Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS

Mónica Sofía Cruz Carrillo
Asesorada por el Ing. Alan Omar Espino Guerra

Guatemala, enero de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN

SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESO Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MÓNICA SOFÍA CRUZ CARRILLO
ASESORADA POR EL ING. ALAN OMAR ESPINO GUERRA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA INDUSTRIAL

GUATEMALA, ENERO DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADORA	Inga. Alba Maritza Guerrero Spinola De López
EXAMINADOR	Ing. Cesar Ernesto Urquizú Rodas
EXAMINADOR	Ing. Carlos Humberto Pérez Rodríguez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Industrial con fecha noviembre de 2020.

Mónica Sofía Cruz Carrillo

Guatemala, julio 2021

Ing. César Ernesto Urquizú Rodas
Director de Escuela de Ingeniería Mecánica Industrial
Facultad de Ingeniería.
U.S.A.C.
Presente.

Estimado Ingeniero César Ernesto Urquizú Rodas

Por este medio, hago constar que yo, el Ingeniero Industrial Alan Omar Espino Guerra, con colegiado número once mil trescientos setenta y seis (11376), doy como visto bueno el desarrollo del trabajo de investigación final de graduación del alumno Mónica Sofía Cruz Carrillo, identificado con CUI (2123 78031 0101), alumno a quien he podido apoyar como asesor de su protocolo de tesis.

Dando por concluido el desarrollo de la misma investigación y planteando las soluciones inmediatas y efectivas para el beneficio de la empresa donde se desarrolló la misma.

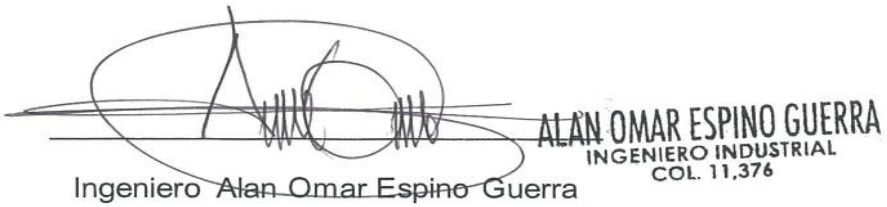
Doy por concluido de forma eficiente ante mi persona el desarrollo de su trabajo de investigación, como tema: **"SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS".**

Línea de investigación: administración de operaciones.

Área: estrategia de operaciones en un entorno global.

Aprovecho la oportunidad para expresarle mi consideración.

Atentamente.



Ingeniero Alan Omar Espino Guerra

Colegiado número 11376.

ESCUELA DE
INGENIERÍA MECÁNICA INDUSTRIAL
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF.REV.EMI.122.021

Como Catedrático Revisor del Trabajo de Graduación titulado **SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS,** presentado por la estudiante universitaria **Mónica Sofía Cruz Carrillo,** apruebo el presente trabajo y recomiendo la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

Renaldo Girón Alvarado
Ingeniero Industrial
Colegiado No. 5977

Ing. Renaldo Girón Alvarado
Catedrático Revisor de Trabajos de Graduación
Escuela de Ingeniería Mecánica Industrial

Guatemala, noviembre de 2021.

/mgp

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

LNG.DIRECTOR.016.EMI.2022

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS**, presentado por: **Mónica Sofía Cruz Carrillo**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

"ID Y ENSEÑAD A TODOS"

Ing. César Ernesto Urquizú Rodas
Director
Escuela de Ingeniería Mecánica Industrial

Guatemala, enero de 2022

Facultad de Ingeniería

Decanato
24189101-
24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.053.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al Trabajo de Graduación titulado: **SISTEMA DE GESTIÓN ADMINISTRATIVA PARA EL ASEGURAMIENTO DE LOS PROCESOS Y CONTROLES EN EL MANEJO DE LA INFORMACIÓN DE UN INGENIO AZUCARERO Y SUS DERIVADOS,** presentado por: **Mónica Sofía Cruz Carrillo,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada

Decana

Guatemala, enero de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por darme la vida y sabiduría para poder alcanzar esta meta.
Mis padres	Elva Carrillo y Alfredo Cruz, por su amor incondicional que será siempre una inspiración. Por todo el apoyo que me han brindado y su orientación.
Mis hermanos	David Cruz, Ingrid y Marisol Arroyo quienes han sido mi más grande apoyo y mi ejemplo.
A mi sobrino	Elio Núñez, por su ánimo y ser un apoyo.
Mis tíos	Ana de Arana y Tulio Arana, por ser un apoyo en mi carrera.
Pamela Morales	Que siempre ha sido un apoyo incondicional y cariño sincero.
Mi novio	Kevin Monzón, por ser un apoyo, por sus ánimos y su amor.
Mis amigos	Por ser una parte muy importante en mi vida.

AGRADECIMIENTOS A:

La Universidad de San Carlos de Guatemala	Mi segundo hogar y gran fuente de inspiración.
Facultad de Ingeniería	Por los conocimientos adquiridos.
A mi asesor	Por su asesoría, tiempo, dedicación y apoyo durante la realización de las prácticas.
Mis catedráticos	Por ser importante influencia en mi vida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Cm	Centímetro
GPa	Gigapascales
°C	Grados centígrados
kg	Kilogramo
kV	Kilovoltio
kW	Kilowatt
MPa	Megapascales
m^3	Metro cúbico
m^3/h	Metro cúbico por hora
m/s	Metro sobre segundo
mm	Milímetro
Nm	Newton-metro
O_2	Oxígeno
ft/s	Pies sobre segundo
%	Porcentaje
psi	*Pound force per square inch*
In (pulg)	Pulgadas
rpm	Revoluciones por minuto
Fe	Símbolo del elemento químico hierro
ton	Tonelada

GLOSARIO

Agua residual — **L**as aguas que han recibido uso y cuyas calidades han sido modificadas.

Biodegradable — Es el producto o sustancia que puede descomponerse en sus elementos químicos que los conforman, debido a la acción de agentes biológicos, como plantas, animales, microorganismos y hongos, bajo condiciones ambientales naturales.

Bunker — Combustible que normalmente proviene de la primera etapa del proceso de refinación (destilación atmosférica), viscoso y con alto contenido energético, lo cual lo hace apto para ser usado en calderas, hornos y en las plantas de generación eléctrica.

