Estado	Versión	Dirección IP	Dispositivo principal
	USW-16-PoE-PT	Actualizado	7.1.26	192.168.1.133	USW-24-PoE #4
	USW-16-PoE_1er Piso Anexo	Actualizado	7.1.26	192.168.1.137	THERMOSOLUTIONS_SANTA_ANA-UDM... #5
	USW-16-PoE_2do Piso Anexo	Actualizado	7.1.26	192.168.1.191	THERMOSOLUTIONS_SANTA_ANA-UDM... #3
	USW-16-PoE-MP	Actualizado	7.1.26	192.168.1.131	USW-Lite-8-PoE-Filtros #8
	USW-16-PoE-SSA	Actualizado	7.1.26	192.168.1.104	USW-24-PoE #6
	USW-24-PoE	Actualizado	7.1.26	192.168.1.35	THERMOSOLUTIONS_SANTA_ANA-UDM... #7
	USW-48-PoE	Actualizado	7.1.26	192.168.1.36	THERMOSOLUTIONS_SANTA_ANA-UDM... #1
	USW-Lite-8-PoE-MP	Actualizado	7.1.26	192.168.1.180	USW-16-PoE-MP #9
	USW-Lite-8-PoE-Filtros	Actualizado	7.1.26	192.168.1.194	USW-16-PoE-MP #1

Topología física

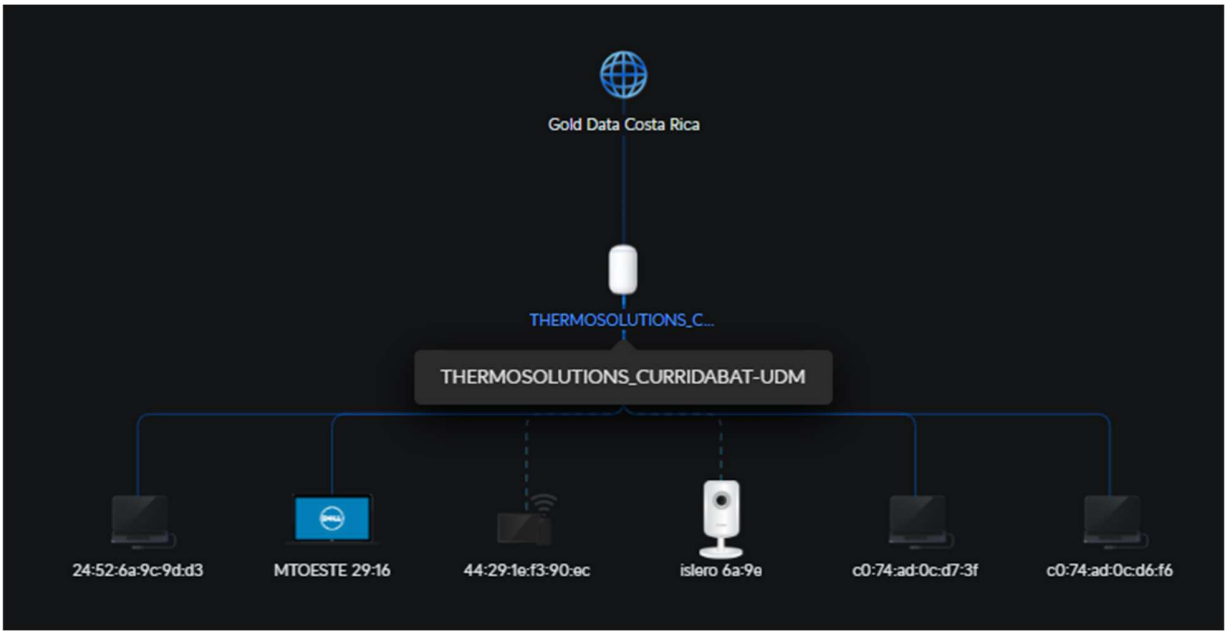
Durante la revisión de la infraestructura tecnológica, se identifica que cada rea o departamento cuenta con su propio switch como punto de red, esto permite una mejor segmentación de la red y tiempos de respuestas más rápidos ante un posible incidente o falla ya que esta distribución mejora el rendimiento loca y apoya la disponibilidad del servicio, lo cual viene a cumplir con el requisito de la norma ISO en el control 8.9, sin embargo se detectaron debilidades con las puertas abiertas de los gabinetes o con las llaves pegadas en las cerraduras lo que facilita el acceso no autorizado a cualquiera de estos dispositivos por parte de cualquier persona, esta situación compromete la integridad y la confidencialidad de la red.

