ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TESIS DE GRADO

"DISEÑO DE UN ESQUEMA DE AUDITORÍA EN SEGURIDAD INFORMÁTICA EN LOS CONTROLES DE ACCESO A LOS ACTIVOS DE INFORMACIÓN BAJO LOS LINEAMIENTOS DE LA NORMA ISO 27001 PARA UNA EMPRESA DE INDUSTRIA AUTOMOTRIZ."

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA

Presentado por:

ANGELA MERCEDES YANCE SALTOS

GUAYAQUIL – ECUADOR

2024

AGRADECIMIENTO

Mi agradecimiento es a Dios por darme la inteligencia y sabiduría de enfrentar todos los obstáculos para llegar a la meta y a mi esposo quien me apoyó constantemente en todas mis decisiones y fue un pilar fundamental en muchas ocasiones para poder culminar este logro tan anhelado.

Asimismo, quiero agradecer a mi tutor por su valiosa ayuda en la orientación y desarrollo de este proyecto.

A mi familia en general por brindarme su apoyo incondicional.

DEDICATORIA

A mi padre celestial, el que me acompaña siempre en mis buenos y malos momentos y me da fortaleza para levantarme cada día, Dios; a mi esposo por su gran apoyo incondicional y a mi familia, por su constante acompañamiento emocional y espiritual.

TRIBUNAL DE SUSTENTACIÓN

……..

Ing, Lenin Freire C., MSIG

COORDINADOR MSIG / MSIA

……..

Ing, Lenin Freire C., MSIG

DIRECTOR DEL TRABAJO DE TITULACIÓN

……..

Lic. Juan Carlos García., MSIG

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL”

(Reglamento de Graduación de la ESPOL)

RESUMEN

El presente trabajo de titulación tiene como objetivo principal Diseñar un esquema de una auditoría de seguridad informática en los controles de acceso a los activos de información con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación y recomendaciones de seguridad y controles que incorpore estándares ajustados a la seguridad como lo es la norma ISO 27001 enfocado a una empresa de industria automotriz.

Se desarrolló bajo la modalidad de estudios, investigaciones y experiencia laboral siguiendo una metodología del modelo Ciclo de Deming y de los lineamientos de la Norma ISO 27001 enfocada en el dominio del control de accesos, el cual permitió la elaboración de un buen esquema que será útil para próximas auditorías y a distintas empresas.

Este estudio consta de cinco capítulos en los cuales se desarrolla cada tema que permite elaborar un esquema para realizar una buena auditoría informática: el Capítulo 1, conformado por el antecedente, descripción y solución del problema, incluyendo los objetivos primarios y secundarios, y la metodología a seguir para la estructura del diseño. Capítulo 2, denominado Marco Teórico, en el que contiene todas las bases teóricas para el respectivo diseño a realizar. Capítulo 3, consta del Diseño del Esquema del Alcance de la Auditoría a realizar, en el que contiene la respectiva descripción de las

fases del diseño. Capítulo 4, Diseño del esquema de desarrollo de la auditoría, conformado por los respectivos diseños que se aplicarían en la revisión de los documentos para la auditoría tales como el Documento de Calidad, Cláusulas de la Norma ISO 27001 y las Observaciones y No conformidades que podrían encontrarse en una auditoría informática. Capítulo 5, se exponen los resultados de la auditoría, revisiones posteriores, evaluación del diseño propuesto y las conclusiones y recomendaciones. Finalmente, se presentan las referencias bibliográficas y los anexos correspondientes.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOS

DA: Declaración de Aplicabilidad.

ISO: (Internacional Organization for Standardization) es la Organización Internacional de Normalización, cuya principal actividad es la elaboración de normas técnicas internacionales.

SI: Sistemas Informáticos.

SGSI: Sistema de Gestión de Seguridad de la Información.

TAACS: Son técnicas de auditoría asistidas por computadora en las cuales se emplean procedimientos de auditoría con el ordenador, el cual se obtiene información precisa y ahorra tiempo al auditor.

TI: Tecnología de Información.

TIC: Tecnologías Informáticas y de las Comunicaciones.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad informática se ha convertido en un aspecto crítico en el panorama actual de la TI, hemos visto que, con el aumento de las amenazas cibernéticas y la creciente dependencia de los activos de información en las organizaciones, es imperativo establecer fuertes controles de acceso para proteger estos activos.

Los controles de acceso no solo se refieren a la gestión de contraseñas y la autenticación de usuarios, sino que abarcan un conjunto más amplio de medidas diseñadas para regular y monitorear el acceso a los activos de información, esto incluye la implementación de políticas de acceso, la asignación de privilegios adecuados, la gestión de identidades, entre otros aspectos.

En este sentido la auditoría informática se presenta como una herramienta esencial para evaluar la efectividad de estos controles y garantizar el cumplimiento de los requisitos establecidos por la norma ISO 27001.

Por tanto, la auditoría informática y la seguridad informática son dos aspectos fundamentales en la gestión de la TI de cualquier organización y ambas se encuentran estrechamente relacionadas. Mientras la auditoría informática se enfoca en evaluar y mejorar los controles y procesos relacionados con la TI, la seguridad informática se centra en proteger los activos de información; por

lo que, son vitales para garantizar la integridad, confidencialidad y disponibilidad de los activos de información, y a su vez nos ayudan a protegerlos contra amenazas internas y externas. [1]

En este contexto, es importante comprender también los principios y directrices establecidos por la norma ISO 27001 para controlar el acceso a los activos de información y los requisitos específicos que estos controles deben cumplir para garantizar su seguridad.

Además, se deben diseñar esquemas de auditoría que puedan evaluar de manera sistemática y exhaustiva la implementación y funcionalidad de estos controles e identificar posibles deficiencias y áreas de mejora.

Por tanto, el objetivo del presente documento es proporcionar un marco conceptual y metodológico para el diseño de un esquema de auditoría de seguridad informática en el control de acceso a los activos de información, según los lineamientos de la norma ISO 27001.

Se cubren los principales aspectos de la auditoría en el campo de la seguridad de la información, control de acceso y seguridad informática y se propone un plan de auditoría basado en las mejores prácticas y estándares internacionales en la materia.

Además, para llevar a cabo esta tarea, es importante indicar que se debe contar con un enfoque metodológico sólido que permita una adecuada planificación, ejecución y documentación del proceso de auditoría, y considerar las mejores prácticas y estándares internacionales para la auditoría de seguridad informática, así como las herramientas y técnicas disponibles para realizar una evaluación integral de los controles de acceso a los activos de información.

Diseñar un esquema de auditoría de seguridad informática para controlar el acceso a los recursos de información según los lineamientos de la norma ISO 27001 es una tarea esencial para garantizar la efectividad y adecuación de los controles implementados dentro de una organización, que en el caso del presente documento se tomará como referencia a una empresa de industria automotriz.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La empresa de industria automotriz es una empresa que se compromete con la visión de movilidad para todos, mientras persiguen su misión que es la de producir felicidad para todos basándose en los valores, y así construir una sociedad en el camino impulsado por cada uno de sus empleados, es decir que se caracteriza por mantener contentos a sus empleados y clientes, además de ofrecer un buen producto de calidad con excelente seguridad, por tanto para salvaguardarlos deben tener en cuenta muchos factores que no están claros a la actualidad, y es por ello que se propone este diseño para que les sirva de ayuda para buscar las

vulnerabilidades y asegurar los activos de información tanto de los clientes como de los usuarios que conforman la empresa.

1.2. Descripción del Problema

Hoy en día se sabe que la información es un activo muy valioso y de vital importancia en una organización, en el que sirve de mucha ayuda para la toma de decisiones en los niveles gerenciales, los costos derivados de la pérdida de la información no son sólo económicos directos, sino que también afectan a la imagen de la empresa [2]; es por ello que su acceso y control deben ser protegidos y asegurados de tal manera que no pueda ser divulgada, accedida accidentalmente o ilegalmente por usuarios sin la debida autorización.

Además, se sabe que la auditoría informática nos permite la revisión y la evaluación de controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de información con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

Existen muchas empresas públicas o privadas que no les dan importancia a las auditorías informáticas principalmente por dos factores; el primero el alto costo resultante de este proceso y el segundo y de mayor peso es el desconocimiento, puesto que se piensa “es el método

para evaluar al personal y por ende el removimiento del cargo", lo cual no es de agrado para ningún colaborador de cualquier organización. [3]

Considerando lo anteriormente dicho la empresa de industria automotriz, es una organización que día a día va creciendo paulatinamente, y es consciente que la información que se maneja debe estar protegida y controlada; también tiene conocimiento de que no se cuenta con los mecanismos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información al 100%; ya que no tienen identificado, ni estandarizado qué controles y qué procesos son los más relevantes para el control de acceso a los activos de información, y por esta razón tienen la necesidad de realizar una auditoría de seguridad informática en los controles de acceso a los activos de información con el fin de garantizar los tres pilares de la seguridad de la información basados en la norma ISO 27001, para evitar correr el riesgo de exponer la información para que sea alterada, degradada o extraviada; debido a que no se han enfocado en la seguridad de la información ni en realizar auditorías internas para poder identificar estas falencias que poseen a la actualidad los procesos críticos de la organización.

1.3. Solución Propuesta

Se puede mencionar que, luego de abordar la problemática que existe actualmente en la empresa de industria automotriz se ha planteado

diseñar un esquema de auditoría informática que permita proporcionar un reporte donde se detallen los puntos críticos en el dominio de control de acceso de acuerdo con la Norma ISO 27001 y así poder tomar las correctas medidas preventivas y correctivas para asegurar la confidencialidad, integridad y disponibilidad de los activos de información en ese dominio.

Se ha tomado en consideración dentro del diseño el dominio del Control de acceso de acuerdo a la norma ISO 27001 porque este es un arma de seguridad muy poderosa que sirve de barrera para evitar accesos no autorizados a información de cualquier organización, además la tarea de salvaguardar la información confidencial de la propia organización y de los clientes, se complica en ciertas ocasiones, puesto que, se tiene bastante personal especializado en las distintas áreas de informática y otras áreas, por las cuales hay que asegurarse que cada persona tenga su acceso de acuerdo sus roles, funciones y responsabilidades del cargo.

Adicionalmente sabemos que uno de los principales motivos por los que se necesitan los controles de acceso es porque se vive en un periodo donde la tecnología está avanzando con el pasar del tiempo y esto produce que aumente las posibilidades de ser atacados por algún tipo de brecha en la seguridad de manera discreta o indiscreta, mucho más en la actualidad en donde nos vemos expuestos a más vulnerabilidades por el

tema ocasionado por la pandemia, en donde el trabajo empezó a realizarse de forma remota.

Para la ejecución de esta propuesta se contará con los recursos obtenidos durante mi experiencia laboral e investigaciones realizadas durante este trayecto en los procesos establecidos para el control de acceso a los activos de información, para realizar la identificación y evaluación de los controles de acuerdo con la norma establecida.

1.4. Objetivo general

Diseñar un esquema de una auditoría de seguridad informática en los controles de acceso a los activos de información con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación y recomendaciones de seguridad y controles basados en la norma ISO 27001.

1.5. Objetivos específicos

- Conceptualizar la importancia de realizar un esquema de auditoría informática, control de accesos a los activos de información e implementación de la norma ISO 27001.

- Proporcionar un estándar y/o herramienta básica para realizar auditorías efectivas y eficientes de sus controles de seguridad enfocándose en el dominio de la Norma ISO 27001 “Control de

Acceso”, y así asegurar la protección de los activos de información de una empresa automotriz.

- Recomendar lineamientos de seguridad en los controles de acceso a los activos de información.

1.6. Metodología

De acuerdo con el problema planteado la metodología que se va a seguir para diseñar el esquema de auditoría informática alineada a la norma ISO 27001 es la descriptiva, puesto que se hará énfasis en la importancia y estructura que conlleva una auditoria informática respecto al dominio de control de acceso a los activos de información de la organización, y se seguirá además el modelo llamado Ciclo de Deming (PLAN-DO-CHECK-ACT), Ver *Figura 1.1*

Figura 1.1: Etapas del Ciclo de Deming
Fuente: Autor

- ✓ PLAN: Planificar.
- ✓ DO: Hacer.
- ✓ CHECK: Chequear.
- ✓ ACT: Actuar.

Fase "Planificar": Incluirá el esquema de alcance, objetivos e identificación de los activos de información para alcanzar las metas establecidas en la auditoría.

Fase "Hacer": Incluirá el esquema de revisión y análisis de los controles establecidos de acuerdo con la norma ISO 27001.

Fase "Chequear": Incluirá el esquema de la revisión más exhaustiva de las técnicas/herramientas usadas para la revisión de controles encontrados en el proceso de la auditoría.

Fase "Actuar": Incluirá el esquema de las observaciones y no conformidades del diseño de la auditoría.

Para realizar el diseño del esquema de la auditoría se utilizará diferentes tipos de investigación, la Investigación de Campo y la Investigación Interpretativa y Explicativa.

Las técnicas que se utilizarán para el diseño de la auditoría serán:

Técnica de Verificación Verbal.

Encuesta. - Es útil para recopilar información de un gran universo de datos o grupos de personas.

Entrevista. - Pueden ser efectuadas al personal de la empresa auditada o personas beneficiadas de los programas o actividades a su cargo.

