# FORTALECIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL ÁREA ADMINISTRATIVA DE COMBUSCOL SA

# STRENGTHENING OF THE INFORMATION SECURITY POLICIES OF THE ADMINISTRATIVE AREA OF COMBUSCOL SA

**Ing. Carlos Eduardo Gutiérrez Berbesi**
**Ing. Herman Montenegro Jimenez**
**Ing. José Luis Cárdenas Rozo**

**Ing. Héctor Manuel Herrera Herrera**

## RESUMEN

El presente proyecto de investigación se construye a través de una metodología cualitativa y descriptiva con el fin analizar y fortalecer las políticas de seguridad en la empresa COMBUSCOL SA, su función principal es mitigar los riesgos, amenazas y vulnerabilidades, proteger los activos y así mantener la Integridad, Confidencialidad y Disponibilidad de la información.

Así como detectar e identificar patrones a través de políticas para definir eventos sospechosos en el tráfico de información, que generen alertas tempranas, y permitan responder de la forma más efectiva ante cualquier amenaza de ataque a sus activos de información.

***Palabras clave:*** confidencialidad, integridad, disponibilidad, controles de acceso y riesgos.

## ABSTRACT

This project is built through a qualitative and descriptive methodology in order to analyze and reinforcement security policies in COMBUSCOL SA company, it´s main function is mitigate risks, threats and vulnerabilities, protect assets and in this way maintain the integrity, confidentiality and availability of information.

As well detect and identify patterns through policies to define suspicious events in data traffic to generate early warnings and allow to respond most effectively to any threat of attack on the information assets.



***Keywords:*** *confidentiality, integrity, availability, access controls and risks.*


## INTRODUCCIÓN

Las Tecnologías de Información son recursos esenciales para la productividad y competitividad de las organizaciones; sin embargo, como cualquier recurso, está sujeto a múltiples amenazas que se pueden materializar en riesgos, con múltiples consecuencias.

Hoy en día las amenazas tecnológicas son parte de nuestra cotidianeidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de ransomware hasta amenazas sofisticadas como los ataques día cero (en inglés, zero-day attack) lo cual requiere la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información (Francisco Javier Valencia-Duque, 2017).

A través de la historia la información siempre ha estado presente en todos los aspectos de la vida y el ser humano le ha dado un valor subjetivo, por lo que actualmente se considerada el segundo mayor activo de una empresa porque es uno de los recursos fundamentales para el desarrollo normal de los procesos que manejen y los cuales son la razón de ser de la organización.

Es indiscutible la importancia que tiene la información para una organización por lo que se puede tomar como referente la definición que da la ISO 27001/2013 “La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente”, de acuerdo a lo anterior es necesario que las organizaciones tomen las medidas necesarias para mantener protegida la información y así mismo los sistemas en los que se encuentra soportada esta.

Este proyecto es basado en la operación y manejo de la información del área administrativo de la compañía COMBUSCOL SA. En la cual se fortalecerán las políticas de seguridad que permitan proteger la información a través de acciones de aseguramiento para los tres pilares: Integridad, Confidencialidad y Disponibilidad.

**Pregunta investigación**

¿Cómo fortalecer las políticas de seguridad de la información del área administrativa de COMBUSCOL SA, para la detección, prevención, protección y seguridad de los activos de información, frente a los riesgos y accesos no autorizados?

**Objetivo general**

Fortalecer las políticas de seguridad que permitan proteger la información de COMBUSCOL SA en su área Administrativa, a través de acciones de aseguramiento de la información, teniendo en cuenta los requisitos operativos y tecnológicos de seguridad de la compañía, con el fin de asegurar el cumplimiento de los principios de la información: Integridad, Confidencialidad y Disponibilidad.

**Objetivos específicos**

- ✓ Identificar las falencias o debilidades de los principios de seguridad de la información, integridad, confidencialidad y disponibilidad en Combuscol SA.

- ✓ Proponer controles a través de la Norma ISO 27001/2013 para consolidar las políticas de seguridad en Combuscol SA
- ✓ Fortalecer el cumplimiento a los lineamientos de usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo en Combuscol SA.

**Alcance**

Es basado en el fortalecimiento de tres lineamientos específicos de las políticas de seguridad de la información: uso de usuarios y contraseñas, uso del correo electrónico y uso del almacenamiento externo, esto aplicaría para todos los funcionarios del área Administrativa de COMBUSCOL SA.

## REFERENTES TEÓRICOS

**Antecedentes**

Este proyecto es basado en la operación y manejo de la información del área administrativo de la compañía combustibles de Colombia SA o COMBUSCOL SA.

COMBUSTIBLES DE COLOMBIA S.A. es una compañía 100% colombiana, creada en marzo de 2005. Como agentes Comercializadores Minoristas e Industriales de la cadena de abastecimiento de combustibles, operamos una red de Estaciones de Servicio en importantes ciudades del país como Bogotá, Cali, Medellín, Pasto, Ipiales y Santa Marta; y suministramos combustible a nivel industrial, enmarcados dentro del Decreto 4299 de Minminas y sus modificatorios.

Con más de diez años de experiencia; Combuscol se constituye como una empresa operadora de una red de Estaciones de Servicio, realizando actividades de comercialización y distribución de combustibles, lubricantes y demás derivados del petróleo.

La compañía, también presta servicios relacionados que hacen de las Estaciones, lugares integrales en donde los clientes pueden tanquear su vehículo con TECHRON, un aditivo de gran calidad para la conservación del motor de los vehículos y realizar actividades adicionales como lavado, cambio

de aceite, lubricentro, montallantas y tienda.

Combuscol cuenta con una amplia experiencia en el transporte, almacenamiento y control de suministro de combustible, lo que nos permite asesorar a nuestros clientes para que puedan operar de manera segura y eficiente.

Desde el inicio, Combuscol ha tenido la visión de satisfacer la necesidad de los clientes, implementando servicios y promociones que hacen de la Red de Estaciones de Servicio, una ruta importante para seguir y utilizar gracias al Servicio Superior que se presta, con un excelente equipo humano; pilar fundamental de la compañía, que trabaja viviendo los principios y valores para generar satisfacción a los clientes; bienestar y calidad de vida para los empleados y sus familias; rentabilidad para los accionistas y progreso para la sociedad. (COMBUSCOL, s.f.)