Algunas de las recomendaciones que cumplen con los requisitos de la norma de la protección de redes de la ISO/IEC:27001 son:

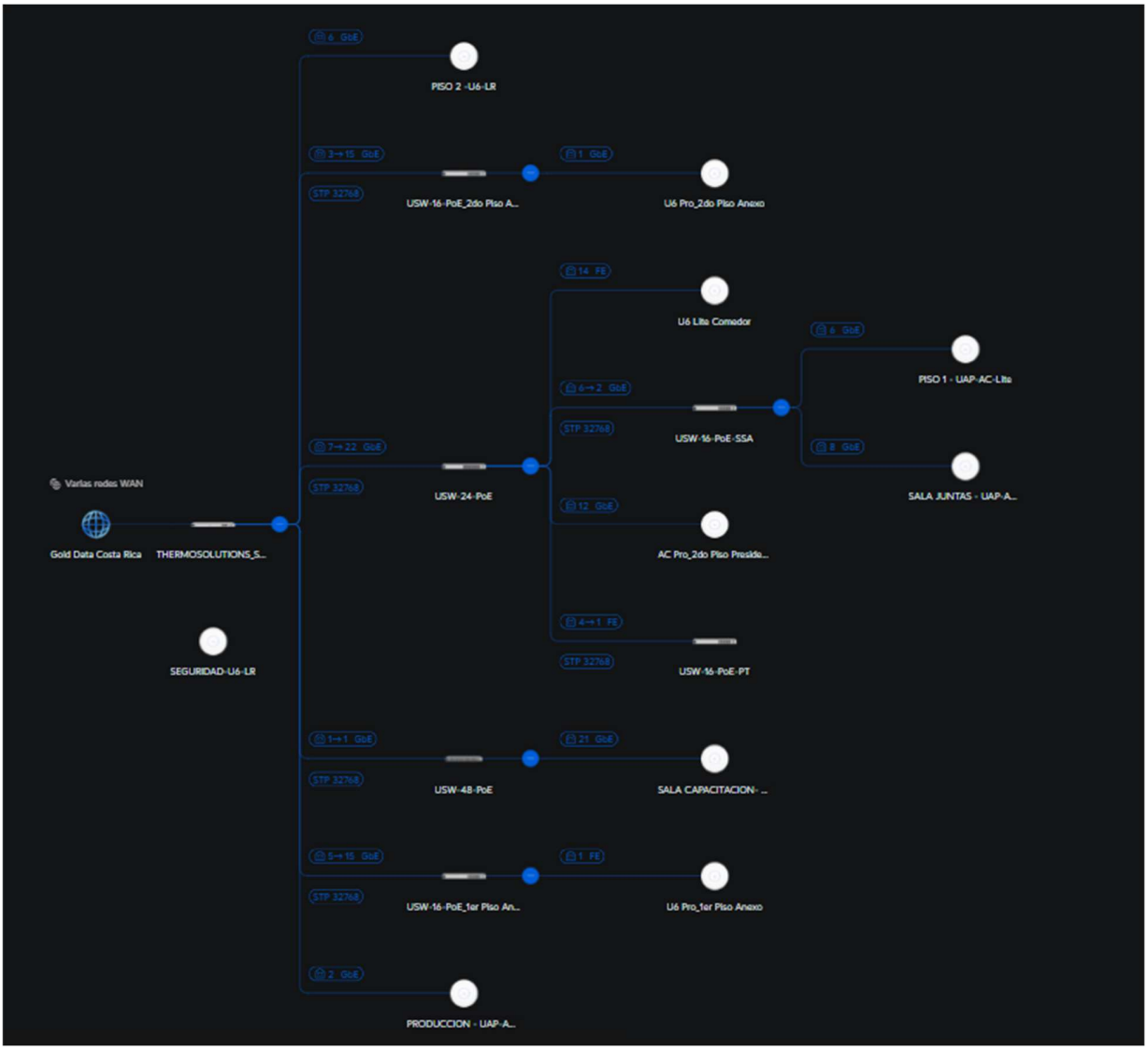
- Hay que asegurar que todos los dispositivos estén de manera segura, lo que implica mantener los gabinetes cerrados con llave.
- Retirar las llaves de las cerraduras y mantenerlos bajo custodia controlada en poder del encargado de TI.
- Documentar hallazgos y tomar decisiones correctivas inmediata si se detectan desviaciones.