Técnica de Verificación Escrita.

Análisis. - Separa en elementos o partes las transacciones u operaciones que están sometidas a examen.

Conciliación. - Hacer coincidir o que concuerden dos conjuntos de datos seleccionados, separados o independientes.

Técnica de Verificación Documental.

Comprobación. - Examinar verificando la evidencia que apoya a una transacción u operación, demostrando autoridad, legalidad, propiedad y certidumbre.

Técnica de Verificación Física.

Inspección. - Examen físico y ocular de activos, documentos, valores con el objeto de demostrar su existencia y autenticidad.

Los Instrumentos por utilizar serán:

- ✓ Cuestionarios para entrevistas.
- ✓ Observación.
- ✓ Checklist.[3]

CAPÍTULO 2

MARCO TEÓRICO

2.1. Seguridad Informática

La seguridad informática protege la integridad y confidencialidad de la información almacenada en los sistemas informáticos, minimizando los riesgos tanto físicos como lógicos, con base en políticas y estándares internos y externos de la empresa, siendo este el campo responsable de proteger contra amenazas a las que está expuesta.[4]

2.2. Auditoría Informática.

Es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo

discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados.

En esta definición hay palabras que destacan sobremanera: examen, metódico, puntual, discontinuo. Esta relevancia podría justificarse diciendo que la auditoría informática es un examen, pues debe partir de una situación dada; que este es metódico, puesto que seguirá un plan de trabajo perfectamente sistematizado que permite llegar a conclusiones suficientemente fundamentadas (conclusión ésta exigible a cualquier auditoría); que es puntual, ya que se da en un corte en el calendario para llevarla a cabo, y que es discontinua, extraña al servicio de informática, en aras de buscar la objetividad requerida, por lo que será ejecutada por personas ajenas al departamento independientes de las funciones a auditar. [5]

2.2.1. Objetivo de la Auditoría Informática.

El propósito de la auditoría informática es garantizar que los sistemas informáticos protejan los activos (hardware y software), mantengan la integridad de los datos y logren su misión y visión mediante el uso eficiente y eficaz de los recursos informáticos, recopilando, agrupando y evaluando evidencia para determinar si las empresas contribuyen. De igual forma, verifica el estricto cumplimiento de las normas y leyes pertinentes y el manejo

efectivo de todas las TIC en poder de la organización en general. [4]

2.2.2. Tipos de auditoría informática.

Existen 2 tipos de auditoría informática:

Auditoría Informática Interna: Una auditoría informática interna es realizada por empleados dentro de una organización con el propósito de evaluar los controles internos, la eficiencia operativa y el cumplimiento de las políticas y procedimientos de seguridad establecidos.

Auditoría Informática Externa: Una auditoría informática externa es realizada por una organización independiente de la organización encargada de garantizar el cumplimiento de la seguridad de la información, los controles internos y las regulaciones externas, tales como: leyes y regulaciones del sector.[1]

2.2.3. Importancia de la Auditoría Informática

La importancia de las auditorías informáticas radican en que permiten determinar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de la configuración de la plataforma

informática, el nivel de calidad de los servicios prestados por la unidad encargada y la situación de los contratos con proveedores de productos y servicios, entre otros aspectos, todo ello en el ámbito del uso y aplicación de las TIC en la organización. [6]

Además, permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización, es por ello que se hace énfasis en la revisión independiente, puesto que, el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de esta.

2.3. Norma ISO 27001.

La Norma ISO 27001 es el único estándar aceptado a nivel internacional para proveernos las reglas de la seguridad de la información, pero como cualquier norma ha tenido su evolución para llegar a lo que es ahora. [6]

La ISO 27001 seguridad de la información, es un estándar que nos brinda una serie de pasos a seguir para contar con planes de contingencia, normas legales, lineamiento para la protección de la información que se maneja diariamente en las empresas.

2.3.1. Importancia de la ISO 27001.

La importancia de implementar la ISO 27001 seguridad de sistemas es demostrar, que al aplicar dicho estándar obtendremos mayores beneficios, dada la evolución que ha tenido el manejo de la información y los riesgos en aumento que vemos en los sistemas de seguridad se hace necesario, sino indispensable contar con un Plan de seguridad de sistemas efectivos, y dado que el estándar anteriormente mencionado es altamente recomendado y utilizado, nos basaremos en él.

2.3.2. Anexo A de la Norma ISO 27001:2013.

En el Anexo A se incluyen los objetivos de control y controles enumerados del 5 al 18, que se encuentran basados en la ISO/IEC 27002:2013, las cuales se encuentran alineadas con ella y se deben usar en contexto con la Norma ISO 27001.

A continuación, se visualiza en la *Tabla 2.1* el dominio que se usará en el presente documento:

A.9 CONTROL DE ACCESO	
A.9.1 Requisitos del negocio para control de acceso.	
Objetivo: Limitar el acceso a información y a instalaciones de procesamientos de información.	
A.9.1.1	Política de control de acceso.
A.9.1.2	Acceso a redes y a servicios en red.
A.9.2 Gestión de usuarios.	

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	
A.9.2.1	Registro y cancelación del registro de usuarios.
A.9.2.2	Suministro de acceso de usuarios.
A.9.2.3	Gestión de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios.
A.9.2.5	Revisión de los derechos de acceso de usuarios.
A.9.2.6	Retiro o ajuste de los derechos de acceso.
A.9.3 Responsabilidades de los usuarios.	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	
A.9.3.1	Uso de información de autenticación secreta.
A.9.4 Control de acceso a sistemas y aplicaciones.	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.	
A.9.4.1	Restricción de acceso a la información.

Tabla 2.1: Dominio "CONTROL DE ACCESO" del Anexo A de la ISO 27001
Fuente: Norma ISO 27001:2013

2.4. Activos de Información

Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

Los activos se encuentran relacionados, directa o indirectamente, con las demás entidades de acuerdo a la *Figura 2.1.*

Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, en los niveles de los subestados, confidencialidad, integridad y disponibilidad.

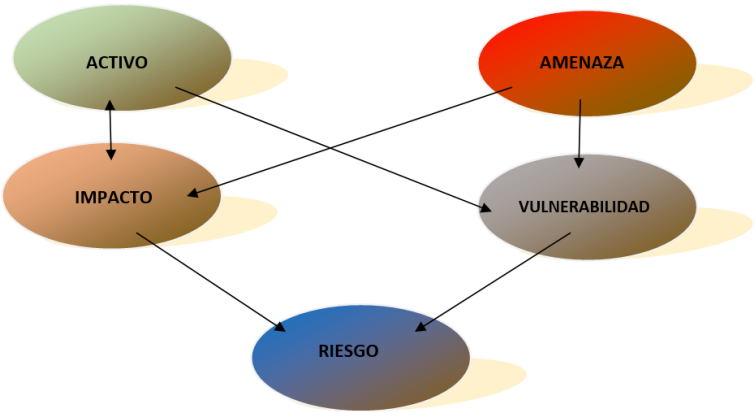

Figura 2.1: Relación de activos
Fuente: Autor

CAPÍTULO 3

DISEÑO DEL ESQUEMA DEL ALCANCE DE LA AUDITORÍA

Realizar el diseño del esquema del alcance de la auditoría es crucial y muy importante en la realización de cualquier auditoría, para asegurar que se cubran todos los aspectos relevantes y se pueda cumplir con todos los objetivos establecidos en la auditoría, es decir, debemos establecer los límites y restricciones para garantizar que la auditoría se realice de forma efectiva, enfocándose en los aspectos más relevantes y así evitar desviaciones innecesarias.

Para poder realizar el diseño del esquema del alcance de la auditoria en seguridad informática en los controles de acceso a los activos de información

bajo lineamiento de la Norma ISO 27001, es necesario y fundamental seguir un conjunto de pasos para obtener resultados efectivos, y así, establecer las áreas específicas que serán evaluadas durante la auditoría, por lo que, se debe definir claramente los objetivos de la auditoría y definir los límites del alcance, es decir, determinar qué sistemas y áreas se van a evaluar, para ello se debe tener un entendimiento claro del contexto organizacional de la empresa a la que se va a auditar, en donde se realiza la identificación de los procesos críticos que son primordiales para el funcionamiento de la organización, la identificación de los activos de información que se deben proteger, así como su nivel de criticidad a la que están expuestos. Además en este esquema del alcance se debe incluir la definición de objetivos específicos que se persiguen realizando la selección de controles necesarios (controles de acceso), y por último paso, pero no menos importante se lleva a cabo la revisión del documento de aplicabilidad, en donde se realiza una revisión minuciosa de todo el proceso y se verifica que se hayan cumplido todos los pasos anteriores.

Es por ello que cada uno de estos pasos juega un papel muy importante en el diseño del alcance de la auditoría y contribuye a garantizar la integridad y eficacia de este proceso, además de asegurar la efectividad de las medidas de seguridad implementadas.

3.1 Entendimiento del Contexto Organizacional:

Comprender el contexto de la organización es el primer paso significativo para diseñar el alcance de la auditoría de seguridad informática en los controles de acceso, porque se debe recopilar información relevante sobre la organización, como su misión, visión, valores, estructura organizacional incluyendo funciones tercerizadas y procesos clave más destacados.

No sólo se busca comprender a cabalidad la organización en sí, sino también su entorno, por ello también es importante conocer la industria en la que opera la empresa y los factores externos que pueden afectar la seguridad informática, todo esto con el objetivo de conocer sus particularidades y desafíos específicos en la seguridad informática.

Además de lo anteriormente dicho, se debe tener un contexto general de la TI de la organización, ya que eso permite conocer a la organización desde la TI, identificar los riesgos significativos y sobre esta base se sugiere el enfoque de la auditoría.

Se debe tener en cuenta que, los elementos del entendimiento deben ser claros, concisos y específicos, no es recomendable poner textos genéricos que no proporcionen un entendimiento apropiado de la organización, de la misma forma tampoco se debe extender innecesariamente.

Toda la información recopilada se debe manejar con memos (Ver *Anexo 1*) de las reuniones establecidas, incluyendo las evidencias revisadas en conjunto con la organización, se debe documentar los procedimientos aplicados para la obtención del entendimiento, incluyendo el nombre del auditor que realizó el trabajo y la fecha.

Este análisis proporciona una visión general del contexto en el que se realiza la auditoría y forma la base para definir los objetivos de la misma.

Por tanto para la realización de este esquema se tomará en consideración el organigrama estructural de una empresa de industria automotriz mostrado en la *Figura 3.1* y así poder avanzar con los siguientes pasos.

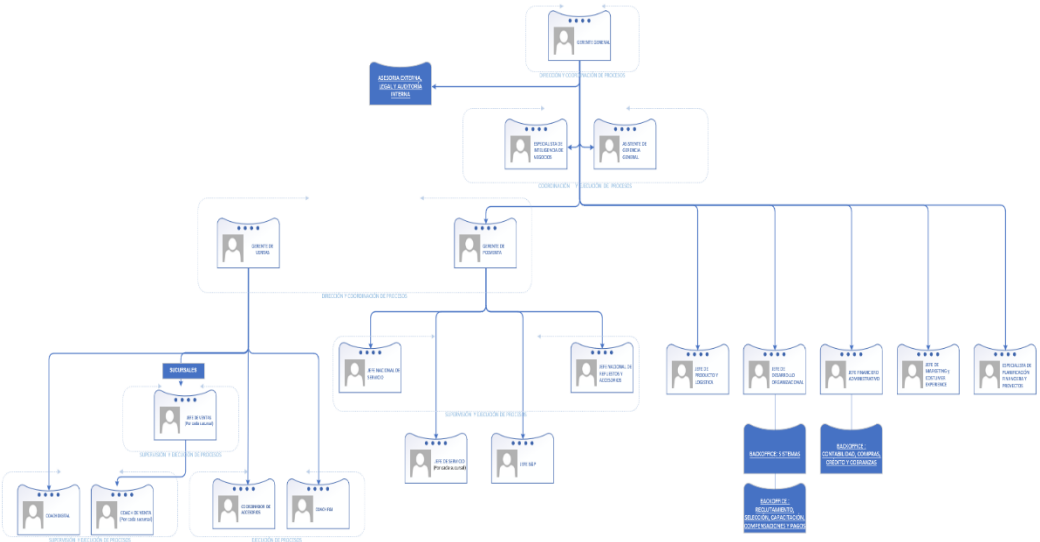

Figura 3.1: Organigrama empresarial de industria automotriz
Fuente: Autor

En este organigrama se visualiza que, su estructura organizacional no está estructurada jerárquicamente por cargos de alto mando, sino también por funciones y procesos, además se puede visualizar que el área de sistemas, recursos humanos, financiero y contabilidad lo maneja una empresa externa a la organización como un BACKOFFICE.

Por tanto en estos casos también se debe solicitar su estructura organizacional.

3.1.1 Identificación de Procesos Críticos:

Como parte del proceso de entendimiento del contexto organizacional se debe realizar la identificación de los procesos críticos de la organización que se van a auditar, el cual implica identificar aquellas actividades y funciones en el entorno de seguridad informática que son esenciales para el funcionamiento de la organización y que están enfocados en los controles de acceso, en donde se realiza una revisión detallada de cada uno de estos procesos y se establecen criterios claros para determinar su nivel de criticidad, esto implica realizar un análisis exhaustivo y detallado en las distintas áreas y sistemas que conforman la estructura empresarial.