Calentamiento global — Se refiere al aumento gradual de las temperaturas de la atmósfera y océanos de la Tierra que se ha detectado en la actualidad, además de su continuo aumento que se proyecta a futuro.

Confiabilidad — Probabilidad de que una parte de la maquina o equipo esté funcionando adecuadamente en un momento preciso y bajo circunstancias definidas.

Contaminación	Pertenencia de cualquier impureza material o energética, en un medio a niveles superiores a los normales.
Demanda	Hace referencia a la cantidad de bienes (productos), o servicios que se solicitan o se desean en un determinado mercado de una economía a un precio específico.
Desgaste	Partículas pequeñas de material producidas por el rozamiento de dos superficies en contacto.
Evaluación	Valoración de conocimientos, actitud y rendimiento de una persona o de un servicio.
Lubricación	Tarea con el fin de controlar el desgaste entre dos superficies.
Merma	Disminución o reducción del volumen o la cantidad de una cosa.
Meta	Objetivo o propósitos a alcanzar.
Monitoreo	Proceso mediante el cual se obtienen, interpretan y evalúan los resultados de una o varias muestras, con una frecuencia de tiempo determinada.

Orden de trabajo	Instructivo en el cual se describe las tareas de mantenimiento a realizar por el departamento de mantenimiento.
Planeación estratégica	Arte y ciencia de formular, implantar y evaluar decisiones interfuncionales que permitan a la organización llevar a cabo sus objetivos.
Sistema CIP	Por sus siglas *Cleaning in Place*, es aquel que permite llevar a cabo la limpieza de tuberías, equipos y accesorios en línea, bombeando en contracorriente agua mezclada con algún tipo de detergente.
Tiempo muerto	Tiempo en el cual se detiene el proceso productivo.
Tolerancia	Diferencia dimensional entre un agujero y un eje.

RESUMEN

El azúcar es uno de los principales productos de exportación de Guatemala, siendo el sector agrario el que mayor cantidad de personas emplea dentro del territorio lo que tiene una representación directa en el Producto Interno Bruto PIB del país, esto pretende estimar la idea de la importancia del sector azucarero para la economía de Guatemala. Dentro del sector azucarero se encuentra la empresa objeto de estudio que tiene la sede central en zona 10 de la ciudad, que emplea a más de dos mil personas en distintas etapas del proceso productivo.

Actualmente, la empresa tiene problemas para el traslado de información que es necesaria en la central para la eficiente gestión administrativa, el retraso o deficiencias en el sistema de información incide de manera directa en las actividades que se desarrollan, es por ello que surge la necesidad de determinar la manera de mejorar dicho proceso a través de la creación de un plan que logre identificar los indicadores adecuados para la medición de los procesos.

Asimismo, se considera necesario analizar la existencia, inexistencia o deficiencias en el monitoreo actual de la información que se traslada para verificar la manera que se lleva a cabo la retroalimentación de dicha información, identificando las necesidades de la gerencia respecto a los factores que inciden en las funciones que realizan, de esta manera detectar oportunidades de mejora y la solución adecuada para la problemática planteada.

Tener una buena administración de la información facilita la coordinación y toma de decisiones, un mejor manejo, brindar un buen servicio tanto de cliente interno con externo y lograr el cumplimiento de las auditorías.

OBJETIVOS

General

Desarrollar un sistema de gestión administrativa para el aseguramiento de los procesos y controles en el manejo de la información.

Específicos

1. Analizar los factores que afectan el manejo adecuado de la gestión administrativa y las posibles fallas o irregularidades, mediante técnicas de recolección de datos.

2. Determinar los riesgos relevantes de los procesos administrativos de la gestión de la información, para su evaluación, análisis y aplicación de la matriz de identificación de riesgos para su control.

3. Analizar los controles y protocolos de los procesos que se utilizan en el departamento de seguridad y continuidad.

4. Establecer los controles y manuales adecuados para el manejo de la comunicación de informes, bloqueo y desbloqueo de accesos y definición de controles mensuales.

5. Asegurar el cumplimiento de las observaciones y recomendaciones de auditorías operativas por medio de evaluaciones periódicas.

INTRODUCCIÓN

La gestión y monitoreo de la infraestructura tecnológica y los controles de seguridad en la actualidad representan un gran desafío para las empresas, esto debido a la complejidad y diversidad de sus activos tecnológicos de información.

El incremento de amenazas creadas y dirigidas por grupos de criminales expertos quienes pretenden explotar cualquier vulnerabilidad pequeña o grande, no importando su magnitud, con el fin de obtener algún beneficio, afectando la disponibilidad de la información o dañando los activos tecnológicos críticos provocando así, impactos irremediables en los objetivos estratégicos trazados por la organización.

Considerando esta aseveración, es necesario e indispensable el monitoreo, prevención y la detección temprana de incidentes o eventos con el fin de poder emprender acciones proactivas para mitigar los diversos riesgos de forma y tiempo oportuno.

El presente trabajo propone una mejora en el sistema de la gestión administrativa de la información para el departamento de seguridad y continuidad, este se centra en elaborar procedimientos y manuales adecuados para el monitoreo los procesos administrativos y evitar los riesgos recurrentes del día a día.

Adicional se apoyará en manuales que puedan apoyar para lograr el cumplimiento de auditorías internas y externas.

1. INFORMACIÓN GENERAL DE LA EMPRESA Y MARCO TEÓRICO

1.1. La empresa agroindustrial

La empresa agroindustrial se dedica al procesamiento de caña para la producción de azúcar, mieles, alcoholes y energía eléctrica. Cuenta con más de 21,200 colaboradores en México, Guatemala, Nicaragua, Brasil y Estados Unidos, contribuye a alcanzar producción anual de 1,17 millones de toneladas de azúcar y productos derivados.

Se posiciona como empresa líder de la región centroamericana en la producción de azúcar, y se concentra entre los diez más importantes de Latinoamérica. Los productos participan en mercados locales e internacionales, con más de 40 destinos de exportación, en donde abastecen a industrias alimenticias y refinerías.