El firewall permite visualizar y gestionar la estructura física de la red mostrando como están conectados los dispositivos indicando su tipo de conexión ya sea inalámbrica o cableada, numero del puerto al que se encuentra conectado, con una topología a tiempo real de todos los dispositivos conectados a la red desde el Gateway hasta los dispositivos finales, además posee encendido y apagado remoto con el consumo por dispositivo y control de energía.

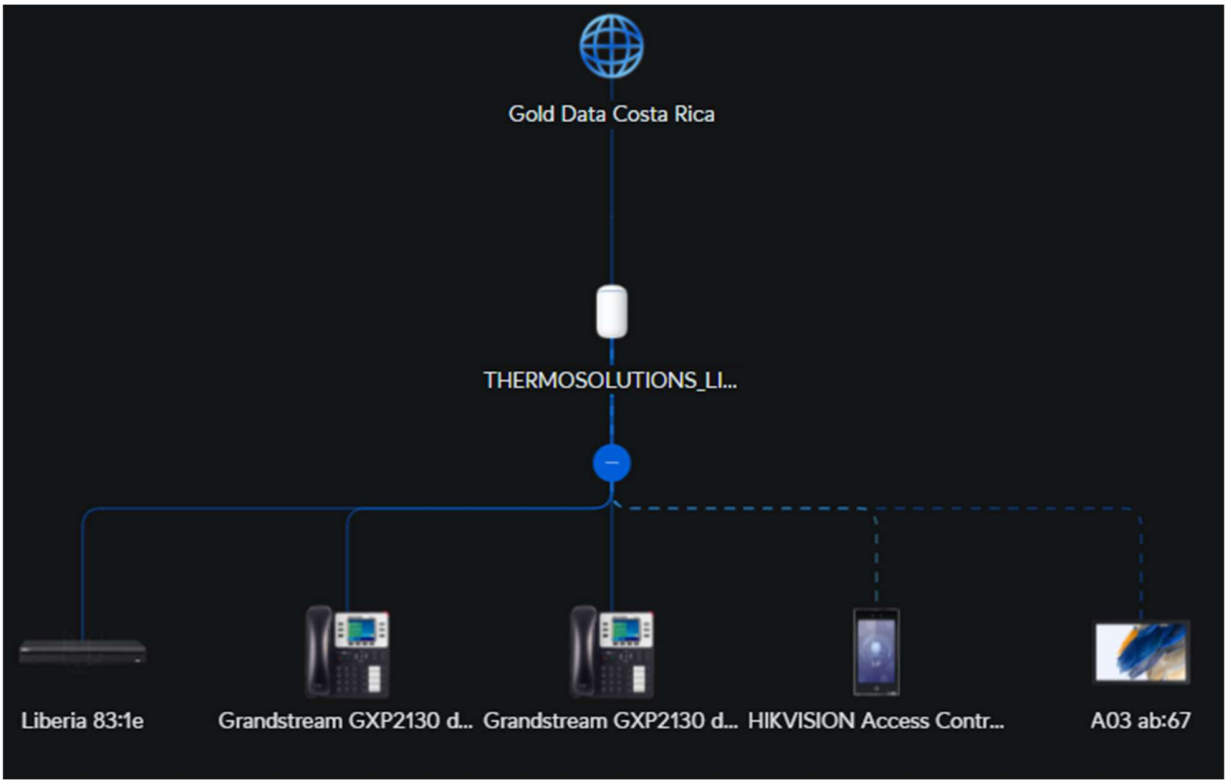
Topología física sucursal Curridabat



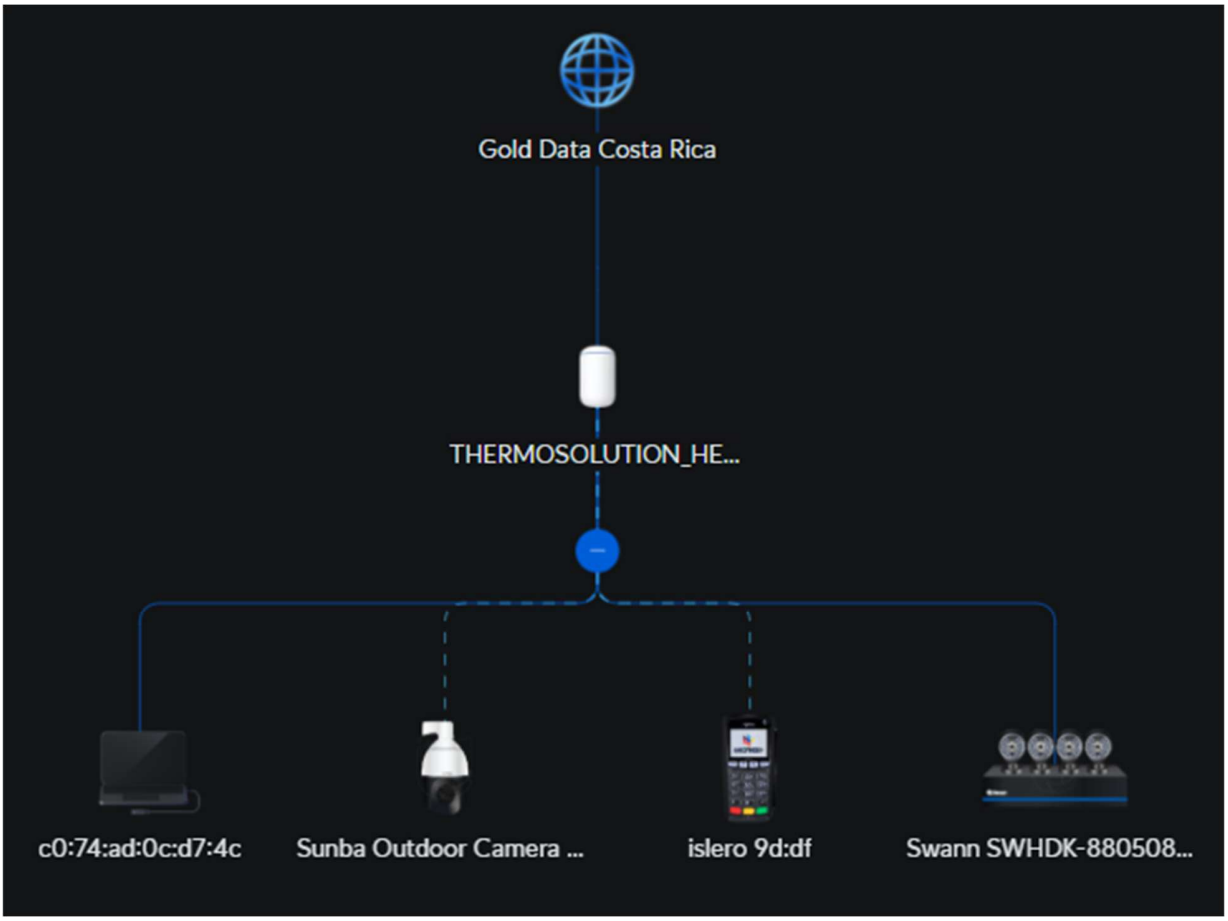
Topología física oficinas centrales



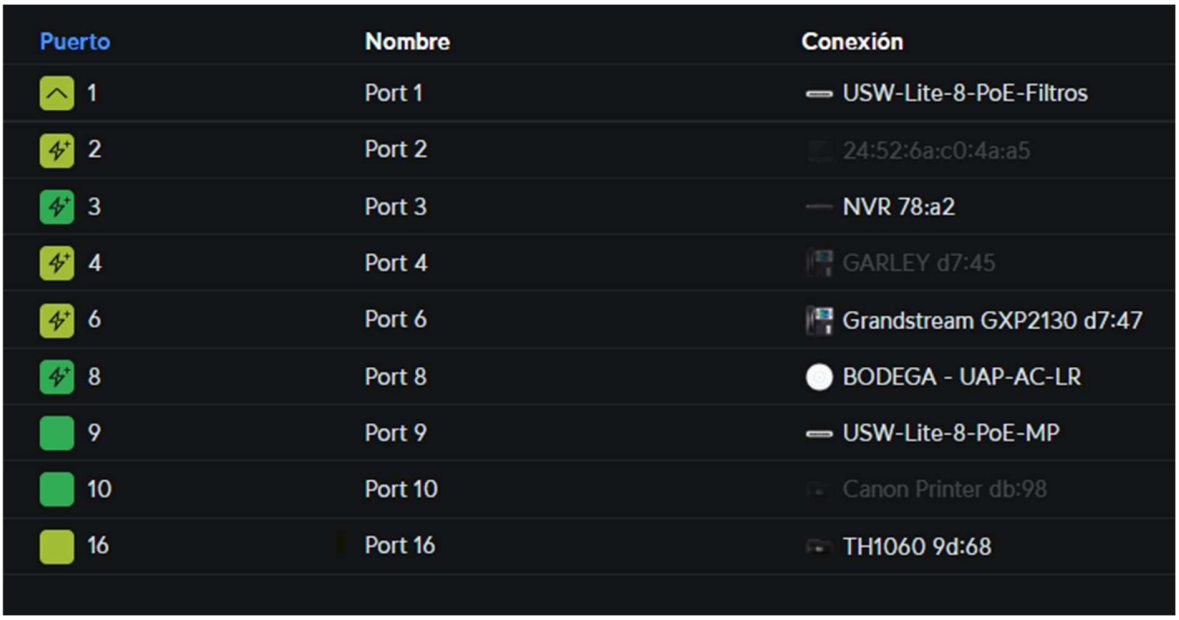