Combuscol SA nos suministró el documento de Políticas de seguridad que manejan actualmente y el cual fue fuente de análisis e investigación.

En la investigación realizada a la compañía COMBUSCOL SA identificamos que las políticas de seguridad establecidas actualmente no cuentan con el referente normativo, hay algunas que faltan y otras por mejorar.

**Estado del arte**

La información se convirtió en el activo más importante para COMBUSCOL S.A. toda vez cuando es completa, precisa y actualizada, es fundamental en la toma de decisiones. COMBUSCOL S.A. es una empresa conformada por personas, recursos materiales e información, la información nos determina el orden y el caos entre los individuos y la interrelación entre personas-recursos. (Raúl J. Martelo, 2015) (Raúl J. Martelo, 2015)

Los sistemas de información a medida que se consultan almacenan y generan información, ponen en riesgo la integridad de la misma; el riesgo no solo proviene del exterior sino también del interior de la organización. Los virus, gusanos, hackers, phishing e ingenieros sociales entre otras. Son amenazas constantes que atentan contra la información de COMBUSCOL S.A. un hacker puede causar pérdidas considerables para COMBUSCOL S.A como lo es robo de datos de clientes, la seguridad de la información no es solo cuestión de tener nombres de usuario y contraseñas, sino

que requiere de unas reglas y diversas políticas de privacidad y protección de datos, estas políticas deben ser integral y encajar en COMBUSCOL sin problemas. (Raúl J. Martelo, 2015)

Hoy en día las amenazas hacen parte de nuestra vida diaria, algunas van desde diversas formas de virus, ataques de ransonware y sofisticados ataques de día cero (en inglés, zero day attack), por esta razón se va a fortalecer el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27000 para la preservación de la confidencialidad, integridad y disponibilidad de la información. (Raúl J. Martelo, 2015)

Uno de los aspectos que se deben tener en cuenta y que no es a menudo claramente comprendido, es que un proyecto de SGSI no es un proyecto del área de Tecnologías de la Información, es un proyecto organizacional y como tal requiere la aprobación y el apoyo de la Dirección para avanzar en su adecuada implementación. Para el fortalecimiento de los SGSI es necesario conocer a fondo las prioridades, que tiene COMBUSCOL S.A. y así llegar a cubrir los diferentes objetivos de COMBUSCOL S.A. y justificar más a una su necesidad en el fortalecimiento del SGSI. (Francisco Javier Valencia-Duque, 2017)

El fortalecimiento y mejora del sistema de gestión de la seguridad de la información de COMBUSCOL S.A. se hará por medio de la norma ISO 27001, esta norma es basada en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar las políticas de la seguridad de la información en la organización. Para un funcionamiento eficaz de COMBUSCOL S.A. se debe identificar y gestionar muchas actividades, un proceso es cualquier actividad que use recursos y cuya gestión permita la transformación de entradas y salidas. A menudo el resultado de un proceso constituye la entrada del proceso siguiente. ((ICONTEC) I. C., 2006)

La seguridad de la información es una disciplina en la que en muchos casos incomoda, la información se convirtió en un activo muy importante para la organización, toda vez cuando es completa, precisa y actualizada. La información es muy importante para la toma de decisiones; la organización es formada por personas, recursos materiales e información, la información a medida que se consulta almacena y se genera más información es ahí cuando es vulnerable y se pone en riesgo la integridad de la misma. (Francisco Javier Valencia-Duque, 2017)

La diversidad y complejidad de los componentes del sistema de tecnología de la información (TI) ha aumentado significativamente en los últimos años. En consecuencia, para que COMBUSCOL S.A. proteja adecuadamente estos sistemas, se han desarrollado varios estándares y marcos. Dichos marcos deben ser aplicables a todo tipo de sectores comerciales, ya sean gubernamentales o privados, empresariales o de pequeñas empresas. Muchas empresas han aplicado en la práctica los marcos NIST SP 800-53 e ISO/IEC 27001:2013. (Ibrahim, 2018)

ISO 27001:2013

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.

La presente Norma puede ser usada por partes internas y externas para evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la propia organización.

El orden en que se presentan los requisitos en esta Norma no refleja su importancia ni el orden en

el que se van a implementar. Los elementos de la lista se enumeran solamente para propósitos de referencia.

La ISO/IEC 27000 describe la visión general y el vocabulario de sistemas de gestión de la seguridad de la información, y referencia la familia de normas de sistemas de gestión de la seguridad de la información (incluidas las NTC-SO/IEC 27003[2], ISO/IEC 27004[3] y ISO/IEC 27005[4]), con los términos y definiciones relacionadas. ((ICONTEC) E. p., 2013)

Las revisiones de NIST SP 800-53 se realizan de acuerdo con los cambios en las responsabilidades según la Ley Federal de Administración de Seguridad de la Información (FISMA), Ley Pública (PL) 107-347. La última versión de este marco consta de cinco funciones (Identificar, Proteger, Detectar, Responder y Recuperar), 22 categorías y 98 subcategorías. Este marco utiliza un modelo de seguridad de cuatro niveles (parcial, basado en el riesgo, repetible y adaptativo) y un proceso de siete pasos (priorizar y determinar el alcance, orientar, crear un perfil actual, realizar una evaluación de riesgos, crear un perfil objetivo, determinar, analizar y priorizar las brechas e implementar el plan de acción). Se enfoca en evaluar la situación actual al determinar cómo evaluar la seguridad, cómo considerar el riesgo y cómo resolver las amenazas a la seguridad. (Ibrahim, 2018)

## METODOLOGÍA

En este capítulo se describe la Metodología para el presente trabajo de investigación, el diseño propuesto conlleva a los pasos de consolidación y fortalecimiento de las políticas de seguridad en Combuscol S.A. teniendo en cuenta un enfoque cualitativo y descriptivo.


*Figura 1 Desarrollo de la metodología*

**Investigación Preliminar**

Este proyecto es basado en la operación administrativa de la compañía Combuscol S.A.

En búsqueda del Proyecto de aplicación para la presente especialización de seguridad de la información, nos basamos en la compañía donde labora uno de nuestros compañeros denominada COMBUSCOL S.A. ya que no maneja normatividad a nivel de las políticas de seguridad de la información.