1.2. Reseña histórica

Sus orígenes se remontan al año 1849, marcando un hito histórico Don Manuel María Herrera visionario y emprendedor, así fue como se proyectó a iniciar la ruta explosiva con otro giro comercial, sin medir cuales podrían ser los alcances exitosos al explotar la tierra para beneficios comerciales, además de iniciar con la compra de una finca base de forma paralela adquiere otra extensión de tierra de suma importancia para robustecer su modelo de negocio. A finales de 1870 se realizan diferentes trabajos de remoción de tierras, infraestructura y trabajos de obra gris, construyendo en parte el terreno para el ingenio Pantaleon.

Tabla I. **Memoria histórica del crecimiento del Ingenio Pantaleon**

AÑO	Evento o trascendencia
1877	Manuel María Herrera constituye Herrera & Compañía con sus dos hijos mayores: Francisco Herrera Moreno y Carlos Herrera Luna. En 1880, Pantaleon producía 40,000 arrobas de azúcar.
1883	Se inicia la expansión de la capacidad del ingenio, se incorporan avanzadas técnicas en agricultura que fueron observadas en otros países.
1893	Inicia la construcción de la estación del ferrocarril en el ingenio Pantaleon que conducía al Puerto de San José, para trasladar eficientemente los productos y favorecer su exportación.
1920	Carlos Herrera Dorión continuo eficazmente la visión de su padre con el fomento de la exportación de azúcar a mercados internacionales.
1973	Con la sustitución del gerente general la empresa toma la decisión de cambiar su nombre, siendo este Pantaleon, S.A. para esa época lograron sobrepasar la producción de un millón de quintales de azúcar.
1984	Fusionan la administración y control de operaciones del ingenio Concepción en Guatemala.
1990	Se inicia la cogeneración de energía eléctrica utilizando el bagazo de caña, aportando de esa manera la generación de energía sostenible en Guatemala.
1992	Para fortalecer el desarrollo social, se logra crear la fundación Pantaleon con esfuerzo de miembros de la familia.
1998	Se fortalece la expansión hacia Nicaragua, adquiriendo el ingenio Monte Rosa, para poder llegar a ser el segundo productor más importante de su país.
2004	Explotando el recurso de la caña, construyen una destilería en Pantaleon para procesar y producir etanol con otros productos relacionados a la melaza.
2006	Concretan la alianza con grupo UNIALCO localizado en Brasil y Manuelita en Colombia, por medio de esa alianza concretan la adquisición del ingenio Vale Do Paraná en Brasil, estableciendo así nuevas oportunidades en expansión territorial.

Continuación de la tabla I.

2008	Arrancan sus operaciones administrativas en un ingenio hondureño.
2010	Casi desde su fundación como corporación Pantaleon, construyen he implementan modelos sociales de apoyos académicos hacia su recurso humano y familiares, se construyeron dos centros educativos en Guatemala y dos en Nicaragua, para el 2010 lograron construir un nuevo centro educativo en Siquinalá, Guatemala.
2011	Adquieren como parte de sus acciones extranjeras el ingenio Pánuco en Veracruz, México. Incrementan la participación en la sociedad de Vale do Paraná, aumentando la capacidad de destilería de Bio Etanol en Guatemala.
2012	La combinación de su trabajo grupal alcanzan la producción de 1 millón de toneladas de azúcar.
2018	Inicia operaciones y producción de azúcar en Brasil.
2019	Por decisión estratégica y de expansión decidieron vender las acciones del ingenio al cual obtenían participación en Honduras. Se logra establecer en Estados Unidos como Pantaleon Commodities Corp.
2020	Logran obtener la administración del ingenio El Mante en Tamaulipas, México.

Fuente: Ingenio Pantaleon. *Nuestra historia*: https://www.pantaleon.com/#nuestra-historia. Consulta: 10 de enero de 2021.

De esa forma fue el crecimiento y expansión macroeconómica del ingenio Pantaleon, no solamente se observan beneficios propios hacia la institución, empleando plataformas sociales se propusieron beneficios a su recurso humano y familiares cercanos de los mismo, no solamente era aventajar a la institución en producción, también fue beneficiar gradualmente disponiendo de escuelas semi privadas, clínicas médicas y otros tipos de beneficios sociales.

1.2.1. Ubicación

Las oficinas administrativas se localizan en Diagonal 6, 10-31 zona 10 de la ciudad capital, Guatemala.

Figura 1. **Oficinas administrativas**

Fuente: Ingenio Pantaleon. *Ubicación.* https://www.google.com/maps/place/Pantale%C3%B3n/@14,6016917,-90,5093126,18z/data=!4m5!3m4!1s0x8589a3c856983847:0x40ceac2cbf38ce93!8m2!3d14,6024436!4d-90,5090599?hl=es. Consulta: 10 de enero de 2021.

Las oficinas administrativas se encuentran distribuidas en más de 5 niveles de un edificio localizado sobre la diagonal 6, la mayoría de actividades que se ejecutan allí es de logística, comercialización, administración, operaciones globalizadas con alcances fuera del país, y la mayoría de su personal es altamente calificado y especializado en sus actividades.

1.2.2. Misión

“Promover el desarrollo transformando los recursos naturales en azúcar y sus derivados, de manera responsable y eficiente, buscando la rentabilidad de los accionistas”[1].

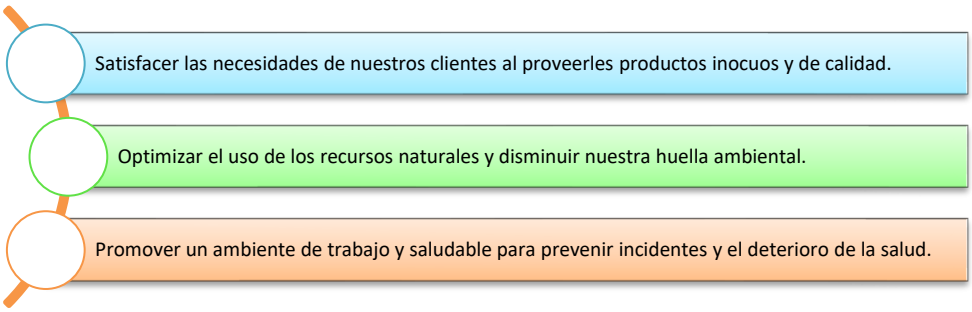
1.2.3. Visión

“En el 2015 seremos una de las cinco organizaciones más grandes de Latinoamérica del mismo mercado”[2].