Este paso se debe realizar con la ayuda de todas las personas involucradas en los determinados departamentos que afectan

este proceso, así como también realizar una exhaustiva revisión de los procesos operativos y sistemas de información clave.

Para poder lograr todo esto, se necesita emplear diversos métodos o técnicas tales como entrevistas con el personal pertinente de cada proceso.

Es muy importante tener en cuenta que, con este paso se logra asegurar la protección y salvaguardar la información sensible, a la misma vez que se garantiza la seguridad, continuidad y operatividad de la organización en general.

En el presente trabajo se presentan los criterios de evaluación que permitirán identificar los procesos críticos de acuerdo al entendimiento del auditor enfocándose en la industria automotriz, cabe mencionar que estos criterios pueden variar según sea el caso, dependiendo del enfoque de la auditoría, de la perspectiva del auditor y de las personas involucradas en el proceso.

Para efecto de muestra se ha tomado como base los procesos de la línea de negocio de Venta, que se encuentra en el mapa de procesos de la organización de industria automotriz mostrado en la *Figura 3.2,* cabe mencionar que en este mapa de procesos de la organización existen dos líneas de negocio: Venta y Postventa.

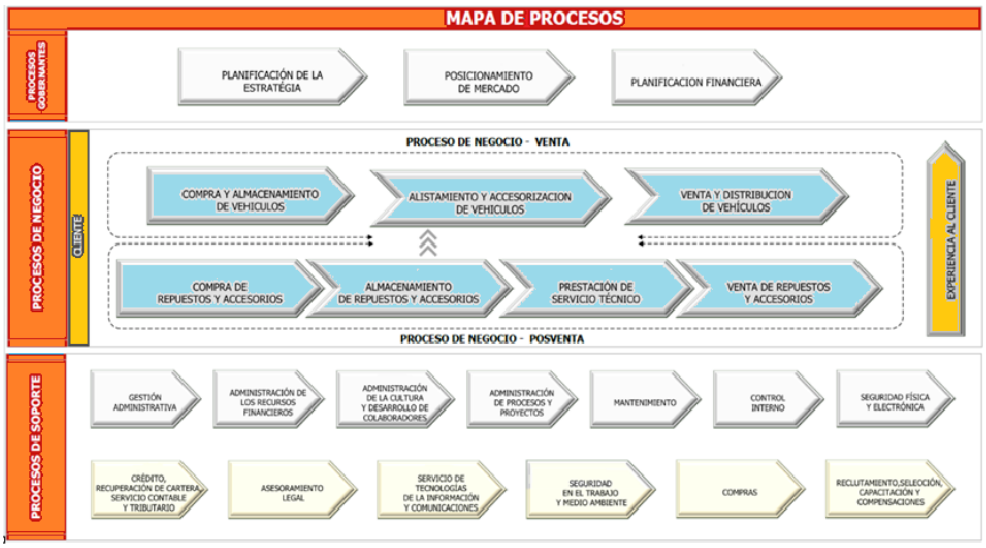

Figura 3.2 : Mapa de procesos de la organización de industria automotriz
Fuente: Autor

Criterio 1: Impacto empresarial.- Se evalúa el impacto de cada interrupción o degradación de procesos en las operaciones, los ingresos, la reputación y el cumplimiento normativo de la empresa, esto implica analizar cómo afecta el proceso a la organización considerando aspectos como la disponibilidad de los recursos y eficacia en las operaciones. Se debe dar mayor prioridad a los procesos con un impacto más negativo.

Criterio 2: Sensibilidad de la Información.- Se identifican los procesos que manejan información confidencial, personal o regulada, es decir los que representan un riesgo para la seguridad de la información, por lo tanto, se debe analizar las implicaciones

que pueden tener en la confidencialidad, integridad y disponibilidad de la información. Aquellos procesos que gestionan datos críticos se les debe dar mayor prioridad.

Criterio 3: Cumplimiento normativo.- Se debe asegurar que, sus procesos se adhieran a las regulaciones y/o estándares establecidos por las autoridades competentes relacionadas con la seguridad, el medio ambiente, calidad entre otras para la industria automotriz. Los procesos que presenten un riesgo de incumplimiento normativo serán identificados como críticos.

Criterio 4: Dependencia de sistemas tecnológicos.- Se debe analizar cuáles son los procesos que son altamente dependientes de los sistemas y tecnologías de la información. A los procesos que más dependen de TI se les debe dar mayor prioridad.

Criterio 5: Complejidad e importancia.- Se evalúa la complejidad del proceso y su importancia para las operaciones de la organización. Se debe dar mayor prioridad a los procesos más complejos e importantes.

En base a estos criterios establecidos, se elabora la *Tabla 3.1* para medir el nivel de criticidad de los procesos, en donde la escala se la maneja del 1 al 3, considerando 1 como menor prioridad y 3 como máxima prioridad, por lo tanto, la suma de las prioridades de los criterios me dará como resultado el nivel de criticidad del proceso.

IDENTIFICACIÓN DE PROCESOS CRÍTICOS							
Líderes de los procesos:							
Responsable:							
Fecha Elaboración:							
Criterios / **Procesos**		1.-Impacto empresarial.	2.-Sensibilidad de la información.	3.-Cumplimiento normativo.	4.-Dependencia de sistemas tecnológicos.	5.-Complejidad e importancia.	Nivel de criticidad.
1	Compra y almacenamiento de vehículos.						
2	Alistamiento y Accesorización de Vehículos.						
3	Venta y Distribución de Vehículos.						
4	Compra de Repuestos y Accesorios.						
5	Almacenamiento de Repuestos y Accesorios.						
6	Prestación de Servicio Técnico.						
7	Venta de Repuestos y Accesorios.						

Tabla 3.1 :Tabla de medición de nivel de criticidad de los procesos
Fuente: Autor

3.1.2 Identificación de activos de información:

En este proceso se realiza un inventario exhaustivo de los diferentes sistemas y mecanismos utilizados para controlar el acceso a la información, es decir, consiste en reconocer y clasificar todos los elementos de información relevantes que la organización tiene a su disposición, esto incluye desde datos confidenciales hasta sistemas de información críticos, como bases de datos, sistemas de almacenamiento, aplicaciones informáticas, documentos, activos intangibles como la propiedad intelectual, información financiera, entre otros.

Mediante esta identificación y categorización, se obtiene una visión clara de todos los sistemas y se establece una base sólida para el análisis posterior.

Por lo tanto, este proceso de identificación minucioso y detallado le permite comprender a fondo los recursos que deben ser protegidos y evaluar su importancia dentro de la infraestructura tecnológica de la organización, así como conocer el impacto que tendría su compromiso o alteración en el cumplimiento de los objetivos estratégicos y operativos, fortaleciendo la seguridad y minimizando los riesgos potenciales, contribuyendo así a la protección de la integridad, confidencialidad y disponibilidad de la información de la empresa.[7]

Para este proceso se puede obtener ayuda de Magerit y la Norma ISO 27005, ambas son ampliamente reconocidas en el ámbito de la seguridad de la información y ofrecen enfoques sólidos para la valoración de activos de información. La elección entre una u otra dependerá de varios factores, incluyendo la preferencia de la organización, la complejidad de sus sistemas y procesos, y los requisitos específicos de cumplimiento, pero también se puede combinar según las necesidades.

Lo más importante es que la metodología seleccionada se adapte adecuadamente al contexto y los objetivos de la organización, y que se implemente de manera efectiva para gestionar los riesgos de seguridad de la información de manera eficiente y eficaz.

Por lo tanto, para este proceso se tomará de referencia Magerit para la identificación de los activos de información.

Los tipos de activos de acuerdo a Magerit que se utilizará en la *Tabla 3.2* son:

[D] Datos / Información: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de

datos) o será transferido de un lugar a otro por los medios de transmisión de datos.[8]

[S] Servicios: Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.[8]

[SW] Software – Aplicaciones informáticas: Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.[8]

[HW] Equipamiento informático (hardware): Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.[8]

[P] Personal: En este epígrafe aparecen las personas relacionadas con los sistemas de información.[8]

Se tomará como ejemplo el Proceso: Venta y Distribución de Vehículos.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN			
Proceso:	Venta y Distribución de Vehículos.		
Líder del proceso:			
Responsable:			
Fecha Elaboración:			
Código	**Tipo Activo**	**Descripción**	**Responsable**
D001	Datos/Información	Información de clientes.	
D002	Datos/Información	Información de vehículos.	
D003	Datos/Información	Información financiera.	
D004	Datos/Información	Información de empleados.	
D005	Datos/Información	Contratos de clientes.	
D006	Datos/Información	Credenciales a los sistemas.	
D007	Datos/Información	Datos de validación de credenciales.	
D008	Datos/Información	Datos de control de acceso.	
D009	Datos/Información	Registro de actividad de sistema.	
HW001	Equipos informáticos (hardware)	Equipos de cómputo.	
HW002	Equipos informáticos (hardware)	Informática móvil.	
SW001	Software	Software de venta y distribución.	
SW002	Software	Software de inventario.	
S001	Servicios	Gestión de privilegios.	
S002	Servicios	Gestión de identidades.	
P001	Personal	Usuarios internos	
P002	Personal	Usuarios externos	

Tabla 3.2: Identificación de Activos de Información
Fuente: Autor

Luego que se identifican los activos de información se procede a determinar su nivel de criticidad, y para este trabajo se usarán las

características de seguridad de la información considerados por la Norma ISO 27001, las cuales son: Confidencialidad, Integridad y Disponibilidad.

En cuanto a la escala para medir la criticidad de los activos de información está dada de acuerdo a la *Tabla 3.3,* en donde cada nivel de la escala representa el nivel de afectación del criterio de seguridad en el caso de que el activo identificado sea impactado negativamente por cualquier evento o incidente de seguridad de la información.

ESCALA DE VALORACIÓN DE LOS CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN.		
Criterio	**Valor**	**Descripción**
CONFIDENCIALIDAD	1	No existe afectación en el funcionamiento de la organización, porque el activo es público.
	2	Puede paralizar parcialmente el funcionamiento de la organización, porque el activo podrá ser utilizado o divulgado a personas no autorizadas.
	3	Puede paralizar significativamente el funcionamiento de la empresa, porque el activo ha sido divulgado a personas no autorizadas.
INTEGRIDAD	1	No existe afectación en el funcionamiento de la organización, si es que el activo no está completo o es alterado.
	2	Puede paralizar parcialmente el funcionamiento de la organización, si es que el activo no está completo o es alterado.
	3	Puede paralizar significativamente el funcionamiento de la empresa, si es que el activo no está completo o es alterado.
DISPONIBILIDAD	1	No existe afectación en el funcionamiento de la organización, si es que el activo no está disponible o es destruido.
	2	Puede paralizar parcialmente el funcionamiento de la organización, si es que el activo no está disponible o es destruido.
	3	Puede paralizar significativamente el funcionamiento de la organización, si es que el activo no está disponible o es destruido.

Tabla 3.3:Escala de Valoración de los criterios de seguridad de la información
Fuente: Autor

En base a estos criterios y escala establecidas, se elabora la *Tabla 3.4* para medir el nivel de criticidad de los activos de información, en donde la suma de las prioridades de los criterios me dará como resultado el nivel de criticidad del activo de información.

IDENTIFICACIÓN DE ACTIVOS CRÍTICOS DE INFORMACIÓN						
Proceso:			Venta y Distribución de Vehículos.			
Líder del Proceso:						
Responsable:						
Fecha Elaboración:						
Criterios / **Activos**			1.- Confidencialidad	2.-Integridad.	3.- Disponibilidad.	Nivel de criticidad.
1	D001	Información de clientes.				
2	D002	Información de vehículos.				
3	D003	Información financiera.				
4	D004	Información de empleados.				
5	D005	Contratos de clientes.				
6	D006	Credenciales a los sistemas.				
7	D007	Datos de validación de credenciales.				
8	D008	Datos de control de acceso.				
9	D009	Registro de actividad de sistema.				
10	HW001	Equipos de cómputo.				
11	HW002	Informática móvil.				
12	**SW001**	**Software de venta y distribución.**				
13	SW002	Software de inventario.				

14	S001	Gestión de privilegios.				
15	S002	Gestión de identidades.				
16	P001	Usuarios internos				
17	P002	Usuarios externos				

Tabla 3.4: Identificación de Activos Críticos de Información
Fuente: Autor

3.2 Definición de objetivos y alcance de la auditoría:

Con base a la información recopilada en los procesos anteriores en donde se tuvo un contexto general de la organización, la identificación de procesos críticos y la identificación de activos críticos, podemos establecer los objetivos específicos que se pretende lograr con la auditoría y establecer los límites y restricciones dentro de los cuales se llevará a cabo la auditoría, por ejemplo identificar vulnerabilidades en los sistemas, evaluar el cumplimiento normativo, valorar la efectividad de los controles de seguridad existentes, etc.