**Análisis de la situación Actual**

Durante esta fase se analiza y documenta: el contexto de la organización, las políticas de seguridad actuales, la normatividad vigente en cuanto a estas y las buenas prácticas en Seguridad de la Información.

**Propuestas de mejoras**

En esta fase se documenta, se realizan recomendaciones y se propone que Combuscol S.A. adopte buenas prácticas, ceñidas a la norma para que haya una buena gestión de la seguridad de la información.

**Resultados de la investigación**

En esta última fase se muestra el resultado de la investigación, propuestas de mejora y sus conclusiones respectivas.

## ANALISIS Y RESULTADOS

### GAP

El análisis inicial a la compañía COMBUSCOL S.A. se realizó por medio del GAP (análisis de brechas). Por medio de este análisis se encontró los siguientes resultados

*Tabla 1 Estado de Controles*

| ESTADO | CRITERIO |
|---|---|
| Inexistente | No se lleva a cabo el control de seguridad en los sistemas de información. |
| Inicial | Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad. |
| Repetible | La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación. |
| Definido | El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección. |
| Administrado | El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado. |
| Optimizado | El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores. |
| No aplicable | A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración. |

***Fuente:*** *(Gary@isect.com, s.f.)*

De acuerdo a la tabla 1 existe una medición de controles del GAP, (análisis de brechas) donde nos muestra el detalle de criterio significativo de cada uno de los estados. Se tiene el estado más crítico llamado inexistente, es cuando no se tiene un control de seguridad establecido. Y existe el estado optimo que es más recomendable a plasmar, debido que existe el control, se aplica bajo un procedimiento, este mismo es aprobado y se mide periódicamente.

*Tabla 2 Nivel de Madurez Combuscol SA*

| Nivel de Madurez de Combuscol SA | | | |
|---|---|---|---|
| **Item** | **Código** | **Control** | **Estado de Madurez Actual** |
| 1 | A.8.3.1. | Gestión de soportes extraíbles | **Inicial** |
| 2 | A.8.3.2. | Eliminación de soportes | **Inexistente** |
| 3 | A.8.3.3. | Soportes físicos en tránsito | **Inicial** |
| 4 | A.9.2.1. | Registro y baja de usuario | **Inicial** |
| 5 | A.9.2.2. | Provisión de acceso de usuario | **Definido** |
| 6 | A.9.2.3. | Gestión de privilegios de acceso | **Inicial** |
| 7 | A.9.2.4. | Gestión de la información secreta de autenticación de los usuarios | **Inexistente** |
| 8 | A.9.2.5. | Revisión de los derechos de acceso de usuario | **Inexistente** |
| 9 | A.9.2.6. | Retirada o reasignación de los derechos de acceso | **Inicial** |
| 10 | A.9.4.1. | Restricción del acceso a la información | **Definido** |
| 11 | A.9.4.2. | Procedimientos seguros de inicio de sesión | **Repetible** |
| 12 | A.9.4.3. | Sistema de gestión de contraseñas | **Inicial** |
| 13 | A.9.4.4. | Uso de utilidades con privilegios del sistema | **Definido** |
| 14 | A.9.4.5. | Control de acceso al código fuente de los programas | **Inicial** |
| 15 | A.10.1.1 | Política de uso de los controles criptográficos | **Inexistente** |
| 16 | A.10.1.2 | Gestión de claves | **Inexistente** |
| 17 | A.13 2.1. | Políticas y procedimientos de intercambio de información | **Inicial** |
| 18 | A.13 2.2. | Acuerdos de intercambio de información | **Inicial** |
| 19 | A.13 2.3. | Mensajería electrónica | **Inicial** |
| 20 | A.13 2.4. | Acuerdos de confidencialidad o no revelación | **Inicial** |

***Fuente:*** *Autor.*

La evaluación de madurez realizada a profundidad para la empresa Combuscol, nos dio una visual del estado actual que se encuentra la compañía Combuscol con respecto a la seguridad de sus activos de información. Como resultado se obtiene la medición de los controles inexistentes o iniciales siendo estos los más críticos. Se identifican muy pocos controles en estado definido y un solo control en estado repetible.

Como se observa en la tabla anterior los ítems de la norma ISO 27001 2013: A.8.3.2, A.9.2.4, A.9.2.5, A.10.1.1 y A.10.2.1 se encuentran en el estado inexistente, los cuales son de prioridad en la empresa Combuscol S.A. llevarlos al estado de definido para así tener un proceso y controles donde se comunican y se documentan.

También podemos percatar que los ítems de la norma ISO 27001 2013: A.8.3.1, A.8.3.3, A.9.2.1, A.9.2.3, A.9.2.6, A.9.4.3, A.9.4.5, A.13.2.1, A.13.2.2, A13.2.3 y A.13.2.4 se encuentran en el estado inicial, la empresa Combuscol S.A. ha iniciado estos controles y reconoce que existe falencias, pero no los ha llevado a un estado de madurez definido. El código A.9.4.2 se encuentra en el estado repetible aquí los procedimientos son seguidos por varias personas, pero no se ha llevado a la comunicación formal.

Teniendo en cuenta este nivel de resultado, y siendo este muy bajo, se da a proponer controles de seguridad de la información de la norma ISO 27001 2013. Los controles propuestos, son los más compatibles y son los que cumplen para los tres lineamientos planteados. Se propone para el lineamiento uso de usuarios y contraseñas, los controles de seguridad de la información de la norma ISO 27001 2013 más acordes de la línea A.9.2, A.9.4 y A.10.1. Se propone para el lineamiento uso del correo electrónico, los controles de seguridad de la información de la norma ISO 27001 2013 más acordes de la línea A.13.2. Para el último lineamiento uso de almacenamiento externo, se propone los controles de seguridad de la información de la norma ISO 27001 2013 más acordes de la línea A.8.3.


*Figura 2 Estado de Controles Combuscol*

El resultado del diagrama sobre el estado actual, se muestra un nivel de controles inexistentes como es uno de los más altos, con una medición del 29%, y siendo este estado el más crítico, debido que no posee controles de seguridad de los sistemas de información. También se evidencia en el diagrama un nivel de controles iniciales, con una medición del 36%, también siendo este crítico, dado que algunos existen, pero no existe un proceso formal para ser ejecutados. Se identifica en el diagrama el estado de repetible, con una medición del 17%, como nivel leve, ya que la medida de aseguramiento se realiza, pero con procedimientos propios informales. Existe un estado de controles como definido, con una medición del 18%, siendo este un nivel también leve, puesto que el control si se aplica conforme a un proceso documentado, pero este no ha sido aprobado por el responsable de seguridad de la información ni el comité de dirección. Se evidencia un último estado de control como administrado, siendo este nivel medio, siendo este control acordado y aplicado bajo un procedimiento documentado formalmente y aprobado.