1.2.4. Política de calidad

Su compromiso hacia la sociedad radica con diferentes valores y aspectos trascendentales.

Figura 2. **Política de calidad**



Fuente: Ingenio Pantaleon. *Políticas*: https://www.pantaleon.com/desarrollo-responsable/un-equipo-responsable/politica-integral-de-gestion/#:~:text=Satisfacer%20las%20necesidades%20de%20nuestros,el%20deterioro%20de%20la%20salud. Consulta: 10 de enero de 2021.

[1] Ingenio Pantaleon. *Antecedentes históricos*. p. 8.
[2] Ibíd.

1.2.5. Estructura de la empresa

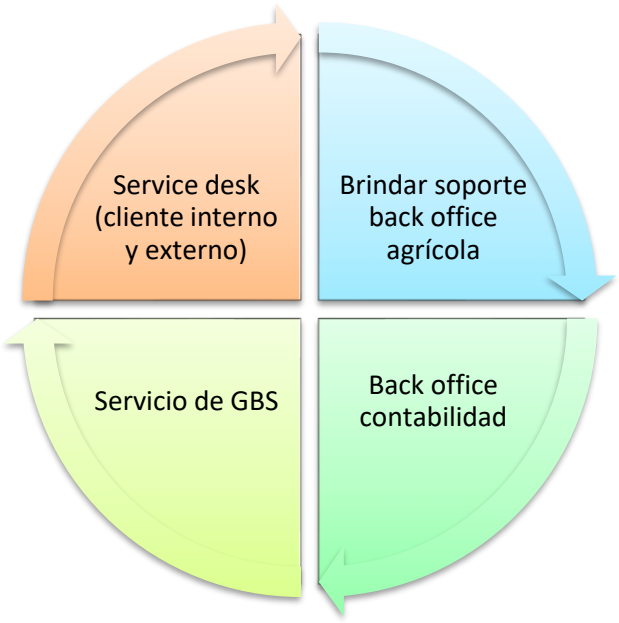
Se organizan con jerarquía vertical, trasladando las diferentes tareas, acciones y operaciones con formato descendente, hasta llegar a los trabajadores de nivel inferior.

Con ese tipo de organigrama con el que trabaja el ingenio, logran distribuir las cargas labores y administrativas eficientemente hasta el momento, las líneas de comunicación y de mando se respetan por el cargo asignado, no obstante si alguna persona encuentra dificultades para lograr realizar las tareas asignadas puede apoyarse en su superior inmediato o superior similar al que tiene asignado, de esa forma se vela por propiciar con el adecuado ambiente laboral reduciendo a su mínima expresión cualquier fuente o causa de error que pueda repercutir en los trabajos asignados o resultados esperados.

1.2.6. Servicios administrativos

Las acciones distribuidas por cargos y tipo de trabajo diseñado en sus ejecuciones diarias se fundamentan en los siguientes servicios, estos logran ser realizados por tareas compartidas a nivel administrativas con responsabilidad compartida y trabajo en equipo.

Figura 3. **Servicios administrativos**



Fuente: Departamento de producción. Ingenio Pantaleon.

1.3. Organización

La organización se distribuye por programación de tareas globales, las tareas globales regionales o extranjeras se construyen en los altos mandos, ellos diseñan las estrategias a implementar anualmente, y continuamente miden los alcances obtenidos en la última temporada de zafra, evalúan los índices económicos de exportación a los mercados abiertos para participar con cierta cantidad de producción de azúcar, evalúan cual fue el desempeño energético obtenido en los últimos periodos para implementar acciones que mejoren el desempeño en consumo de insumos, mano de obra y mostrar mejora económica hacia el consorcio al cual pertenecen, los trabajadores de rangos bajos quienes trabajan en los campos de cosecha y corte de caña desempeñan grandemente el alcance de las metas anuales.

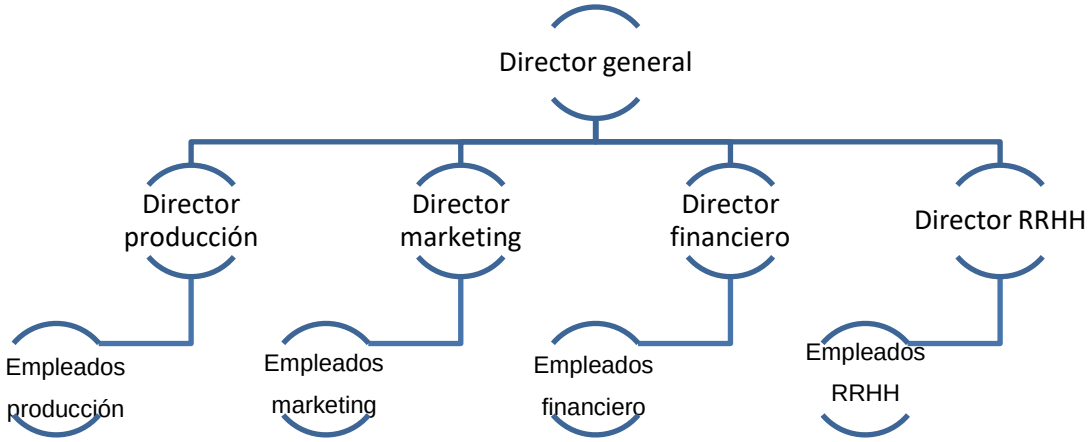
1.3.1. Estructura organizativa

Las actividades operativas y administrativas son trasladadas desde la parte superior jerárquica, trasladándose en los mandos medios y llegando hasta los trabajadores del último nivel, preservando la intención de perfección en la ejecución de las tareas asignadas ya sea por rango administrativo o por atributos del puesto que se desempeña.

1.3.2. Organigrama

La empresa desarrollo el diseño eficiente para trasladar sus tareas hacia los mando medios he inferiores de forma eficiente.

Figura 4. **Organigrama de la empresa**



Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

Con este tipo de organigrama se dividen y trasladan las acciones que conllevan a la producción del azúcar en el ingenio, se emiten comunicados internos sobre cualquier nueva disposición o tareas emergentes que logran suscitarse por cualquier tipo de evento externo a la organización.