Pero en este trabajo se debe asegurar que, los sistemas de control de accesos estén completamente implementados de manera efectiva y cumplan con los estándares de seguridad establecidos por las entidades regulatorias pertinentes, además esta auditoría busca de manera exhaustiva detectar posibles vulnerabilidades y riesgos en los controles de acceso con el objetivo principal de corregirlos a tiempo y prevenir cualquier tipo de amenaza o brecha de seguridad que pueda

poner en riesgo la integridad, confidencialidad de la información y datos sensibles de la organización.

En esta parte también se debe definir los roles y responsabilidades de los auditores y los equipos responsables de la seguridad informática.

3.3 Revisión del documento de aplicabilidad

El documento de aplicabilidad es un componente clave del SGSI según la norma ISO 27001, en este documento se establece cómo se aplicarán los controles de seguridad de la información en la organización, por tanto es fundamental determinarlo en el proceso del alcance de la auditoria.

Hay que revisar el documento de aplicabilidad existente para:

• Asegurar que los controles de acceso a los activos de información estén adecuadamente definidos y documentados.

• Identificar cualquier brecha o área de mejora en los controles de acceso y asegurar de que se aborden en el proceso de auditoría.

Revisar la documentación y los registros aplicables, como políticas de seguridad, informes de incidentes anteriores y registros de actividad, todo esto, ayuda a evaluar la efectividad de los controles

implementados y a obtener una visión completa de la seguridad de TI de la organización para realizar una buena auditoria.

Entonces, se puede decir que, la DA es una lista de objetivos y controles que la organización ha seleccionado de acuerdo con sus necesidades comerciales y también sus excepciones a ciertos controles, el cual demuestra cómo una organización gestiona el riesgo.

Pero este documento no debe ser lo suficientemente detallado como para proporcionar información valiosa, puesto que, podría caer en manos de alguien que podría hacer un mal uso de ella.

En la *Tabla 3.6* se muestra un ejemplo de la DA para la cláusula “Control de Acceso”, debido a que, para este trabajo sólo nos estamos enfocando en ese control, pero para tener una visión más completa de la DA que se usa en una auditoría de todos los controles de la Norma ISO 27001, se puede ver en el *Anexo 2.*

En este ejemplo se ha colocado los siguientes campos: Las cláusulas, secciones de las mismas, objetivo de control, el porcentaje de ejecución de los controles actuales, identificación de los controles de acuerdo a la *Tabla 3.5* , si es aplicable o no dicho control, y una justificación.

DEFINICIÓN DE CONTROLES SELECCIONADOS	
LR	Requerimientos legales.
CO	Obligaciones contractuales.
BR/BP	Requerimientos del negocio / mejores prácticas adoptadas.
RRA	Resultado de la valoración de riesgos.

Tabla 3.5: Significado de los campos de la Declaración de Aplicabilidad
Fuente: Autor

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección				Aplicable (Si/No)	Justificación
Cláusula	Sección	Objetivo de control / control		LR	CO	BR/BP	RRA		
9 Control de Acceso	9.1	Requisitos del negocio para el control de acceso							
	9.1.1	Política de control de acceso	0,00%						Requisito obligatorio en la norma.
	9.1.2	Acceso a redes y a servicios en red	0,00%						
	9.2	Gestión de acceso de usuarios							
	9.2.1	Registro y cancelación del registro de usuarios	0,00%						
	9.2.2	Suministro de acceso de usuarios	0,00%						
	9.2.3	Gestión de derechos de acceso privilegiado	0,00%						
	9.2.4	Gestión de información de autenticación secreta de usuarios	0,00%						
	9.2.5	Revisión de los	0,00%						

		derechos de acceso de usuarios							
	9.2.6	Retiro o ajuste de los derechos de acceso	0,00%						
	9.3	Responsabilidades de los usuarios							
	9.3.1	Uso de información de autenticación secreta	0,00%						
	9.4	Control de acceso a sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información	0,00%						
	9.4.2	Procedimientos de ingreso seguro	0,00%						
	9.4.3	Sistema de gestión de contraseñas	0,00%						
	9.4.4	Uso de programas y utilitarios privilegiados	0,00%						
	9.4.5	Control de acceso a códigos fuente de programas	0,00%						

Tabla 3.6:Declaración de Aplicabilidad sobre la cláusula "Control de Acceso"
Fuente: Información del Anexo A de la Norma ISO 27001

Finalmente se debe comunicar claramente el alcance de la auditoría a todas las partes interesadas, incluyendo la alta dirección, los propietarios de los activos de información y los equipos operativos afectados. Luego se debe obtener la aprobación formal del alcance de la auditoría por parte de la dirección y confirmar que todas las partes interesadas están de acuerdo con los objetivos y los límites establecidos.

CAPÍTULO 4

DISEÑO DEL ESQUEMA DE DESARROLLO DE LA AUDITORÍA.

En este capítulo, se abordará de manera exhaustiva y detallada el diseño completo del esquema de desarrollo de la auditoría informática en los controles de acceso a los valiosos y sensibles activos de información bajo los lineamientos establecidos por la Norma ISO 27001, de acuerdo a lo que ya fue definido en el capítulo anterior, es decir en el diseño del alcance de la auditoría.

Además se sentará las sólidas y robustas bases necesarias para el completo y adecuado desarrollo de la auditoría, estableciendo de manera firme y

segura los pilares fundamentales e inquebrantables sobre los cuales se llevará a cabo de forma rigurosa y altamente profesional todo el complejo y minucioso proceso de evaluación, análisis y estricto control.

Por tanto, se lleva a cabo siguiendo una serie de pasos detallados. Se realiza el plan detallado de la auditoría , en donde se coloca de forma general o detallada los procesos que seguirán los auditores, como se visualiza en la *Tabla 4.1*, dicho plan debe ser firmado por la empresa auditada, para continuar con una revisión exhaustiva del documento de calidad, el cual incluye los procedimientos y políticas establecidos para garantizar la seguridad integral de los activos de información. Esta revisión abarca un análisis minucioso de cada aspecto relevante, asegurando que se cumplan los más altos estándares de protección de los mismos.

A continuación, se procede a realizar un análisis detallado de las cláusulas establecidas en la norma ISO 27001, para que luego se lleve a cabo una serie de observaciones, con el objetivo de identificar posibles brechas o áreas de mejora en los controles de acceso existentes, dichas observaciones son documentadas detalladamente y se analizan en profundidad para determinar las posibles causas y consecuencias de las debilidades encontradas.

Además de las observaciones también se registra meticulosamente las no conformidades encontradas durante la auditoría. Estas no conformidades

pueden estar relacionadas con incumplimientos de los controles de acceso o con la falta de implementación adecuada de las cláusulas establecidas en la norma ISO 27001.

PLAN DE AUDITORÍA				
Nombre de la organización:				
Representante de la dirección:				
TIPO DE AUDITORÍA				
☐ Auditoría Interna	☐ Auditoría Externa	☐ Seguimiento		
Auditor Líder : Equipo auditor:				
Objetivos de Auditoría:				
Alcance de Auditoría:				
Criterio de Auditoría & Documentos de Referencia:				
Idioma:				
Lugar / Sitio de Auditoría:				
Día	**Hora**	**Auditor**	**Área / Departamento / Proceso / Procedimiento / Función**	**Nota**

Declaración de Confidencialidad: Todas las informaciones evidenciadas durante la realización de esta Auditoría serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la organización.	
Por favor revisar este plan de Auditoría, firmar y devolverlo.	
Representante de la Dirección _____	**Fecha** _____

Tabla 4.1: Formato del Plan de Auditoría
Fuente: Autor

4.1 Revisión del Documento de Calidad.

La revisión del documento de calidad es esencial para comprender la estructura y los procesos/procedimientos relacionados con la seguridad de la información dentro de la organización. Este documento proporciona una visión detallada de las políticas, procedimientos y controles implementados para proteger los activos de información.

En la auditoría, se verifica la existencia y el cumplimiento de este documento, así como la adecuación de sus contenidos. Se evalúa si se ha definido una estructura clara y concisa que englobe todos los aspectos relevantes, se han establecido los procedimientos necesarios para garantizar el cumplimiento de los estándares y se han identificado claramente los responsables de su implementación y mantenimiento.

Además, se revisa minuciosamente la actualización y disponibilidad del documento, asegurando en todo momento que refleje de manera

precisa y completa las prácticas y controles establecidos en la Norma ISO 27001, y se realiza una exhaustiva comparación entre los requisitos establecidos en el documento y las prácticas reales de la organización. De esta forma, se busca garantizar la correcta gestión de la calidad en materia de seguridad informática, proporcionando una base sólida para el análisis y mejora continua de los controles de acceso a los activos de información.

Asimismo, el documento de calidad sirve como una guía para el proceso de auditoría, ofreciendo pautas claras sobre qué información recopilar, cómo analizarla y cómo documentar adecuadamente los hallazgos y recomendaciones. Por lo tanto, al contar con un documento de calidad, se asegura la consistencia en la ejecución de la auditoría, permitiendo que diferentes auditores sigan el mismo enfoque y metodología. En resumen, el documento de calidad en una auditoría en seguridad informática garantiza la integridad, eficiencia y transparencia del proceso de auditoría.[9]

En el Anexo 3 se muestra un ejemplo de este documento, en donde se debe colocar toda la información recopilada del capítulo anterior, como es el objetivo y alcance de la auditoría, los criterios y documentos de referencia utilizados, que en este caso se puede colocar “ISO 27001:2013 - Declaración de aplicabilidad”, y demás documentos

usados en la auditoría como los requisitos legales, algún otro manual, o matriz de riesgos según sea el caso.

4.2 Revisión de las Cláusulas de la Norma ISO 27001.

En el desarrollo de la auditoría en seguridad informática se realiza una revisión exhaustiva de las cláusulas establecidas en esta norma.

Estas cláusulas abordan diferentes aspectos relacionados con la gestión de la seguridad de la información, incluyendo el contexto de la organización, el liderazgo y el compromiso de la dirección, la planificación del sistema de gestión de seguridad de la información, el soporte y los recursos necesarios, la operación del sistema de gestión de seguridad de la información, la evaluación del desempeño y la mejora continua.

El dominio “Control de acceso” se encuentra principalmente dentro de la cláusula 9, "Evaluación del desempeño", aunque este control también puede estar presente en otras cláusulas y secciones de la norma, como en la cláusula 5 "Liderazgo" y la cláusula 7 "Soporte", su evaluación y mejora continua se realizan principalmente en el contexto de la cláusula 9.

Esta cláusula se centra en la evaluación continua del desempeño del SGSI, lo cual incluye la revisión y mejora de los controles

implementados para garantizar la seguridad de la información, es decir en esta evaluación involucra la revisión de incidentes de seguridad, auditorías internas, así como la monitorización continua de los controles para asegurar su efectividad y adecuación.

Durante esta auditoría, se evalúa los controles de acceso implementados por la organización en función de estas cláusulas, asegurando que cumplan con los requisitos establecidos y garantizando la protección de los activos de información de la empresa.

Es importante tener en cuenta que durante este proceso se utilizan múltiples herramientas y técnicas especializadas para evaluar la efectividad y eficiencia de los controles de acceso implementados.

Entre las herramientas más utilizadas se encuentran las de escaneo de vulnerabilidades, que permiten identificar posibles debilidades en los sistemas de control de acceso. Asimismo, las herramientas de análisis de logs son utilizadas para examinar los registros de eventos y detectar posibles brechas de seguridad, también se aplican técnicas de pruebas de penetración, las cuales simulan ataques reales para evaluar la resistencia de los sistemas. Además se utilizan técnicas de análisis de tráfico de red para examinar el flujo de datos y detectar posibles amenazas o anomalías en la red y las TAACS**.**

Asimismo, se emplean técnicas de revisión de políticas y procedimientos, que implican analizar y evaluar las normas y reglamentos establecidos para el control de accesos, y estos se llevan a cabo mediante las técnicas establecidas en el *Capítulo 1*, como son las encuestas, entrevistas, análisis, conciliación, comprobación, e inspección, de las cuales se usan en este trabajo.

Para ello, se elabora la *Tabla 4.2* con el detalle respectivo de cada control y las técnicas de revisión para cada una de ellas, en base a la información que ya se ha recopilado hasta el momento, sobre el Dominio “Control de Acceso”. Para visualizar la tabla completa con todos los controles de Seguridad de la Norma ISO 27001:2013, Ver Anexo 4.

Para efecto de ejemplo se toma el control “Restricción de acceso a la información”.

Para visualizar un modelo de Entrevista, Ver Anexo 5.