No se evidencian controles optimizados, con un nivel de medición del 0%. Este control de optimización es el control de nivel más alto y es un nivel que se debe medir periódicamente debido que su procedimiento debe estar documentado, aprobado y formalizado.

**Controles proactivos OWASP**

Partiendo de las políticas de seguridad actuales de Combuscol nos mostraron unas falencias en algunos controles críticos e inexistentes como los son Usuarios y contraseñas, uso de correo electrónico y el uso de almacenamiento externo; al revisar los riesgos más significativos en OWASP encontramos que en el año 2021 los riesgos mayormente materializados fueron control de acceso, fallas criptográficas y SQL inyección. Por esta razón nos enfocamos en las más grandes falencias que hoy en día tiene Combuscol. (OWASP, s.f.)

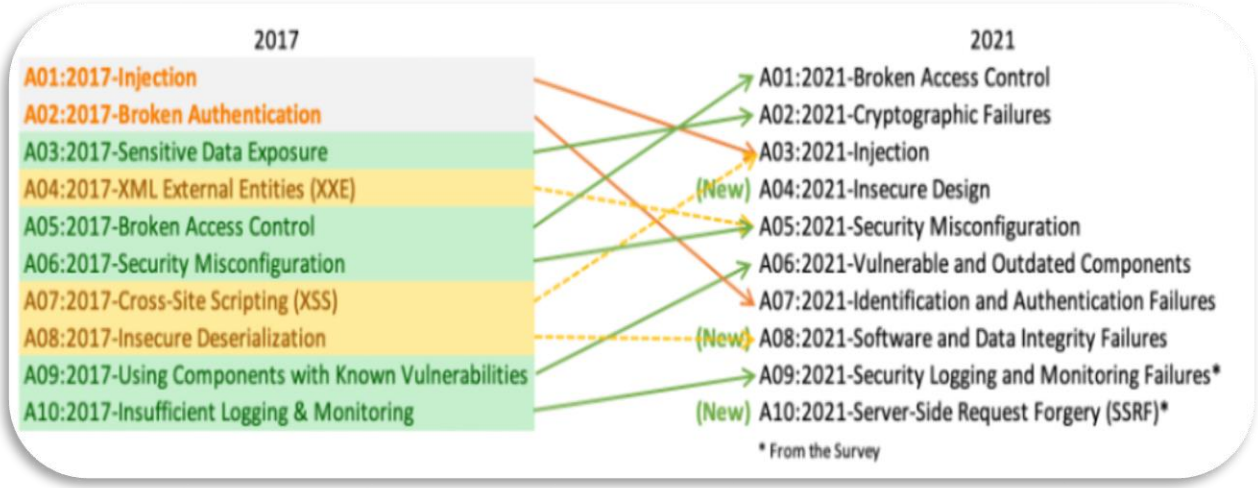


*Figura 3 OWASP Top Ten*

**Análisis de riesgos**

Con el fin de mitigar los riesgos a los que están expuestos los activos de la información de Combuscol SA, se realizara un análisis de las amenazas a los que estos están expuestos, dentro de este análisis también se evaluara la probabilidad, como el impacto que tendrían la materialización de estos riesgos.

***Identificación de activos críticos***

De acuerdo a la información suministrada por Combuscol SA, se identifican los activos de la información y su criticidad en la siguiente tabla:

***Tabla 3 Activos de la Información***

| ID | ACTIVO | TIPO DE ACTIVO | CRITICIDAD |
|---|---|---|---|
| 1 | Tecnico de Soporte | Servicio | Critico |
| 2 | Correo electronico (Gmail) | Servicio | Critico |
| 3 | Firewall Fortigate | Hardware | Muy Critico |
| 4 | Servicio de directorio activo y DNS | Servicio | Muy Critico |
| 5 | Servidor ERP Enterprise | Servicio | Muy Critico |
| 6 | BD de CRM | Servicio | Critico |
| 7 | Servidor BD Integra | Servicio | Critico |
| 8 | Servidor de Backup VEEAM | Software | Critico |
| 9 | NAS de almacenamiento | Hardware | Muy Critico |
| 10 | Sistema de CCTV | Hardware | Critico |

***Fuente:*** *Autor*

Se realizó una identificación de los activos actuales que se encuentran en producción de la empresa Combuscol S.A. y se identificó los más críticos y que van de la mano junto a los tres lineamientos identificados (Uso de usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo). Se evaluó el tipo de activo y el nivel de criticidad, con el fin de tener claridad al momento de proponer el ítem con respecto a la norma ISO 27001: 2013.

Al identificar los activos críticos, se procede a evaluar los riesgos de cada uno de estos, se procede a evaluar la probabilidad y el impacto

***Tabla 4 Evaluación de Riesgos***

| ACTIVO | RIESGO | PROBABILIDAD | IMPACTO | CONTROL / METODOLOGIA |
|---|---|---|---|---|
| Tecnico de Soporte | Revelación de información a personal no autorizado | Media | Alto | PR.DS-5 |
| Correo electronico (Gmail) | Acceso a información sensible debido a que las contraseñas de los usuarios no son seguras | Medio | Alto | A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, AC-3, AC-4 |
| Firewall Fortigate | Accesos no autorizados (a nivel de Firewall) | Medio | Muy Alto | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, PR.AC.1, PR.AC-6, PR.AC-7, PR.AC-4 |
| Servicio de directorio activo y DNS | Acceso no autorizado al sistema operativo del Servidor | Alto | Muy Alto | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, PR.AC.1, PR.AC-6, PR.AC-7, PR.AC-4 |
| Servidor ERP Enterprise | Perdida de integridad y confidencialidad por acceso de personal no autorizado | Alto | Muy Alto | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, PR.AC.1, PR.AC-6, PR.AC-7, PR.AC-4 |
| BD de CRM | Acceso interrumpido al activo y deterioro del servicio a los clientes | Medio | Alto | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, PR.AC.1, PR.AC-6, PR.AC-7, PR.AC-4 |
| Servidor BD Integra | Perdida de integridad y confidencialidad por acceso de personal no autorizado | Medio | Alto | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, PR.AC.1, PR.AC-6, PR.AC-7, PR.AC-4 |
| Servidor de Backup VEEAM | Interrupción de las actividades del sistema externo de almacenamiento y/o de la integridad y disponibilidad de la información contenida en él. | Alto | Medio | A.8.3.1, A.8.3.2, A.8.3.3, PR.DS-3, PR.IP-6. PR.PT-2 |
| NAS de almacenamiento | Modificación o Eliminación de los repositorios por errores del personal autorizado. | Bajo | Medio | A.8.3.1, A.8.3.2, A.8.3.3, PR.DS-3, PR.IP-6. PR.PT-2 |
| Sistema de CCTV | Actividades de procesamiento de información no autorizada | Bajo | Medio | A.8.3.1, A.8.3.2, A.8.3.3, PR.DS-3, PR.IP-6. PR.PT-2 |