1.3.3. Departamento seguridad y continuidad

Su enfoque intermitente es velar por que los trabajadores sin importar el rango administrativo que posean en la empresa desarrollen sus tareas o trabajos asignados bajo altos estándares de seguridad, se prevé cualquier tipo de riesgo hacia la salud física, evitando las fuentes de peligro que puedan propiciar algún accidente de leve, moderado a fatal.

Para lo cual se asignan supervisores de campo, los supervisores incorporan bitácoras donde anotan cualquier observación que para ellos pueda parecer imprudencia o negligencia, luego este tipo de acciones es reportado al departamento de recursos humanos donde se inicia la investigación previa para citar al trabajador y notificarle por que se le está citando y cual pude ser el apercibimiento hacia la mala conducta observada.

No obstante, estas cuadrillas se supervisores tienen asignadas tareas de supervisar y medir el nivel de estrés en los trabajadores en las oficinas administrativas, evalúan la disposición ergonómica de los lugares físicos asignados, para saber cuál es el tiempo permisible antes de padecer de cansancio crónico o dolencias físicas por mal posicionamiento en tiempos prolongados de trabajo.

La tarea dura y difícil es garantizar que la salud de los jornaleros pueda ser respetada, estos jornaleros trabajan bajo condiciones inhumanas en los campos

de corte de caña, bajo temperaturas superiores a los 40 grados de calor, se exponen a residuos de caña quemada propiciando así enfermedades respiratorios a largo plazo, sus manos sufren inmediatamente abrasión por cortes de restos de hojas y partes punzocortantes de los troncos de la caña, pueden ser picados por serpientes y sufrir insolación.

1.3.4. Descripción de puestos

Las actividades relacionadas a cada puesto fueron brevemente explicadas en las oficinas administrativas por los niveles de confidencialidad de la empresa.

Tabla II. **Descripción de puestos**

Puesto	Descripción breve
Director general	Su función se centra en proveer el liderazgo hacia el ingenio, velará por exigir sobre el cumplimiento de metas trazadas previamente para superar los niveles de producción estimados, su estrategia es fortalecer los canales de comercio de la empresa hacia los mercados internacionales y nacionales compradores de su producto básico azúcar y derivados, generar potencia con el menor uso de bagazo de caña, vender la potencia a mercados intermediarios que promuevan la fidelidad de la marca, por último garantizar que en sus instalaciones y en su empresa se viva un clima laboral adecuado para generar producción eficientemente de forma permanente y constante en vías de expansión y mejora constante.
Director producción	Su rol y función es garantizar la disponibilidad de materias primas que serán procesadas desde el momento que se programa la siembra, al momento de la zafra garantizar que los equipos, máquinas y herramientas se encuentran trabajando en óptimas condiciones, que todo su recurso humano se encontrará disponible desde el día cero cuando inicia la temporada de quema en las fincas y recolección por medio de corte con jornaleros externos contratados a destajo. Con esas funciones se hace brecha para garantizar que llegará a la meta estimada en el procesamiento de azúcar apta para poder ser comercializada en el país y hacia el extranjero.

Continuación de la tabla II.

Director marketing	Velara por alcanzar sus clientes metas, satisfaciendo las necesidades de sus actuales clientes sosteniendo los índices de calidad en la producción de azúcar, para el mercado interno y los mercados extranjeros, diseñar campañas donde se pueda percibir que el ingenio destaca entre sus competidores, concientizar a nuevos consumidores a comprar este producto evitando productos sustitutos, aventajando con el cierto grado de beneficio económico de adquisición a comparación de la competencia.
Director financiero	Su función principal es garantizar que la inversión que se realiza diariamente produzca la rentabilidad esperada, no solamente verificar que no se trabaje en operaciones con índices marginales de perdidas, si no que se sostengan los niveles de comercios establecidos por años atrás, además de incorporar la marca en nuevos mercados o sectores donde no se conocía.
Director RRHH	Su rol para la empresa es consolidar el conjunto de estrategias diseñadas por los altos mandos, promoviendo el clima organizacional adecuado para lograr construir los objetivos trazados por cada dependencia, sus atributos inician desde el diseño inteligente de cada puesto asociado a ciertas tareas específicas donde se espera transformar la energía física de la persona en recursos monetarios para la empresa, diseñando módulos y filtros de selección que orienten a obtener al personal idóneo para las tareas esperadas a realizar.
Empleados producción	Deberán realizar el conjunto de tareas asignadas por sus superiores inmediatos, deberán colaborar con tareas de orden y control para garantizar que en su área de trabajo se pueda desarrollar competentemente sin entorpecer las actividades y tránsito de alguno de sus compañeros.
Empleados marketing	Deberán satisfacer la demanda de sus superiores, con tareas de desarrollo en marketing digital o publicitario para impulsar constantemente la imagen corporativa del ingenio y darlo a conocer con nuevos consumidores de la marca.

Continuación de la tabla II.

Empleados financiero	Su trabajo no podría situarse exclusivamente en oficinas administrativas, en ciertos momentos deberán realizar visitas a las instalaciones del ingenio para garantizar que los recursos asignados a cada departamento de producción se encuentren físicamente y que puedan ser útiles y empleadas para las tareas asignadas, deberán realizar todo el trabajo de oficina que cumpla con las tareas de control, supervisión, auditoría y entrega de resultados contables a las máximas autoridades donde determinaran si los números en producción versus los gastos fueron positivos, iguales o negativos.
Empleados RRHH	Los empleados de este departamento deberán trabajar constantemente evaluando el clima organizacional, velarán por los resultados obtenidos para cada empleado en sus niveles de eficiencia, si se presentan quejas laborales, prestarles la debida atención y proporcionar el seguimiento esperado para validar cual es la causa y cuál puede ser el método de solucionarlo, dentro de estas actividades deberán desarrollar programas de capacitación continua que garanticen que los trabajadores no importando el cargo o rango en la empresa puedan desarrollar nuevas fortalezas con su crecimiento personal.

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

1.4. Marco teórico

Se plantea la incorporación del presente marco teórico para fortalecer la investigación, de esa forma poder dar nuevo orden administrativo con alcances estratégicos hacia la propuesta de ciertos aspectos que beneficiarán sustancialmente a la empresa.