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	**Sección**	**Objetivo de control / control**			
9 Control de Acceso	9.1	Requisitos del negocio para el control de acceso			
	9.1.1	Política de control de acceso	Revisión de políticas y procedimientos	Sí	
	9.1.2	Acceso a redes y a servicios en red			
	9.2	Gestión de acceso de usuarios			
	9.2.1	Registro y cancelación del registro de usuarios			
	9.2.2	Suministro de acceso de usuarios			
	9.2.3	Gestión de derechos de acceso privilegiado			
	9.2.4	Gestión de información de autenticación secreta de usuarios			
	9.2.5	Revisión de los derechos de acceso de usuarios			
	9.2.6	Retiro o ajuste de los derechos de acceso			
	9.3	Responsabilidades de los usuarios			
	9.3.1	Uso de información de autenticación secreta			
	9.4	Control de acceso a sistemas y aplicaciones			
	9.4.1	Restricción de acceso a la información	Revisión de políticas y procedimientos Verificación Verbal: Entrevistas Verificación Documental: Comprobación	Sí	Entrevista1.docx Comprobación1.xls
	9.4.2	Procedimientos de ingreso seguro	Revisión de políticas y procedimientos	Sí	
	9.4.3	Sistema de gestión de contraseñas			
	9.4.4	Uso de programas y utilitarios privilegiados			

	9.4.5	Control de acceso a códigos fuente de programas			

Tabla 4.2 : Revisión de las cláusulas del Dominio "Control de Acceso" de la Norma ISO 27001:2013
Fuente: Información del Anexo A de la Norma ISO 27001:2013

4.3 Revisión de las Observaciones y No Conformidades.

Una vez que se concluye en forma exhaustiva todos los pasos anteriormente mencionados, en donde se realizó un análisis a fondo de todos los datos recopilados y se realizó la comparación de los resultados contra los estándares generalmente aceptados, se procede a emitir las observaciones y no conformidades encontradas en el proceso de la auditoría.

4.3.1 Observaciones.

Dentro de las observaciones se debe colocar los hallazgos o situaciones que, si bien no representan una violación directa de las políticas, normas o regulaciones, pueden indicar áreas de mejora o aspectos que requieren atención.

Al realizar las observaciones, es importante proporcionar una descripción clara y concisa de la observación, incluyendo el contexto, los sistemas o procesos involucrados, y cualquier información relevante que respalde el hallazgo, así como también es necesario clasificarlas según su gravedad y relevancia, esto

facilita la priorización de las acciones correctivas y preventivas necesarias en la auditoría que permitan mejorar la postura de seguridad de la organización.

Un ejemplo de observación puede ser:

Durante la auditoría se observaron algunas deficiencias, en primer lugar, se notó que no se estaban realizando registros adecuados de los accesos a los activos de información, lo que dificulta la trazabilidad y el seguimiento de posibles incidentes de seguridad. Además, se encontraron fallos en la gestión de contraseñas, ya que no se estaban aplicando las políticas establecidas como la obligatoriedad de cambiarlas regularmente y la utilización de contraseñas fuertes. Asimismo, se identificaron problemas en la asignación de permisos, con usuarios que tenían privilegios innecesarios o no se les habían revocado los accesos después de cambios de roles o desvinculaciones laborales.

Estas observaciones evidencian la necesidad de mejorar los controles de acceso a los activos de información para garantizar una adecuada protección de la seguridad.

4.3.2 No conformidades.

Dentro de las no conformidades se debe colocar los incumplimientos o violaciones de las políticas, normas, regulaciones o controles de seguridad establecidos.

Al revisar las no conformidades, es esencial incluir claramente la política, norma, regulación o control de seguridad que se ha incumplido proporcionando una evidencia sólida y documentada que respalde dicha “no conformidad”, como capturas de pantalla o registros de auditoría.

Cada una de estas no conformidades es cuidadosamente documentada y analizada en conjunto con el equipo responsable de la gestión de seguridad de los activos de información de la organización. Se generan informes detallados que destacan las no conformidades encontradas y se proponen acciones correctivas específicas para su pronta resolución.

Es importante destacar que todas las acciones correctivas propuestas son diseñadas para abordar de manera efectiva las no conformidades identificadas. Estas acciones pueden incluir desde la actualización o reforzamiento de los controles de acceso, hasta la implementación de nuevas políticas o

procedimientos que contribuyan a mejorar la seguridad informática de la organización.

Un ejemplo de no conformidad puede ser:

Durante la auditoría en seguridad informática en los controles de acceso a los activos de información bajo el lineamiento de la Norma ISO 27001, se identificaron varias no conformidades. Estas no conformidades están relacionadas con la falta de implementación de controles de acceso adecuados, como la falta de políticas claras de acceso, la falta de protección de contraseñas, la falta de autenticación de dos factores y la falta de seguimiento de las actividades de acceso. Además, se detectaron deficiencias en la documentación y registro de los accesos a los activos de información, lo que dificulta la trazabilidad y el monitoreo de las actividades. Estas no conformidades representan un riesgo significativo para la seguridad de los activos de información y deben ser abordadas de manera urgente para garantizar la confidencialidad, integridad y disponibilidad de la información.

En conclusión al revisar las observaciones y no conformidades, es fundamental mantener un enfoque objetivo, imparcial y

basado en hechos. Además, es importante asegurarse de que las recomendaciones sean factibles, escalables y alineadas con los objetivos y estrategias establecidos en la auditoría.

A continuación se muestra en la *Tabla 4.3* el formato utilizado para evidenciar las observaciones y no conformidades en la auditoría.

NOTA DE AUDITOR					
Nombre de la organización:					
Representante de la dirección:					
TIPO DE AUDITORÍA					
☐ Auditoría Interna		☐ Auditoría Externa		☐ Seguimiento	
Tipo: **OB** = Observación / **NC** = No conformidad					
Auditor Líder :		**Auditor:**			
Fecha:					
Proceso / área	**Cláusula / Norma**	**Descripción / Evidencia**	**Tipo (OB/NC)**	**Prioridad (Baja/Media/Alta)**	**Acción Correctiva / Preventiva**
Declaración de Confidencialidad: Todas las informaciones evidenciadas durante la realización de esta Auditoría serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la organización.					

Tabla 4.3: Documento del auditor para registrar las Observaciones y No conformidades de la auditoría
Fuente: Autor

CAPÍTULO 5

RESULTADOS

5.1 Resultados de la Auditoría.

Una vez completada la documentación exhaustiva de los hallazgos/observaciones obtenidos tras el riguroso análisis, se procede de manera minuciosa y detallada a elaborar el informe final de la auditoría en seguridad informática de control de accesos.

Este informe es un documento formal que se prepara con las conclusiones obtenidas luego de haber realizado el trabajo de auditoría, dichos resultados se tienen que presentar a los distintos niveles de la gerencia y para ello se necesita conocimiento de las diferentes técnicas

de presentación necesaria para comunicar los resultados obtenidos en la auditoría.

Dentro de las principales técnicas de presentación que se tiene son:

Resumen ejecutivo: Es un informe conciso y fácil de leer que presenta los hallazgos/observaciones a la gerencia en un forma comprensible. Los hallazgos/observaciones y las recomendaciones se deben de comunicar desde una perspectiva de negocio, en un lenguaje que los miembros de la alta gerencia puedan entender y aplicar a su visión de negocio.

Anexos detallados: Son un tipo de informe de naturaleza más técnica, ya que la gerencia de operaciones requerirá los detalles para corregir las situaciones reportadas.

Presentación visual: Se pueden incluir diapositivas o gráficas de computadora donde se presente los resultados del trabajo realizado. Usualmente es usado a lo interno del departamento de auditoría para presentar el reporte o estatus de los trabajos, o presentar a otros departamentos para compartir ciertas informaciones.

Antes de comunicar los resultados a la alta dirección, se debe discutir los hallazgos/observaciones con el personal a cargo del área auditada mediante una entrevista para llegar a un acuerdo sobre ellos y desarrollar un plan de acción correctivo para cada uno de ellos, en

dicha entrevista se debe asegurar de que los hechos presentados en el informe estén correctos, que las recomendaciones o acciones correctivas sean realistas y eficientes; en caso de que no lo sean buscar alternativas con el auditado y sugerir fechas de implementación para los planes de acción acordados. En caso de existir algún desacuerdo, se debe profundizar sobre la importancia de los hallazgos/observaciones identificados, y cuáles son los efectos de no corregir dichas debilidades del control.

Una vez que se ha llegado a un acuerdo con el auditado, el auditor líder debe enviar un corto resumen a la alta dirección y al comité de auditoría.

En conclusión los informes de auditoría son el producto final del trabajo de auditoría y son utilizados para presentar a la gerencia los hallazgos/observaciones y las recomendaciones, el cual su objetivo principal sirve para proporcionar una visión global y profunda de la situación actual de los controles de acceso y para trazar una senda precisa hacia la mejora continua.

Para lograr este cometido, se comienza con una introducción rigurosa que sienta las bases conceptuales y contextualiza el alcance del trabajo realizado. A continuación, se describen de forma exhaustiva los objetivos establecidos para alcanzar un nivel óptimo de seguridad y se

detalla la metodología detallada empleada en la auditoría, que garantiza la fiabilidad y el rigor científico del proceso, toda esta información ya fue elaborada en los capítulos anteriores.

Después de establecer los cimientos necesarios, se entra en la fase de presentar los hallazgos/observaciones documentados tras el minucioso análisis llevado a cabo. La información recolectada se complementa con recomendaciones claras y concisas, que orientan a la organización hacia la implementación de mejoras concretas y efectivas, dicha información se encuentra en el documento elaborado con anterioridad “Notas del auditor”.

En la *Tabla 5.1* se puede visualizar un ejemplo de Informe Final.

INFORME FINAL						
Nombre de la organización:						
Representante de la dirección:						
TIPO DE AUDITORÍA						
☐ Auditoría Interna	☐ Auditoría Externa			☐ Seguimiento		
Auditor Líder : **Equipo auditor:**						
Introducción (Alcance):						
Objetivos de Auditoría:						
Metodología:						
Fecha Inicio Auditoría:						
Fecha Fin Auditoría:						
Nro. Hallazgos/Observaciones encontradas:	**Mayores:**		**Intermedio:**		**Menores:**	
Hallazgos/Observaciones:	**Proceso/área:**					
	Cláusula/Norma:					
	Descripción:					
	Recomendaciones:					
	Acción correctiva/preventiva:					
Hallazgos/Observaciones:	**Proceso/área:**					
	Cláusula/Norma:					
	Descripción:					
	Recomendaciones:					
	Acción correctiva/preventiva:					
Nro. No Conformidades encontradas:	**Mayores:**		**Intermedio:**		**Menores:**	

No conformidades:	**Proceso/área:**	
	Cláusula/Norma:	
	Descripción:	
	Recomendaciones:	
	Acción correctiva/preventiva:	
No conformidades:	**Proceso/área:**	
	Cláusula/Norma:	
	Descripción:	
	Recomendaciones:	
	Acción correctiva/preventiva:	
Personas claves entrevistadas / involucradas:	**Apellidos y Nombres/Cargo**	**Área/Proceso**
ANEXOS:		
Declaración de Confidencialidad: Todas las informaciones evidenciadas durante la realización de esta Auditoría serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la organización.		

Tabla 5.1 :Formato del Informe final de la Auditoría
Fuente: Autor

5.2 Revisiones Posteriores.

Estas revisiones meticulosas y rigurosas se realizan con el firme propósito de garantizar la implementación efectiva de todas las medidas de seguridad, así como evaluar minuciosamente su eficacia en la protección integral y total de dichos activos de información.

Durante este exigente proceso, se lleva a cabo un minucioso examen de todos los registros detallados y evidencias relevantes, con el objetivo primordial de asegurar de manera inequívoca y firme que los controles de acceso están siendo aplicados de manera escrupulosa y en absoluta consonancia con todas las políticas y procedimientos definidos y establecidos en el Documento de Aplicabilidad, además de velar por el cumplimiento riguroso de todas y cada una de las cláusulas impuestas por la destacada norma ISO 27001.

Como parte integral de este proceso tan riguroso, también se lleva a cabo la identificación y documentación exhaustiva de cualquier observación o no conformidad encontrada durante toda la exhaustiva auditoría, lo cual constituye un elemento fundamental y sólido para la posterior generación de conclusiones y recomendaciones sólidas y confiables, las cuales se presentan al final del completo e integral proceso de auditoría en seguridad informática.

A continuación, en la *Figura 5.1* se establece un plan de acción para las revisiones posteriores / seguimiento de los hallazgos de la auditoría:

	Modo de	Nombre de tarea	Duración	Responsable	Predecesoras
1		**Preparación**	**16 días**		
2		Revisión y preparación de documentos relevantes	7 días	Equipo de auditoría	
3		Asignar recursos y responsabilidades	2 días	Líder de equipo auditor	2
4		Comunicación del plan a los interesados.	3 días	Jefe del Proceso	3
5		Establecer fechas límite.	2 días	Líder de equipo auditor	4
6		Obtener aprobación del plan de acción.	2 días	Líder de equipo auditor	5
7		**Ejecución**	**30 días**		
8		Revisión y Análisis detallado de los hallazgos encontrados en la auditoría anterior.	7 días	Equipo de auditoría	6
10		Clasificación de hallazgos según su nivel de criticidad.	2 días	Equipo de auditoría	8
11		Revisión de acciones correctivas/recomendaciones sobre los hallazgos encontrados	21 días	Equipo de auditoría	10
12		**Monitoreo y Seguimiento**	**28 días**		
13		Seguimiento continuo de la implementación de las acciones correctivas/recomendaciones	21 días	Equipo de auditoría	11
14		Verificación de la correcta implementación de las acciones correctivas/recomendaciones	7 días	Equipo de auditoría	13
15		**Cierre y Documentación**	**9 días**		
16		Elaboración del informe final de la resolución de los hallazgos/recomendaciones	7 días	Equipo de auditoría	14
17		Presentación de informe final a la alta dirección.	2 días	Líder de equipo auditor	16

Figura 5.1 Plan de acción desarrollado en Gantt
Fuente: Autor

5.3 Evaluación del Diseño Propuesto.

El diseño propuesto para la realización de una auditoría en seguridad informática en los controles de acceso a los activos de información bajo lineamiento de la ISO 27001 para una empresa automotriz, se evaluó bajo un proceso integral en la que se realizó de manera teórica y metodológica sin llevar a cabo la auditoría real, debido al enfoque del

presente trabajo de titulación que se centra en tres objetivos fundamentales:

- Conceptualizar la importancia de realizar un esquema de auditoría informática.
- Proporcionar un estándar y/o herramienta básica para realizar auditorías efectivas y eficientes de sus controles de seguridad.
- Recomendar lineamientos de seguridad en los controles de acceso a los activos de información.