***Fuente:*** *Autor*

Respecto a la identificación de cada uno de los activos y su nivel de criticidad sobre la posible materialización del riesgo, y para su mitigación de los mismos, se evaluó los controles y la metodología que aplica a la remediación de cada uno de los riesgos. Los controles propuestos y aplicados son referentes a la NIST y a la ISO 27001:2013.

*Tabla 5 Mapa de Riesgos*

| MAGNITUD DE RIESGO : Es el resultado de multiplicar la probabilidad por el impacto | | | | | | | |
|---|---|---|---|---|---|---|---|
| PROBABILIDAD | IMPACTO | MAGNITUD DE RIESGO | DESCRIPCIÓN DE MAGNITUD | UMBRAL DE RIESGO ACEPTADO | TOLERANCIA AL RIESGO | REQUIERE TRATAMIENTO | REQUIERE CONTINGENCIA |
| BAJA | BAJO | 1 | MUY BAJO | X | - | - | - |
| MUY BAJA | BAJO | 2 | MUY BAJO | X | - | - | - |
| BAJA | MUY BAJO | 2 | MUY BAJO | X | - | - | - |
| BAJA | MEDIO | 3 | BAJO | X | - | - | - |
| MEDIA | BAJO | 3 | BAJO | X | - | - | - |
| ALTA | MUY BAJO | 4 | BAJO | X | - | - | - |
| BAJA | BAJO | 4 | BAJO | X | - | - | - |
| MUY BAJA | ALTO | 4 | BAJO | X | - | - | SI |
| MUY ALTA | MUY BAJO | 5 | BAJO | X | - | - | - |
| MUY BAJA | MUY ALTO | 5 | BAJO | X | - | - | SI |
| MEDIO | BAJO | 6 | BAJO | X | - | - | - |
| BAJO | MEDIO | 6 | BAJO | X | - | - | - |
| ALTA | BAJO | 8 | MEDIO | - | X | SI | - |
| BAJA | ALTO | 8 | MEDIO | - | X | SI | SI |
| MEDIA | MEDIO | 9 | MEDIO | - | X | SI | - |
| MUY ALTA | BAJO | 10 | MEDIO | - | X | SI | - |
| BAJA | MUY ALTO | 10 | MEDIO | - | X | SI | SI |
| ALTA | MEDIO | 12 | ALTO | - | - | SI | - |
| MEDIA | ALTO | 12 | ALTO | - | - | SI | SI |
| MUY ALTA | MEDIO | 15 | ALTO | - | - | SI | - |
| MEDIA | MUY ALTO | 15 | ALTO | - | - | SI | SI |
| ALTO | ALTO | 16 | ALTO | - | - | SI | SI |
| ALTO | MUY ALTO | 20 | MUY ALTO | - | - | SI | SI |
| MUY ALTA | ALTO | 20 | MUY ALTO | - | - | SI | SI |
| MUY ALTA | MUY ALTO | 25 | MUY ALTO | - | - | SI | SI |

***Fuente:*** *Autor*

La medición del riesgo frente a los activos se analizó con base a la tabla 5 mapa de riesgos, obteniendo una medición del resultado de multiplicar la probabilidad por el impacto, se visualiza la magnitud de riesgo y la descripción de la magnitud (Muy bajo, bajo, medio, alto, muy alto). Con este resultado se identificó los riesgos que deben ser tratados respecto al orden de prioridad, siendo el umbral muy alto el más crítico y muy bajo o bajo la aceptación del riesgo.

*Tabla 6 Plan de Tratamiento de Riesgos*

| Plan de Tratamiento de riesgos de COMBUSCOL S.A. | | | | | |
|---|---|---|---|---|---|
| Item | Código | Control | Estado de Madurez Actual | Recomendación | Estado de Madurez Destino |
| 1 | A.8.3.1. | Gestión de soportes extraíbles | Inicial | Se debe contar con los procedimientos adecuados para los medios extraibles | Definido |
| 2 | A.8.3.2. | Eliminación de soportes | Inexistente | Generar unas instrucciones definidas de eliminacion segura de informacion en los dispositivos y almacenarlos y clasificarlos para tener disponibilidad | Definido |
| 3 | A.8.3.3. | Soportes físicos en tránsito | Inicial | Desarrollar un procedimiento que gestione e incluya cadena de custodia con sus respectivos soportes de entrega y caracteristicas | Definido |
| 4 | A.9.2.1. | Registro y baja de usuario | Inicial | Expone las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario de Combuscol para obtener acceso a los sistemas de información | Definido |
| 5 | A.9.2.2. | Provisión de acceso de usuario | Definido | El procedimiento se enviara a su aprobacion y formalizacion | Administrado |
| 6 | A.9.2.3. | Gestión de privilegios de acceso | Inicial | Se deben restringir y controlar la asignación de privilegios de acceso en los aplicativos de la compañía, según la necesidad su necesidad de uso | Definido |
| 7 | A.9.2.4. | Gestión de la información secreta de autenticación de los usuarios | Inexistente | Formalizar un procedimiento para la proteccion de las contraseñas como realizar el cambio despues de su primer uso y que se realice cambio despues de cierto periodo definido | Definido |
| 8 | A.9.2.5. | Revisión de los derechos de acceso de usuario | Inexistente | Las personas responsables de cada plataforma deberán realizar una validación de permisos de manera periódica con el fin de controlar los cambios en las labores realizadas por los funcionarios de la compañía | Definido |
| 9 | A.9.2.6. | Retirada o reasignación de los derechos de acceso | Inicial | Se deben realizar las respectivas desvinculaciones y eliminaciones de las plataformas de acuerdo a procedimiento creado | Definido |
| 10 | A.9.4.1. | Restricción del acceso a la información | Definido | 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 | Administrado |