1.4.1. Gestión administrativa

La gestión administrativa es el conjunto de formas, acciones y mecanismos que permiten utilizar los recursos humanos, materiales y financieros de una empresa, a fin de alcanzar el objetivo propuesto. Se basa en cuatro principios fundamentales; el orden es el primero, según cada trabajador debe ocupar el puesto para el que está capacitado.

La falta de orden conlleva a un trabajo menos eficiente y al uso incorrecto de los recursos. El segundo principio es la disciplina; dentro de la gestión administrativa la disciplina es un aspecto importante, ya que las normas y reglas deben ser cumplidas y respetadas por todos.

El tercer principio es la unidad de mando. El empleado debe saber a quién reporta su trabajo y de quién recibirá órdenes, para evitar mensajes erróneos que perjudiquen la calidad del trabajo. Por último, fomentar y valorar la iniciativa en el personal es crucial para motivar; esto repercutirá positivamente en el ambiente de trabajo y en el logro de metas. La gestión administrativa es primordial para la organización, ya que conforma las bases sobre las cuales se van a ejecutar las tareas propias del grupo, conformando una red orientada a cumplir los objetivos empresariales.

1.4.1.1. Modelos

Algunos modelos necesarios que podrían ser implementados en la empresa están dirigidos al control de operaciones administrativas que permitan mejorar las acciones y reacciones ante posibles eventos fortuitos que comprometan el seguimiento de las acciones.

Tabla III. **Modelos de gestiones que se pueden incorporar**

Tipo de gestión	Descripción
Por resultados	Es basada en metas y objetivos dentro de la estructura organizacional, estas deberán estar totalmente de acuerdo con el tipo de planificación estratégica propuesta. Con la gestión por resultados involucra a colaboradores y gerencia en la definición junto a la búsqueda de obtener los resultados previamente proyectados. Los resultados esperados deberán ser monitorizados continuamente. Con este tipo de gestión obtener el resultado esperado marca trascendencia a comparación del método empleado. El conjunto de objetivos que han sido diseñados son el foco de la gestión por resultados, se podrán definir para cada uno de los diferentes niveles organizacionales. Otro diferenciador o característica sobre saliente de este modelo de gestión se refiere a la verificación continua he intermitente. Se deberá validar periódicamente el desempeño del inventario completo de los equipos, asignando revisiones para comparar los resultados obtenidos versus los planificados, de esa forma diseñar mejoras necesarias. Cada perfil involucrado en los procesos tiene conciencia de su participación. Eso crea el clima laboral apto donde se podrían evitar que pierdan el enfoque hacia los objetivos establecidos, mejorando el compromiso organizacional y motivar a su personal.
Democrática	Para este tipo de gestión se considera necesaria la participación de los empleados que participan en los procesos a mejorar, aportando sus ideas para la toma de decisiones y participando activamente hacia la definición del conjunto de estrategias innovadoras. Así es como la gestión democrática reconoce el capital humano de la empresa, promoviendo la construcción de una relación cercana entre la empresa y sus trabajadores. Se emplea este modelo de gestión fuertemente en cooperativas o en industrias con alto nivel de desarrollo de su talento humano. Una variable a considerar dentro de este modelo de gestión, es por parte de la empresa asegurar el nivel de capacidad intelectual y capacidades técnicas de los empleados que podrían participar en el proceso de toma de decisiones.

Continuación de la tabla III.

	En la gestión democrática, los empleados se enfrentan a un determinado problema y, en función de la misión, la visión y los valores de la organización, necesitan encontrar una solución creativa. La comunicación y la transparencia son aspectos indispensables en este modelo de gestión, que tiende a motivar más a los empleados y resalta el sentimiento de pertenencia a la organización.
Basada en procesos	Este tipo de gestión es centrada hacia la mejora constante de cada uno de los procesos organizacionales. Así es como la futura empresa podría adoptarlo en busca del monitoreo y evaluar el desempeño de los procesos para estandarizarlos, sin olvidar el poder identificar e implementar las mejores prácticas. Con este tipo de gestión se busca mejorar le relación en cada uno de los diferentes sectores de la empresa, proyectar la sistematización en los flujos de trabajo para reducir costos. Esto se podría realizar con mapeo he información constante sobre los procesos, su intencionalidad es lograr la fluidez, transparencia, eficiencia y alineación adecuada hacia los objetivos de la organización.
Centralizada	Con este modelo se fortalece el rol de líder, se empodera la toma de decisiones de una sola persona, así de limitada es la responsabilidad. Para esta gestión centralizada el centro de toda la organización y la empresa es el Gerente. Su responsabilidad estará en definir los objetivos, delegar el conjunto de tareas y responsabilidades, controlar los rendimientos, proporcionar pautas y tomar decisiones críticas. Deberá destacar en sus habilidades de liderazgo y preparación el conocimiento académico, experiencia organizacional, por eso se hace recomendable este tipo de gestión, los trabajadores de rangos inferiores no poseen habilidades y conocimientos gerenciales, su crecimiento ha sido empírico esto los hace poco calificados. Este tipo de modelo estaba constituido de forma sólida en empresas con larga trayectoria, las nuevas corporaciones o empresas trabajan con otro enfoque empresarial y vanguardista.

Fuente: elaboración propia.

1.4.1.2. Análisis

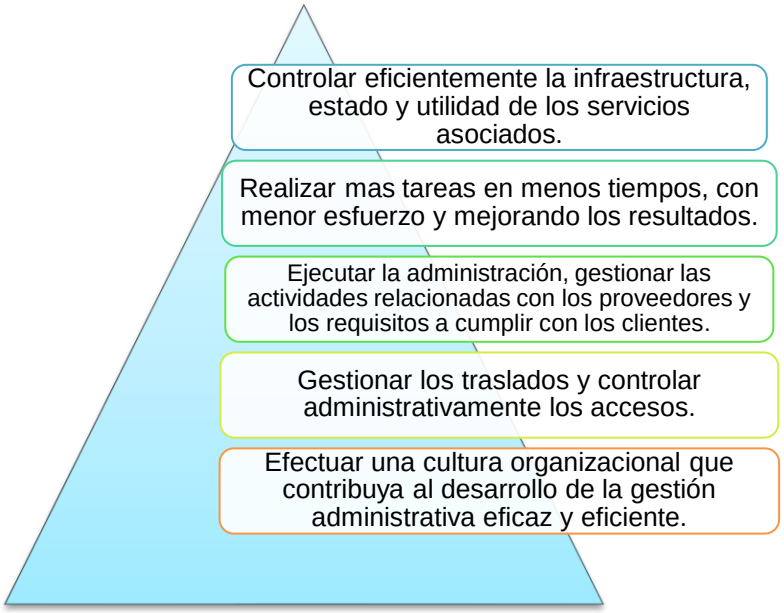
El Análisis de la Gestión Administrativa tiene como finalidad hacer una evaluación integral y conocer el estado en que se encuentra la empresa. Entre los nombres que ha recibido el análisis de gestión administrativa están: Auditoría Gerencial, Auditoría de la Empresa, Análisis Administrativo, Análisis de Operaciones, Investigación de la Empresa, Auditoría de Cumplimiento y Auditoría de Rendimiento.