Además se tomó en consideración los principios básicos de la seguridad informática y de la auditoría informática. Por tanto al cumplir con todos estos objetivos y criterios establecidos se logró asegurar en tener un esquema adecuado y efectivo para la realización de una auditoría en seguridad informática bajo los lineamientos de la ISO 27001, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

El puntaje utilizado para la valoración de cada criterio fue otorgada de acuerdo a la *Tabla 5.2.*

PUNTAJE	DESCRIPCIÓN
0	No está en el diseño.
50	Está parcialmente en el diseño.
100	Está mayormente completo o completo al 100% en el diseño.

Tabla 5.2 : Tabla de valoración de puntaje para evaluación de diseño.
Fuente: Autor

Por tanto de acuerdo a la evaluación realizada se obtiene como resultado para el principio básico de la seguridad informática un 88% y para el principio básico de la auditoría informática un 83% de acuerdo a la *Figura 5.2* y a la *Figura 5.3*.

Para mayor detalle de los resultados de la evaluación Ver Anexo 6.

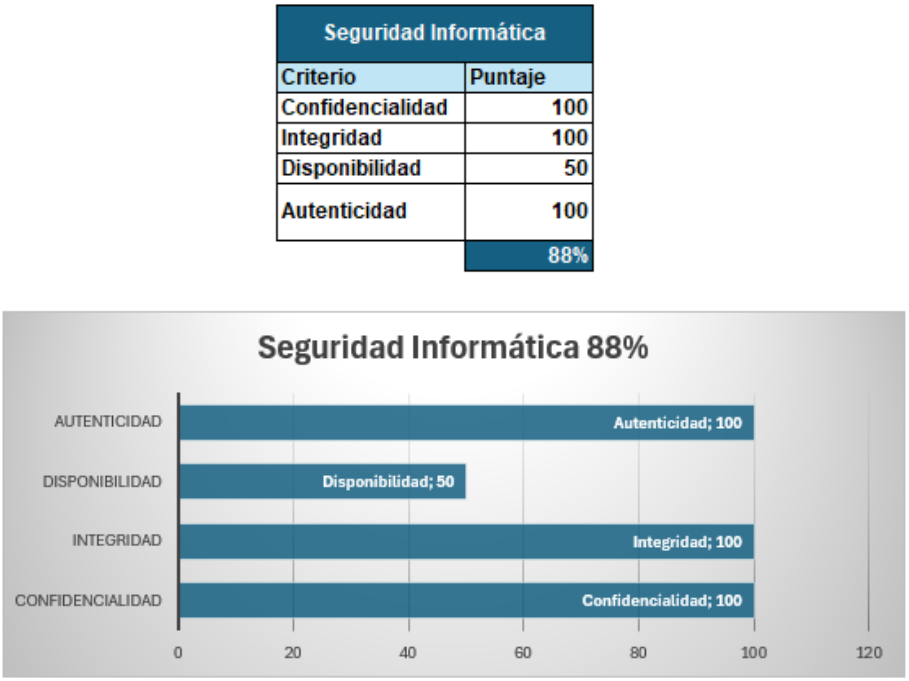

Figura 5.2 : Gráfico estadístico de la valoración obtenida de la evaluación del diseño según principio de seguridad informática..
Fuente: Autor

Auditoría Informática		
	Criterio	**Puntaje**
Preparación y Planificación	Documentación previa	100
	Plan de auditoría	100
	Enfoque basado en riesgos	100
Ejecución de la Auditoría	Recopilación de Evidencia	50
	Herramientas y Técnicas	50
	Metodología Consistente	100
Análisis y Evaluación:	Evaluación de Controles	50
	Identificación de Brechas	50
	Recomendaciones Prácticas	100
Comunicación y Reporte:	Claridad y Precisión	100
	Presentación de Resultados	100
	Seguimiento de Hallazgos	100
Adaptabilidad y Flexibilidad:	Adaptación a Cambios	100
	Innovación	50
Cumplimiento Normativo:	Alineación con la norma ISO 27001	100
		83%

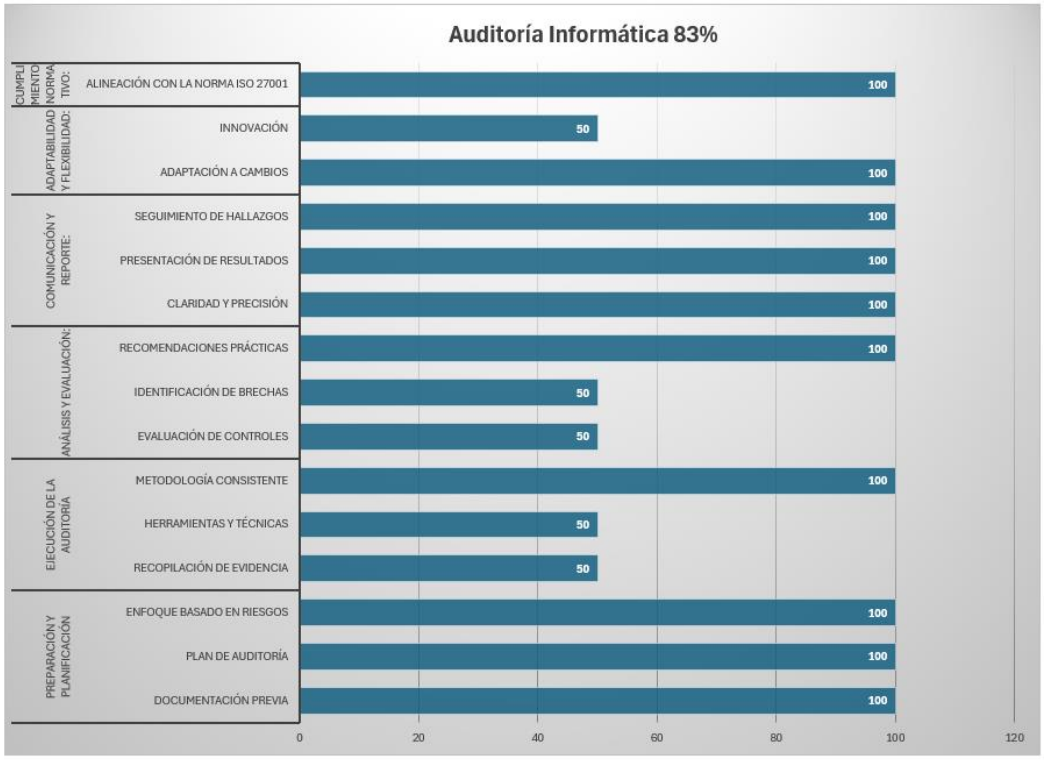

Figura 5.3 :Gráfico estadístico de la valoración obtenida de la evaluación del diseño según principio de auditoría informática.
Fuente Autor

CONCLUSIONES Y RECOMENDACIONES

- El desarrollo del presente trabajo ha permitido establecer una base metódica para realizar una auditoría en seguridad informática alineada a la Norma ISO 27001 para garantizar la efectividad y el éxito del proceso de dicha auditoría, en donde le ayuda al auditor tener los puntos claves que debe tomar en consideración para cada etapa dentro de la auditoría y le proporciona una guía clara para la realización de la misma asegurando que se cubran todos los aspectos relevantes de la seguridad informática.

- Para realizar una auditoría en seguridad informática más profunda se recomienda utilizar mínimo dos técnicas para la revisión de los controles de acceso, para así complementar las revisiones y resultados obtenidas en cada una de ellas.

- Para garantizar una mayor eficiencia y seguridad en el acceso a los activos de información, se recomienda realizar una revisión exhaustiva de los permisos de acceso asignados a cada usuario, eliminando aquellos que no sean necesarios y asegurando que todos los accesos estén adecuadamente justificados y documentados, esto se puede también con la ayuda de TAACS.

- El auditor nunca debe olvidar que el método que siguió para la obtención de la evidencia, debe tener una base científica y debe ser reproducible por cualquier otro auditor calificado, de manera que ambos puedan llegar al mismo resultado o conclusión y debe conocer a la perfección las leyes civiles a fin de poder discernir cuál información debe mantenerse bajo reserva para hacerla pública y cuál debe comunicarse a las autoridades civiles, en caso de detectar algún fraude o acto ilegal por parte de la empresa auditada.

- Por último, se recomienda realizar auditorías internas con relativa frecuencia, por ejemplo, cada dos meses; y externas cada seis meses. Esto evitará el estrés que causa la auditoría y mantendrá al personal siempre en el límite.

BIBLIOGRAFÍA

[1] M. Piattini, «Auditoría Informática. Un enfoque práctico.», [En línea]. Disponible en: https://www.academia.edu/16436334/Auditoria_inform%C3%A1tica_un_enfoque_pr%C3%A1ctico_Mario_Piattini

[2] M. Garzon Garzon, «Diseñar los controles de acceso aplicables a la empresa Spytech S.A.S para su posterior implementación, de acuerdo con el dominio A9 de la norma ISO 27001:2013.», jun. 2016, Accedido: 8 de marzo de 2024. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/11990

[3] P. H. Carla Pamela, «Auditoría informática al sistema contable y su incidencia en la confiabilidad de la información financiera, empresa CODIHE-S.A, período 2018.», bachelorThesis, Universidad Nacional de Chimborazo, 2021. Accedido: 8 de marzo de 2024. [En línea]. Disponible en: http://dspace.unach.edu.ec/handle/51000/7434

[4] G. B. Urbina, «Introducción a la Seguridad Informática».

[5] G. A. Rivas, *Auditoría informática*. Ediciones Díaz de Santos, 1988.

[6] A. P. H. Arias, «Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs)», *Compendium*, ene. 2010, Accedido: 8 de marzo de 2024. [En línea]. Disponible en: https://www.academia.edu/98062460/Auditor%C3%ADa_Inform%C3%A1tica_y_Gesti%C3%B3n_de_Tecnolog%C3%ADas_De_Informaci%C3%B3n_y_Comunicaci%C3%B3n_TICs_

[7] E. A. Suéscum Trejos, «APLICAR UN ESQUEMA SE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 EN EL ÁREA DE POSVENTA EN UNA EMPRESA DE TELECOMUNICACIONES.», 2021, Accedido: 30 de abril de 2024. [En línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/50893

[8] A. Talero y D. Leonardo, «Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en magerit v3.», oct. 2021, Accedido: 30 de abril de 2024. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/43373

[9] D. E. Imbaquingo Esparza, «Método de auditor a informática basado en sistemas de procesamiento avanzado de datos que permita minimizar el riesgo de calidad de los resultados», Tesis, Universidad Nacional de La Plata, 2023. doi: 10.35537/10915/157674.

ANEXOS

Anexo 1

MEMO DE ENTENDIMIENTO DE LA ORGANIZACIÓN	
Propósito de este papel de trabajo:	
Aplicabilidad:	
Auditor Líder:	
Equipo auditor:	
Fecha de reunión:	
1.- Información relacionada con la organización relevante al trabajo del auditor.	
Antecedentes relevantes de la organización:	
Cambios significativos dentro de la organización:	
Organización de la empresa y de TI:	
<u>Área de TI</u> Infraestructura: Desarrollo de Sistemas: Producción: Administración y Control de Calidad: Arquitectura y Soporte de TI:	

Seguridad de la Información:
Auditoría de Sistemas:
Gestión de Riesgos de TI:
Políticas de TI:
Aplicaciones existentes:
Dependencia de TI para los procesos de negocio:
Auditoría de TI:
Aspectos Legales:
Outsourcing y Organizaciones de Servicios:
Otros:

2.- Actividades próximas a realizarse.

Actividad	**Fecha**	**Responsable**

Recordatorio de la comunicación que proveerá el auditor.

[Recordar al auditor la importancia de:]

- Formar conclusiones claras por escrito sin lenguaje restrictivo ni información contradictoria, que no se deban expresar como aseguramiento negativo.
- Cerciorarse de que toda la documentación relevante se incluya en este documento, e informar oportunamente al equipo auditor de los asuntos significativos que puedan impactar la seguridad informática.