| | | | | | |
|---|---|---|---|---|---|
| 11 | A.9.4.2. | Procedimientos seguros de inicio de sesión | Repetible | Se debe controlar el ingreso a las aplicaciones a través de un proceso definido de ingreso seguro, el proceso deberá contar con alternativas como doble factor de autentificación, tokens o medios biométricos, este proceso incluirá bloqueos por fallas de autentificación seguimiento e intentos exitosos y fallidos de ingreso terminar concesiones inactivas y determinar tiempos de conexión | Definido |
| 12 | A.9.4.3. | Sistema de gestión de contraseñas | Inicial | Se debe implantar controles que soliciten cambios de contraseña a intervalos de tiempo de un mes en los diferentes sistemas de información de la compañía | Definido |
| 13 | A.9.4.4. | Uso de utilidades con privilegios del sistema | Definido | Se debe restringir y controlar estrictamente el uso de programas utilitarios, para esto el control deberá incluir la identificación, autenticación y autorización de cada programa, de la misma manera deberá definir las características de los usuarios que tendrán permisos de su uso en la compañía | Administrado |
| 14 | A.9.4.5. | Control de acceso al código fuente de los programas | Inicial | Se debe implementar controles de acceso de doble autenticación de los sistemas donde se encuentren el código fuente como también donde se realiza el alojamiento del respaldo de la información | Definido |
| 15 | A.10.1.1 | Política de uso de los controles criptográficos | Inexistente | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información | Definido |
| 16 | A.10.1.2 | Gestión de claves | Inexistente | Se debe implementar un control para la correcta gestión de las llaves criptográficas que se utilizan para la transferencia de información con los funcionarios | Definido |
| 17 | A.13 2.1. | Políticas y procedimientos de intercambio de información | Inicial | Se debe implementar políticas, procedimientos y controles para la transferencia segura de la información que se transmite en los servidores virtuales de la compañía | Definido |
| 18 | A.13 2.2. | Acuerdos de intercambio de información | Inicial | Se debe documentar contractualmente los acuerdos de transferencia de información entre los proveedores y clientes, los cuales se deben revisar en intervalos de tiemplo planificados | Definido |
| 19 | A.13 2.3. | Mensajería electrónica | Inicial | Implementar politicas de mensajeria segura que refuercen la integridad de la informacion | Definido |
| 20 | A.13 2.4. | Acuerdos de confidencialidad o no revelación | Inicial | Se debe documentar los requisitos para los acuerdos de confidencialidad o no divulgación para los funcionarios y proveedores los cuales se deben revisar en intervalos de tiemplo planificados | Definido |

***Fuente:*** *Autor*

Se propone el plan de tratamiento de riesgo, donde se menciona los controles a sentar, desde el estado de madurez actual, al estado de madurez destino que se propone llegar. Se mencionan los controles a presentar acordes a la norma ISO 27001 2013, con respecto a los tres lineamientos a

fortalecer, uso de usuarios y contraseñas, uso del correo electrónico y uso de almacenamiento externo. Se establecen las recomendaciones para cada uno de los controles propuestos. Con función de dar cumplimento a los controles, y ser apto para la reducción de impacto y la materialización de los riesgos identificados para los tres lineamientos mencionados. Con el objeto de salvaguardar la seguridad de los activos de información de la empresa Combuscol SA.

**Ciclo propuesto de mejora**

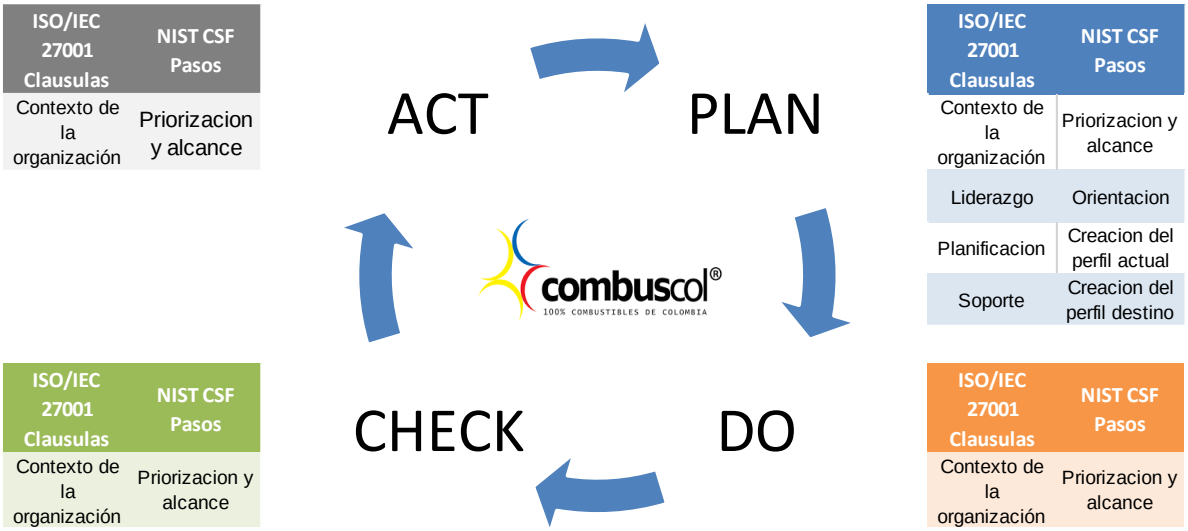


*Figura 4 Ciclo de mejora*

Para fortalecer los 3 lineamientos de usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo en Combuscol S.A. se desarrolló el ciclo propuesto de mejora partiendo de la ISO 27001:2013 la cual especifica los requisitos para establecer, implementar, mantener y mejorar los tres lineamientos escogidos para su fortalecimiento en la empresa Combuscol S.A. teniendo en cuenta los riesgos en ciberseguridad se agregó el estándar de tecnología NIST en la cual se diseñan controles específicos para mejorar la posición frente a los riesgos cibernéticos y así garantizar los procesos con excelentes procedimientos de los cuales las personas pueden ejecutar muy fácilmente.