A través de esta herramienta es posible evitar cualquier desperdicio de tiempo y evaluar los grados de eficiencia y efectividad de los sistemas de control interno, propios de la organización. También es posible afirmar, que el Análisis de Gestión Administrativa pone en evidencia aquellas áreas problemáticas y las debilidades que existen dentro de la empresa.

1.4.1.3. Objetivos

Diferentes objetivos podrían ser empleados para la gestión optima de dirección de recursos humanos y monetarios, se presentan los destacados que permitirán mejorar las operaciones en la empresa de interés.

Figura 5. **Objetivos en la gestión administrativa**



Fuente: elaboración propia.

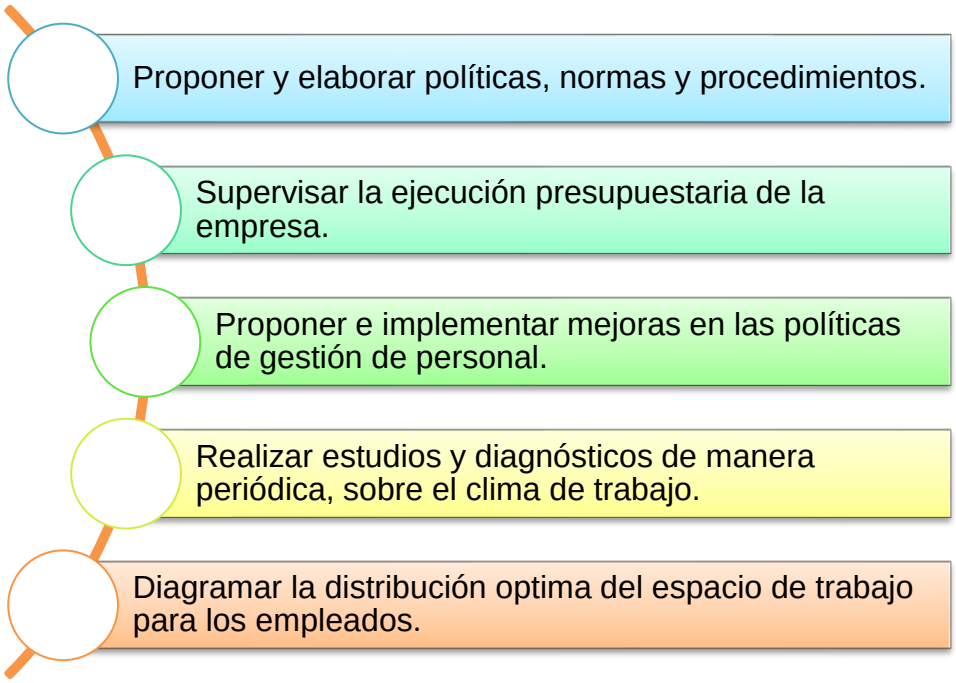
1.4.1.4. Importancia

Para esta gestión que incorpora aspectos administrativos y comerciales consistiría en preparar a la organización y disponerla para actuar, pero de manera anticipada, contemplando todos los medios y procedimientos que necesita para cumplir con sus objetivos y disminuir los efectos negativos o posibles problemas.

1.4.1.5. Características

Algunas características necesarias que podrán optimizar la gestión administrativa incorporando parámetros cualificables y cuantificables.

Figura 6. **Características de la gestión administrativa**

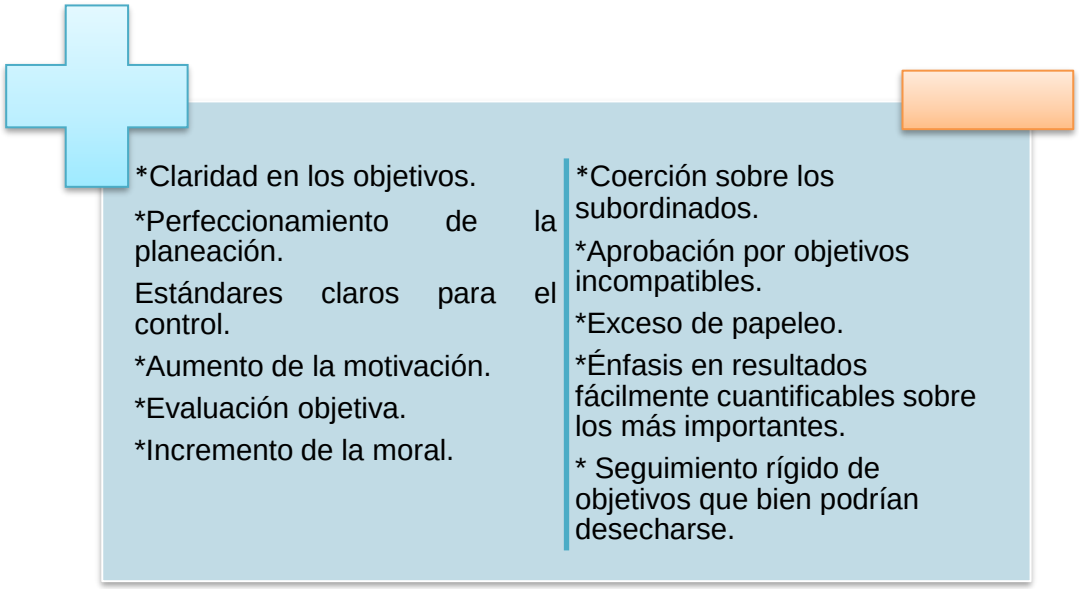


Fuente: elaboración propia.