Anexo 2

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información							
	5.1.1	Políticas de seguridad de la información	0,00 %						Requisito obligatorio para el SGSI de la entidad. Cláusula 5.2 de la norma.
	5.1.2	Revisión de las políticas de seguridad de la información	0,00 %						Requisito obligatorio para el SGSI de la entidad. Cláusula 5.2 de la norma.
6 Organización de la Seguridad de la Información	6.1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información	0,00 %						
	6.1.2	Segregación de deberes	0,00 %						
	6.1.3	Contacto con autoridades	0,00 %						
	6.1.4	Contacto con grupos de interés especial	0,00 %						
	6.1.5	Seguridad de la información en la gestión de proyectos	0,00 %						
	6.2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles	0,00 %						
	6.2.2	Teletrabajo	0,00 %						
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo							
	7.1.1	Verificación de antecedentes	0,00 %						
	7.1.2	Términos y condiciones del empleo	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	7.2	Durante el empleo							
	7.2.1	Responsabilidades de la Alta Gerencia	0,00 %						
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	0,00 %						
	7.2.3	Proceso disciplinario	0,00 %						
	7.3	Terminación y cambio de empleo							
	7.3.1	Término de responsabilidades o cambio de empleo	0,00 %						
8 Gestión de Activos	8.1	Responsabilidad de los activos							
	8.1.1	Inventario de activos	0,00 %						Requisito obligatorio en la norma. Se debe identificar los activos asociados con información en el proceso.
	8.1.2	Propiedad de activos	0,00 %						
	8.1.3	Uso aceptable de los activos	0,00 %						Requisito obligatorio en la norma. Se debe establecer reglas para el uso aceptable de los activos.
	8.1.4	Devolución de activos	0,00 %						
	8.2	Clasificación de la información							

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	8.2.1	Clasificación de la información	0,00 %						
	8.2.2	Etiquetado de la información	0,00 %						
	8.2.3	Manejo de activos	0,00 %						
	8.3	Manejo de medios							
	8.3.1	Gestión de medios removibles	0,00 %						
	8.3.2	Eliminación de medios	0,00 %						
	8.3.3	Transporte de medios físicos	0,00 %						
9 Control de Acceso	9.1	Requisitos del negocio para el control de acceso							
	9.1.1	Política de control de acceso	0,00 %						Requisito obligatorio en la norma.
	9.1.2	Acceso a redes y a servicios en red	0,00 %						
	9.2	Gestión de acceso de usuarios							
	9.2.1	Registro y cancelación del registro de usuarios	0,00 %						
	9.2.2	Suministro de acceso de usuarios	0,00 %						
	9.2.3	Gestión de derechos de acceso privilegiado	0,00 %						
	9.2.4	Gestión de información de autenticación secreta de usuarios	0,00 %						
	9.2.5	Revisión de los derechos de acceso de usuarios	0,00 %						
	9.2.6	Retiro o ajuste de los derechos de acceso	0,00 %						
	9.3	Responsabilidades de los usuarios							
	9.3.1	Uso de información de autenticación secreta	0,00 %						
	9.4	Control de acceso a sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	9.4.2	Procedimientos de ingreso seguro	0,00 %						
	9.4.3	Sistema de gestión de contraseñas	0,00 %						
	9.4.4	Uso de programas y utilitarios privilegiados	0,00 %						
	9.4.5	Control de acceso a códigos fuente de programas	0,00 %						
10 Criptografía	10.1	Controles criptográficos							
	10.1.1	Política en el uso de controles criptográficos	0,00 %						
	10.1.2	Gestión de llaves	0,00 %						
11 Seguridad Física y del Entorno	11.1	Áreas seguras							
	11.1.1	Perímetro de seguridad físico	0,00 %						
	11.1.2	Controles físicos de entrada	0,00 %						
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	0,00 %						
	11.1.4	Protección contra amenazas externas y del ambiente	0,00 %						
	11.1.5	Trabajo en áreas seguras	0,00 %						
	11.1.6	Áreas de entrega y carga	0,00 %						
	11.2	Equipo							
	11.2.1	Instalación y protección de equipo	0,00 %						
	11.2.2	Servicios de soporte	0,00 %						
	11.2.3	Seguridad en el cableado	0,00 %						
	11.2.4	Mantenimiento de equipos	0,00 %						
	11.2.5	Retiro de activos	0,00 %						
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	0,00 %						
	11.2.7	Eliminación segura o reúso del equipo	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	11.2.8	Equipo de usuario desatendido	0,00 %						
	11.2.9	Política de escritorio limpio y pantalla limpia	0,00 %						
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades							
	12.1.1	Documentación de procedimientos operacionales	0,00 %						Requisito obligatorio en la norma.
	12.1.2	Gestión de cambios	0,00 %						
	12.1.3	Gestión de la capacidad	0,00 %						
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	0,00 %						
	12.2	Protección de Software Malicioso							
	12.2.1	Controles contra software malicioso	0,00 %						
	12.3	Respaldo							
	12.3.1	Respaldo de información	0,00 %						
	12.4	Bitácoras y monitoreo							
	12.4.1	Bitácoras de eventos	0,00 %						
	12.4.2	Protección de información en bitácoras	0,00 %						
	12.4.3	Bitácoras de administrador y operador	0,00 %						
	12.4.4	Sincronización de relojes	0,00 %						
	12.5	Control de software operacional							
	12.5.1	Instalación de software en sistemas operacionales	0,00 %						
	12.6	Gestión de vulnerabilidades técnicas							
	12.6.1	Gestión de vulnerabilidades técnicas	0,00 %						
	12.6.2	Restricciones en la instalación de software	0,00 %						
	12.7	Consideraciones de auditoría de sistemas de información							

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	12.7.1	Controles de auditoría de sistemas de información	0,00 %						
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red							
	13.1.1	Controles de red	0,00 %						
	13.1.2	Seguridad en los servicios en red	0,00 %						
	13.1.3	Segregación en redes	0,00 %						
	13.2	Transferencia de información							
	13.2.1	Políticas y procedimientos para la transferencia de información	0,00 %						
	13.2.2	Acuerdos en la transferencia de información	0,00 %						
	13.2.3	Mensajería electrónica	0,00 %						
	13.2.4	Acuerdos de confidencialidad o no-revelación	0,00 %						Requerimiento obligatorio de la norma.
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información							
	14.1.1	Análisis y especificación de requerimientos de seguridad	0,00 %						
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	0,00 %						
	14.1.3	Protección de transacciones en servicios de aplicación	0,00 %						
	14.2	Seguridad en el proceso de desarrollo y soporte							
	14.2.1	Política de desarrollo seguro	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	14.2.2	Procedimientos de control de cambios del sistema	0,00 %						
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	0,00 %						
	14.2.4	Restricción de cambios en paquetes de software	0,00 %						
	14.2.5	Principios de seguridad en la ingeniería de sistemas	0,00 %						Requerimiento obligatorio de la norma.
	14.2.6	Entorno de desarrollo seguro	0,00 %						
	14.2.7	Desarrollo tercerizado	0,00 %						
	14.2.8	Pruebas de seguridad del sistema	0,00 %						
	14.2.9	Pruebas de aceptación del sistema	0,00 %						
	14.3	Datos de prueba							
	14.3.1	Protección de datos de prueba	0,00 %						
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor							
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	0,00 %						Requerimiento obligatorio de la norma.
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	0,00 %						
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	0,00 %						
	15.2	Gestión de entrega de servicios de proveedor							
	15.2.1	Monitoreo y revisión de servicios del proveedor	0,00 %						
	15.2.1	Gestión de cambios a los servicios del proveedor	0,00 %						
16 Gestión de Incidentes de Seguridad	16.1	Gestión de incidentes de seguridad de la información y mejoras							
	16.1.1	Responsabilidades y procedimientos	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
de la Información	16.1.2	Reporte de eventos de seguridad de la información	0,00 %						
	16.1.3	Reporte de debilidades de seguridad de la información	0,00 %						
	16.1.4	Valoración y decisión de eventos de seguridad de la información	0,00 %						
	16.1.5	Respuesta a incidentes de seguridad de la información	0,00 %						
	16.1.6	Aprendizaje de incidentes de seguridad de la información	0,00 %						
	16.1.7	Colección de evidencia	0,00 %						
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información							
	17.1.1	Planeación de la continuidad de la seguridad de la información	0,00 %						
	17.1.2	Implementación de la continuidad de la seguridad de la información	0,00 %						Req. obligatorio de la norma. Es necesario asegurar el nivel de continuidad requerido para la seg. de la informac. durante una situación adversa.
	17.1.3	Verificación, revisión y evaluación de la continuidad del negocio	0,00 %						
	17.2	Redundancias							
	17.2.1	Disponibilidad de facilidades de procesamiento de información	0,00 %						
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales							
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	0,00 %						Req. obligatorio de la norma. Es necesario aplicar todos los requisitos estatutarios, regulatorios y contractuales.
	18.1.2	Derechos de propiedad intelectual (IPR)	0,00 %						
	18.1.3	Protección de registros	0,00 %						

Controles de Seguridad			Controles Actuales	Controles seleccionados y razones de selección				Aplicable (Si / No)	Justificación
Cláusula ISO 27001	Sección	Objetivo de control / control		LR	CO	BR / BP	RRA		
	18.1.4	Privacidad y protección de información personal identificable (PIR)	0,00 %						
	18.1.5	Regulación de controles criptográficos	0,00 %						
	18.2	Revisiones de seguridad de la información							
	18.2.1	Revisión independiente de seguridad de la información	0,00 %						
	18.2.2	Cumplimiento con políticas y estándares de seguridad	0,00 %						
	18.2.3	Revisión del cumplimiento técnico	0,00 %						

Anexo 3

DOCUMENTO DE CALIDAD		
Nombre de la organización:		
Representante de la dirección:		
TIPO DE AUDITORÍA		
☐ Auditoría Interna	☐ Auditoría Externa	☐ Seguimiento
Líder : **Equipo auditor:**		
Objetivos de Auditoría:		
Alcance de Auditoría:		
Criterio de Auditoría & Documentos de Referencia:		

Idioma:	
Fecha:	
Lugar / Sitio de Auditoría:	

Código de Activo	Título de objetivo	Descripción de objetivo	Control	Título de Procedimiento de Organización	Descripción de Procedimiento de Auditoría	Identificador del procedimiento	¿Prevenir o detectar?
SW001	Control de acceso a sistemas y aplicaciones	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	A.9.4.1	Control de restricción de acceso a la información	El acceso a la información debe restringirse en base a las funciones que se desempeñan por parte de los empleados de acuerdo a la política de control de accesos.	CAC-01	Prevenir
SW001	Control de acceso a sistemas y aplicaciones	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	A.9.4.2	Procedimiento de Inicio de Sesión	Los inicios de sesión por parte de los usuarios se deben controlar por medio de un procedimiento seguro de inicio de sesión	CAC-02	Prevenir

Declaración de Confidencialidad: Todas las informaciones evidenciadas durante la realización de esta Auditoría serán tratadas en estricta confidencialidad, y no serán reveladas a un tercero sin el consentimiento escrito de la organización.