Por lo general los problemas en los controles no se deben a fallas tecnológicas, sino a las malas prácticas de las personas que no ejecutan el proceso adecuadamente y realizan procesos que no están definidos en las políticas de gestión de seguridad de la información.

El proceso continuo de identificar, proteger, detectar, responder y recuperar nos ayuda a fortalecer los tres lineamientos de usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo en Combuscol S.A.

Combuscol S.A. debe comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Llegar a un nivel de riesgo aceptable nos lleva a cumplir con los objetivos de Combuscol S.A.

Las políticas de gestión de seguridad de la información dan a Combuscol S.A. la capacidad de mitigar el riesgo, trasferir el riesgo, evitar el riesgo o aceptar el riesgo, dependiendo del impacto potencial de los tres lineamientos usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo. La NIST utiliza procesos de gestión de riesgos para permitir que Combuscol S.A. priorice decisiones en materia de ciberseguridad. Por lo tanto, el marco de la NIST brinda a Combuscol S.A. la capacidad de seleccionar y mejorar su gestión de riesgos de ciberseguridad.

## FLUJO DE MEJORA CONTINUA

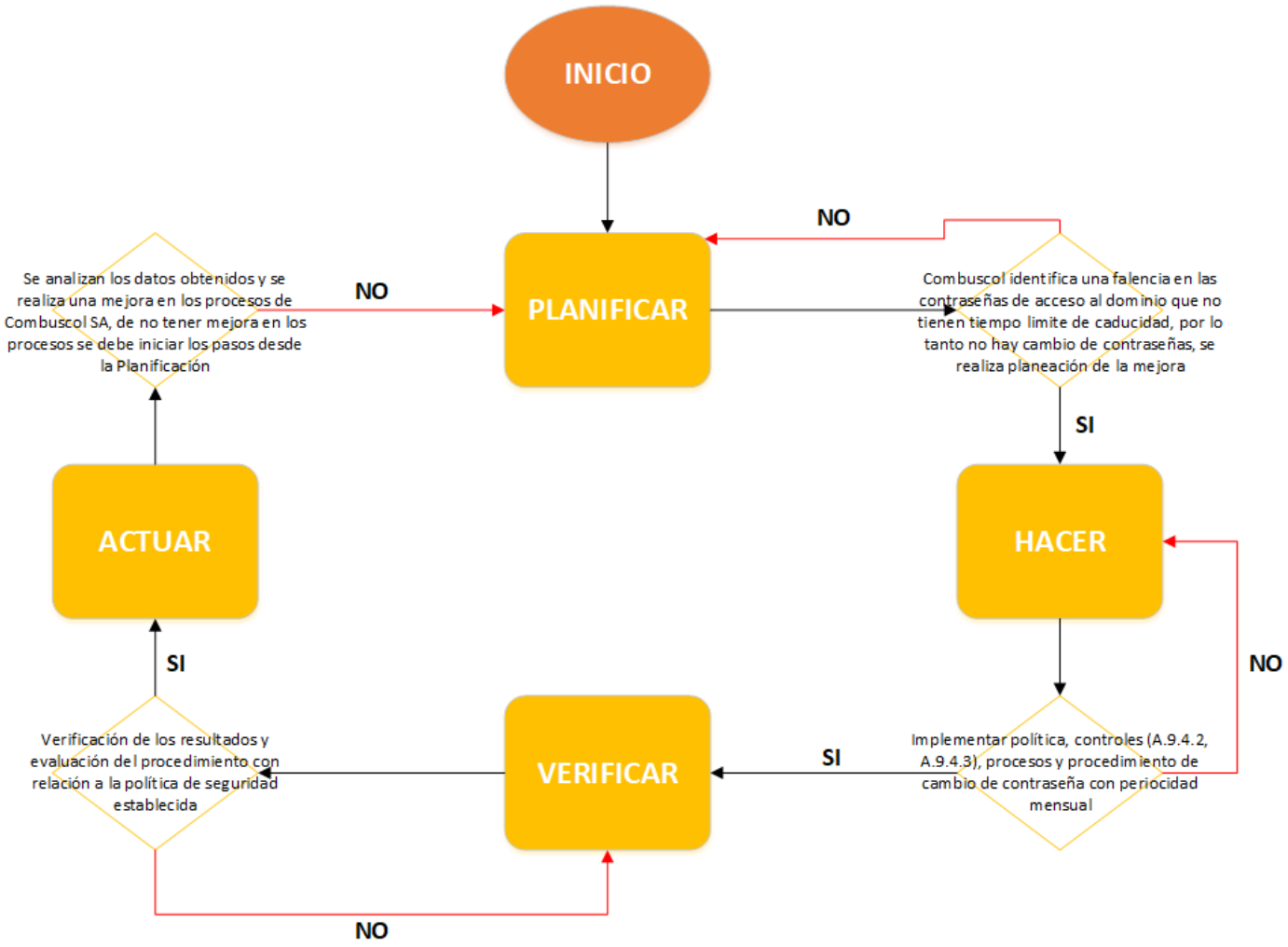


*Figura 5 Diagrama de flujo de mejora continua*

Combuscol siempre ha tenido la visión de satisfacer las necesidades de los clientes, por esto implementa servicios y promociones constantemente, por lo tanto, es necesario ejecutar procesos formales para determinar los riesgos y así identificar los controles para mitigarlos.