Topología física sucursal Liberia



Topología física sucursal Heredia



A continuación, se muestra un ejemplo de la administración de un switch y los dispositivos conectados actualmente.



Puerto	Nombre	Conexión
1	Port 1	USW-Lite-8-PoE-Filtros
2	Port 2	24:52:6a:c0:4a:a5
3	Port 3	NVR 78:a2
4	Port 4	GARLEY d7:45
6	Port 6	Grandstream GXP2130 d7:47
8	Port 8	BODEGA - UAP-AC-LR
9	Port 9	USW-Lite-8-PoE-MP
10	Port 10	Canon Printer db:98
16	Port 16	TH1060 9d:68

PROCEDIMIENTO DE EVIDENCIA DE CONTROL Y ACTUALIZACIÓN DE TOPOLOGÍAS DE RED

Nombre del documento: Evidencia de actualización de topologías de red

Versión: 1.0

Fecha:

Revisado por: [Nombre del Encargado de TI / Seguridad]

El presente documento sirve como evidencia del cumplimiento del procedimiento de actualización, donde se establece la gestión y control de las topologías física y lógica en ThermoSolutions Group.

Se deben detallar las actualizaciones recientes, validaciones realizadas y archivos anexos correspondientes.

Tipo Topología (Física-Lógica)	Descripción del Cambio	Responsable del cambio	Evidencia adjunta

Validación de los diagramas actualizados

Archivo	Fecha Actualización	Verificado por	Estado (Aprobado-Rechazado)

Observaciones

Firma TI: _____ **Firma RH: _____**