Anexo 4

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	**Sección**	**Objetivo de control / control**			
5. Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información			
	5.1.1	Políticas de seguridad de la información			
	5.1.2	Revisión de las políticas de seguridad de la información			
6. Organización de la Seguridad de la Información	6.1	Organización interna			
	6.1.1	Roles y responsabilidad de seguridad de la información			
	6.1.2	Segregación de deberes			
	6.1.3	Contacto con autoridades			
	6.1.4	Contacto con grupos de interés especial			
	6.1.5	Seguridad de la información en la gestión de proyectos			
	6.2	Dispositivos móviles y teletrabajo			
	6.2.1	Política de dispositivos móviles			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	6.2.2	Teletrabajo			
7. Seguridad en los Recursos Humanos	7.1	Previo al empleo			
	7.1.1	Verificación de antecedentes			
	7.1.2	Términos y condiciones del empleo			
	7.2	Durante el empleo			
	7.2.1	Responsabilidades de la Alta Gerencia			
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información			
	7.2.3	Proceso disciplinario			
	7.3	Terminación y cambio de empleo			
	7.3.1	Termino de responsabilidades o cambio de empleo			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
8. Gestión de Activos	8.1	Responsabilidad de los activos			
	8.1.1	Inventario de activos			
	8.1.2	Propiedad de activos			
	8.1.3	Uso aceptable de los activos			
	8.1.4	Devolución de activos			
	8.2	Clasificación de la información			
	8.2.1	Clasificación de la información			
	8.2.2	Etiquetado de la información			
	8.2.3	Manejo de activos			
	8.3	Manejo de medios			
	8.3.1	Gestión de medios removibles			
	8.3.2	Eliminación de medios			
	8.3.3	Transporte de medios físicos			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
9. Control de Acceso	9.1	Requisitos del negocio para el control de acceso			
	9.1.1	Política de control de acceso			
	9.1.2	Acceso a redes y a servicios en red			
	9.2	Gestión de acceso de usuarios			
	9.2.1	Registro y cancelación del registro de usuarios			
	9.2.2	Suministro de acceso de usuarios			
	9.2.3	Gestión de derechos de acceso privilegiado			
	9.2.4	Gestión de información de autenticación secreta de usuarios			
	9.2.5	Revisión de los derechos de acceso de usuarios			
	9.2.6	Retiro o ajuste de los derechos de acceso			
	9.3	Responsabilidades de los usuarios			
	9.3.1	Uso de información de autenticación secreta			
	9.4	Control de acceso a sistemas y aplicaciones			
	9.4.1	Restricción de acceso a la información			
	9.4.2	Procedimientos de ingreso seguro			
	9.4.3	Sistema de gestión de contraseñas			
	9.4.4	Uso de programas y utilitarios privilegiados			
	9.4.5	Control de acceso a códigos fuente de programas			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	**Sección**	**Objetivo de control / control**			
10. Criptografía	10.1	Controles criptográficos			
	10.1.1	Política en el uso de controles criptográficos			
	10.1.2	Gestión de llaves			
11. Seguridad Física y del Entorno	11.1	Áreas seguras			
	11.1.1	Perímetro de seguridad físico			
	11.1.2	Controles físicos de entrada			
	11.1.3	Seguridad de oficinas, habitaciones y facilidades			
	11.1.4	Protección contra amenazas externas y del ambiente			
	11.1.5	Trabajo en áreas seguras			
	11.1.6	Áreas de entrega y carga			
	11.2	Equipo			
	11.2.1	Instalación y protección de equipo			
	11.2.2	Servicios de soporte			
	11.2.3	Seguridad en el cableado			
	11.2.4	Mantenimiento de equipos			
	11.2.5	Retiro de activos			
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones			
	11.2.7	Eliminación segura o reúso del equipo			
	11.2.8	Equipo de usuario desatendido			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	11.2.9	Política de escritorio limpio y pantalla limpia			
12. Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades			
	12.1.1	Documentación de procedimientos operacionales			
	12.1.2	Gestión de cambios			
	12.1.3	Gestión de la capacidad			
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación			
	12.2	Protección de Software Malicioso			
	12.2.1	Controles contra software malicioso			
	12.3	Respaldo			
	12.3.1	Respaldo de información			
	12.4	Bitácoras y monitoreo			
	12.4.1	Bitácoras de eventos			
	12.4.2	Protección de información en bitácoras			
	12.4.3	Bitácoras de administrador y operador			
	12.4.4	Sincronización de relojes			
	12.5	Control de software operacional			
	12.5.1	Instalación de software en sistemas operacionales			
	12.6	Gestión de vulnerabilidades técnicas			
	12.6.1	Gestión de vulnerabilidades técnicas			
	12.6.2	Restricciones en la instalación de software			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	12.7	Consideraciones de auditoría de sistemas de información			
	12.7.1	Controles de auditoría de sistemas de información			
13. Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red			
	13.1.1	Controles de red			
	13.1.2	Seguridad en los servicios en red			
	13.1.3	Segregación en redes			
	13.2	Transferencia de información			
	13.2.1	Políticas y procedimientos para la transferencia de información			
	13.2.2	Acuerdos en la transferencia de información			
	13.2.3	Mensajería electrónica			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	13.2.4	Acuerdos de confidencialidad o no-revelación			
14. Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información			
	14.1.1	Análisis y especificación de requerimientos de seguridad			
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas			
	14.1.3	Protección de transacciones en servicios de aplicación			
	14.2	Seguridad en el proceso de desarrollo y soporte			
	14.2.1	Política de desarrollo seguro			
	14.2.2	Procedimientos de control de cambios del sistema			
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa			
	14.2.4	Restricción de cambios en paquetes de software			
	14.2.5	Principios de seguridad en la ingeniería de sistemas			
	14.2.6	Entorno de desarrollo seguro			
	14.2.7	Desarrollo tercerizado			
	14.2.8	Pruebas de seguridad del sistema			
	14.2.9	Pruebas de aceptación del sistema			
	14.3	Datos de prueba			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	14.3.1	Protección de datos de prueba			
15. Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor			
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor			
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor			
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones			
	15.2	Gestión de entrega de servicios de proveedor			
	15.2.1	Monitoreo y revisión de servicios del proveedor			
	15.2.1	Gestión de cambios a los servicios del proveedor			
16. Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras			
	16.1.1	Responsabilidades y procedimientos			
	16.1.2	Reporte de eventos de seguridad de la información			
	16.1.3	Reporte de debilidades de seguridad de la información			
	16.1.4	Valoración y decisión de eventos de seguridad de la información			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	**Sección**	**Objetivo de control / control**			
	16.1.5	Respuesta a incidentes de seguridad de la información			
	16.1.6	Aprendizaje de incidentes de seguridad de la información			
	16.1.7	Colección de evidencia			
17. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información			
	17.1.1	Planeación de la continuidad de la seguridad de la información			
	17.1.2	Implementación de la continuidad de la seguridad de la información			
	17.1.3	Verificación, revisión y evaluación de la continuidad del negocio			
	17.2	Redundancias			
	17.2.1	Disponibilidad de facilidades de procesamiento de información			
18. Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales			
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales			
	18.1.2	Derechos de propiedad intelectual (IPR)			
	18.1.3	Protección de registros			
	18.1.4	Privacidad y protección de información personal identificable (PIR)			
	18.1.5	Regulación de controles criptográficos			
	18.2	Revisiones de seguridad de la información			
	18.2.1	Revisión independiente de seguridad de la información			
	18.2.2	Cumplimiento con políticas y estándares de seguridad			

Controles de Seguridad			Técnica usada	Aplicable (Si/No)	Referencia/Documento
Cláusula	Sección	Objetivo de control / control			
	18.2.3	Revisión del cumplimiento técnico			

Anexo 5

MODELO DE ENTREVISTA		
Propósito de este papel de trabajo:		
Proceso/Procedimiento/Política:		
Dueño del proceso/procedimiento/política:		
Auditor:		
Entrevistado:		
Nombre del Activo:		
Fecha de entrevista:		
1.- Información relacionada con: **Dominio: "A.9 Control de Acceso"** **Control: A.9.4 " Control de acceso a sistemas y aplicaciones"**		
Pregunta 1:		
Pregunta 2:		
Pregunta 3:		
Pregunta ……		
2.- Información / Documentos a solicitar para revisión:		
3.- Actividades próximas a realizarse.		
Actividad	**Fecha**	**Responsable**
Recordatorio de la comunicación que proveerá el auditor.		
[Recordar al auditor la importancia de:] • Formar conclusiones claras por escrito sin lenguaje restrictivo ni información contradictoria, que no se deban expresar como aseguramiento negativo. • Cerciorarse de que toda la documentación relevante se incluya en este documento, e informar oportunamente al equipo auditor de los asuntos significativos que puedan impactar la seguridad informática.		

Anexo 6

Principios de Seguridad Informática			
Criterio	**Definición**	**Puntaje**	**Observación**
Confidencialidad:	Verificar si en el diseño propuesto se consideran controles para proteger el acceso no autorizado a los activos de información.	100	Se evidencia en: Capítulo 3: Revisión del documento de aplicabilidad. Capítulo 4: Revisión del documento de calidad y Revisión de las Cláusulas de la Norma ISO 27001.
Integridad:	Verificar si en el diseño propuesto incluye mecanismos para garantizar que la información no sea modificada por personas/entidades no autorizadas, como controles de integridad de datos, registros de auditoría, etc.	100	Se evidencia en: Capítulo 3: Revisión del documento de aplicabilidad. Capítulo 4: Revisión del documento de calidad y Revisión de las Cláusulas de la Norma ISO 27001.
Disponibilidad:	Verificar si en el diseño propuesto se consideran controles que abordan la disponibilidad de los activos de información y de los sistemas para usuarios autorizados, mediante controles como copias de respaldo, planes de contingencia, registros de auditoría, etc.	50	Se evidencia en: Capítulo 3: Revisión del documento de aplicabilidad. Capítulo 4: Revisión del documento de calidad y Revisión de las Cláusulas de la Norma ISO 27001. Nota: No se realiza

			la revisión del dominio de control A.12 SEGURIDAD DE LAS OPERACIONES, en el que se encuentra el control de COPIAS DE RESPALDO, sin embargo si se indica que se realiza un entendimiento general de la organización en el que se incluye los procesos de TI, en el capítulo 3, además los formatos establecidos son flexibles, por lo que se pueden agregar más controles para las revisiones.
Autenticidad:	Verificar en el diseño propuesto la inclusión de controles para autenticar la identidad de usuarios, procesos y dispositivos que acceden a los activos de información, como gestión de identidades y accesos.	100	Se evidencia en: Capítulo 3: Revisión del documento de aplicabilidad. Capítulo 4: Revisión del documento de calidad y Revisión de las Cláusulas de la Norma ISO 27001.

Principios de Auditoría Informática			
Criterio	**Definición**	**Puntaje**	**Observación**
Preparación y planificación:			
Documentación previa:	El diseño propuesto debe incluir lineamientos para la documentación adecuada de las evidencias y hallazgos de la auditoría. Debe establecer un formato y estructura para el informe final de auditoría, incluyendo recomendaciones.	100	Se evidencia en: Todo el Capítulo 3: Diseño del esquema del alcance de la auditoría. Todo el Capítulo 4: Diseño del esquema de desarrollo de la auditoría. Capítulo 5: Resultados de la Auditoría y Revisiones Posteriores.
Plan de auditoría:	En el diseño propuesto debe existir un plan de auditoría que incluya objetivos claros, alcance, metodología y cronograma.	100	Se evidencia en: Capítulo 4: Diseño del esquema de desarrollo de la auditoría.
Enfoque basado en riesgos:	En el diseño propuesto se debe comprobar que se priorice la evaluación de los controles de acceso a los activos de información críticos y de mayor riesgo para la organización.	100	Se evidencia en: Capítulo 3: Identificación de Procesos críticos y de activos de información críticos.
Ejecución de la Auditoría:			

Recopilación de Evidencia:	En el diseño propuesto debe existir el uso de técnicas adecuadas para recopilar evidencia objetiva y relevante (entrevistas, revisiones de registros, observación directa).	50	Se evidencia en: Capítulo 3: Entendimiento del Contexto Organizacional (memos) Capítulo 4: Revisión de las Cláusulas de la Norma ISO 27001 (Entrevistas) Nota: Adicionalmente se mencionan las distintas técnicas que se pueden usar para la recopilación de evidencia en el capítulo 1.
Herramientas y Técnicas:	El diseño propuesto debe definir las técnicas y herramientas de auditoría a utilizar para evaluar los controles de acceso (ej. herramientas de análisis de logs, software de pruebas de penetración, políticas, etc.)	50	Se evidencia en: Capítulo 4: Revisión de las Cláusulas de la Norma ISO 27001 (políticas). Nota: Adicionalmente se mencionan las distintas técnicas y herramientas que se pueden usar en el capítulo 4.
Metodología Consistente:	El diseño propuesto debe incluir una metodología clara y estructurada para la planificación, ejecución y seguimiento de la auditoría.	100	Se evidencia en: Capítulo 1: Metodología Nota: Adicionalmente se menciona la metodología en

			cada capítulo.
Análisis y Evaluación:			
Evaluación de Controles:	El diseño propuesto debe incluir un análisis de la efectividad de los controles de acceso en función de los principios de seguridad informática (confidencialidad, integridad, disponibilidad)	50	Se evidencia en: Capítulo 3: Revisión del documento de aplicabilidad. Capítulo 4: Revisión del documento de calidad y Revisión de las Cláusulas de la Norma ISO 27001.
Identificación de Brechas:	El diseño propuesto debe tener la capacidad para identificar brechas y debilidades en los controles de acceso.	50	Se evidencia en: Capítulo 4: Revisión de las Cláusulas de la Norma ISO 27001. Nota: En el capítulo 4, se mencionan muchas técnicas que se pueden usar para la identificación de brechas, sin embargo para ejemplo sólo se usa 1, pero si se puede usar varias a la vez, y así se tendría un mayor rango de visibilidad de brechas.
Recomendaciones Prácticas:	El diseño propuesto debe incluir recomendaciones prácticas y específicas para la realización de la auditoría en los controles de acceso.	100	Se evidencia en todo el documento.

Comunicación y Reporte:			
Claridad y Precisión:	El diseño propuesto debe tener la redacción de informes de auditoría claros, precisos y comprensibles.	100	Se evidencia en: Capítulo 5: Resultados de la Auditoría.
Presentación de Resultados:	El diseño propuesto debe tener la capacidad para presentar los resultados de la auditoría de manera efectiva a diferentes audiencias (ejecutivos, equipo técnico, etc.).	100	Se evidencia en: Capítulo 5: Resultados de la Auditoría.
Seguimiento de Hallazgos:	El diseño propuesto debe establecer un plan de acción para el seguimiento de los hallazgos y la implementación de las recomendaciones.	100	Se evidencia en: Capítulo 5: Revisiones posteriores.
Adaptabilidad y Flexibilidad:			
Adaptación a Cambios:	El diseño propuesto debe tener la capacidad para adaptarse a cambios imprevistos durante la auditoría, como descubrimiento de nuevas brechas o cambios en el entorno tecnológico.	100	Se evidencia en: Los formatos establecidos en todo el proceso de la auditoría.
Innovación:	El diseño propuesto debe usar enfoques innovadores y herramientas nuevas para mejorar la efectividad de la auditoría.	50	Se evidencia en: Los formatos establecidos en todo el proceso de la auditoría.
Cumplimiento Normativo:			

Alineación con la norma ISO 27001	El diseño propuesto debe cubrir todos los controles de acceso establecidos en la norma ISO 27001, específicamente en el dominio “Control de acceso”. Los objetivos y alcance de la auditoría deben estar claramente definidos y alineados con los requisitos de la norma.	100	Se evidencia en todo el documento.