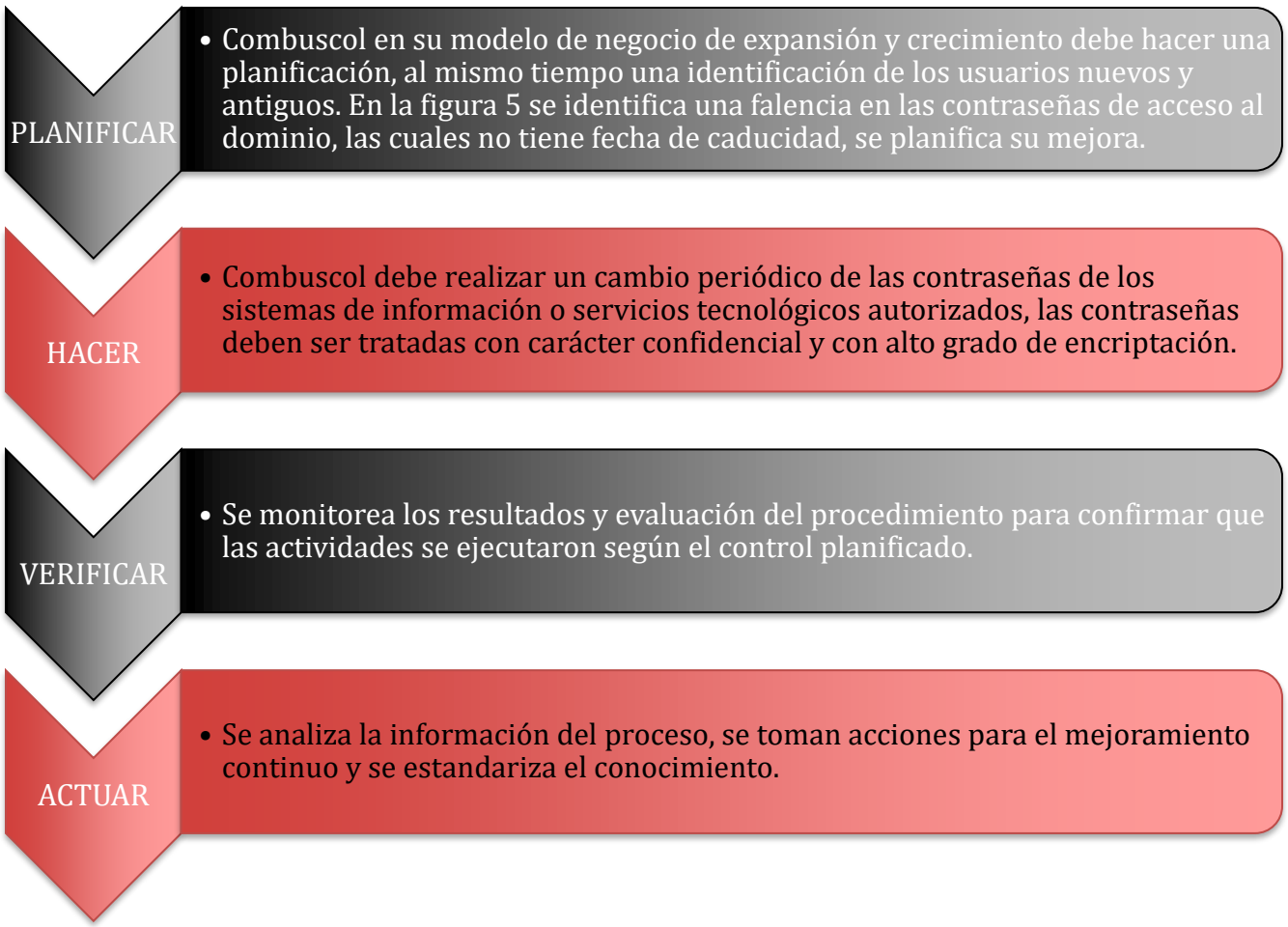


***Figura 6 PHVA***

Este trabajo de investigación se realizó bajo el referente de la norma ISO 27001 2013 la cual se encuentra vigente hasta octubre de 2025.

## CONCLUSIONES

Como resultado del análisis GAP de las políticas de seguridad existentes en Combuscol se encontró que los lineamientos: uso usuarios y contraseñas, uso de correo electrónico y uso de almacenamiento externo tiene un gran porcentaje de controles no implementados, otros existen en etapa inicial pero no son gestionados, un 29% en estado inexistente, un 36% en estado inicial, un 17% en estado Repetible, 18% en estado definido y 1% en estado Administrado.

Se recomienda que se trabaje con la norma ISO/IEC 27001 2013 para aplicar las buenas prácticas y adaptación de controles para la seguridad de la información y la adopción de un Sistema de Gestión de Políticas de Seguridad de la Información (SGSI) debería ser una decisión estratégica para COMBUSCOL S.A., se propone su implementación.

Los resultados de la investigación conllevan al fortalecimiento de los tres lineamientos de las políticas de seguridad en COMBUSCOL SA que se presentan en este documento; la siguiente propuesta quedará a consideración de la Gerencia de la compañía para ser adoptada o implementada durante el año 2023, según cumplimiento o impacto de los objetivos estratégicos de la organización. Proponiendo un Ciclo de mejora para la implementación de las políticas de seguridad de la información para Combuscol SA. descrito en este proyecto.

Se da cumplimiento de fortalecimiento sobre los tres lineamientos propuestos de las Políticas de Seguridad de la Información del presente proyecto, esto ayuda a mitigar los riesgos de seguridad donde puede estar expuesta la información en cuanto a disponibilidad, Integridad y confidencialidad.

## AGRADECIMIENTOS

A la compañía Combuscol S.A. por la colaboración, información y permitirnos elaborar este proyecto, a la universidad, docentes y compañeros.

## REFERENCIAS

(ICONTEC), E. p. (2013). NORMA TÉCNICA NTC-ISO-IEC. *ICONTEC*, 7.

(ICONTEC), I. C. (2006). NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA 27001.*ICONTEC*, 6-45.

COMBUSCOL. (s.f.). *COMBUSCOL*. Obtenido de https://www.combuscol.com/

Francisco Javier Valencia-Duque, M. O.-A. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista lbérica de Sistemas y Tecnologías de Información*, 73-88.

Gary@isect.com. (s.f.). *ISO27k ISMS and controls status with SoA and gaps Spanish*. Obtenido de https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.iso27000.es%2Fassets%2Ffiles%2FISO27k%2520ISMS%2520and%2520controls%2520status%2520with%2520SoA%2520and%2520gaps%2520Spanish.xlsx&wdOrigin=BROWSELINK

Ibrahim, A. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing*, https://link.springer.com/article/10.1007/s11227-018-2479-2#Tab2.

OWASP. (s.f.). *OWASP*. Obtenido de https://owasp.org/www-project-top-ten/

Raúl J. Martelo, J. E. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información Tecnológica – Vol. 26 Nº 2 2015*, 2-13.