1.4.1.6. Ventajas y desventajas

Se deberá coincidir en algún punto intermedio, no es garantizado que implementar mejoras a un sistema de gestión ya existente otorgue solo beneficios y ni un solo problema inesperado, parte de este efecto es concientizar al recurso humano y luchar con la negación hacia el cambio de los modelos administrativos ya conocidos.

Figura 7. **Ventajas y desventajas**



Fuente: elaboración propia.

Las ventas y desventajas mostradas son las síntesis de diferentes autores, según las fuentes consultadas podrían emplearse un sinfín de aspectos que ofrecerían éxito rotundo o fracaso total, por lo cual se deben medir con exactitud todas las acciones previamente a ser incorporadas y ejecutadas en la gestión de operaciones de una empresa de gran valor comercial.

1.4.2. Sistemas de información

Para intereses del presente estudio se hace alusivo a un conjunto de datos oscilantes, intercambiables y que interactúan continuamente entre con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

La importancia de un sistema de información radica en la eficiencia en la correlación de una gran cantidad de datos ingresados a través de procesos diseñados para cada área con el objetivo de producir información válida para la posterior toma de decisiones.

1.4.2.1. Transferencias

Con el sesgo hacia la informática digital interna de la empresa se puede presentar el termino de transferencia, aplicado específicamente a la transferencia de datos. Se representa por el traspaso de información mixta o combinada en un determinado tipo de dispositivo o aparato hacia otro similar o de distinto tipo. Con el avance tecnológico y la demanda constante en implementar tareas que empleen el menor tiempo posible hace esta acción aún más simple pero compleja.

Cuando se habla de transferencia se hace referencia a la tarea que permite realizar una computadora con aparato electrónico. Esta transferencia es siempre de datos y estos pueden estar representados en diferentes estilos ya sea en material multimedia, textos, o software entre otros. De esa forma se puede acceder a diversos archivos y material desde diferentes lugares siempre que se disponga de los dispositivos apropiados y los métodos básicos.

Normalmente, el proceso de transferencia se puede dar de dos maneras básicas: a través de un sistema en red o a través de un puerto, siendo el más común el conocido puerto USB. Dependiendo de la calidad de los aparatos o del método elegido, la velocidad de la transferencia podrá variar. Por otro lado, los dispositivos involucrados en el proceso deben contar con un mismo lenguaje de protocolo que los haga compatibles. En este sentido poseer computadoras en red permite acceder desde un aparato a información que está guardada en otro

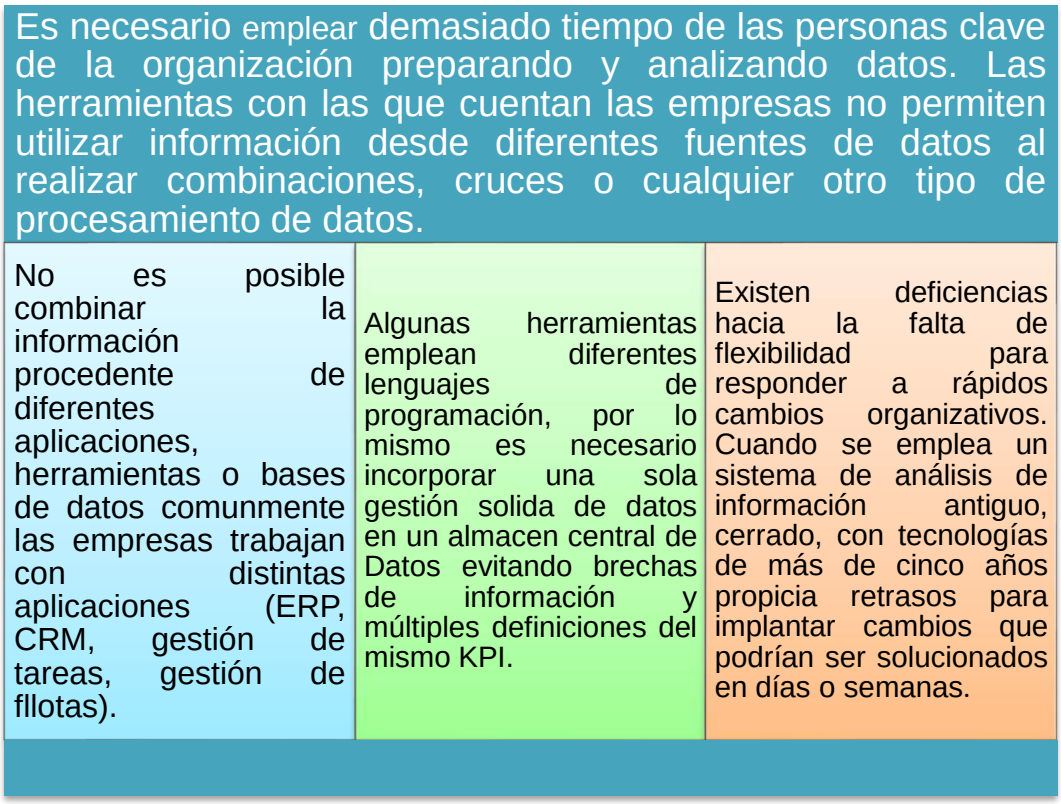
aparato. En el caso de los puertos USB, estos son normalmente utilizados con dispositivos externos como celulares, pen drives, impresoras, otras computadoras y dispositivos de memoria.

La transferencia también puede darse con o sin la necesidad de cables. Si uno necesita cables para llevar a cabo este proceso, estos deberán ser cables trenzados, fibra óptica o cables coaxiales. Las transferencias inalámbricas son básicamente satelitales o con sistemas infrarrojos.

1.4.2.2. Deficiencias

La ciencia de la informática es una materia compleja, no es de fácil entendimiento en sus orígenes o programación, por lo cual dependerá siempre de los atributos del diseñador o sobre los términos específicos para los que fue diseñado algún programa digital o plataforma. Por este tipo de eventos presenta diferentes deficiencias, otros aspectos que limitan hoy los procesos administrativos intra oficinas o a distancia es la dependencia 24/7 del recurso de internet. Se volvió la herramienta versátil practica y efectiva, pero también llego a limitar las operaciones, con la sistematización, intercambio de datos, planimetrías, medición de resultados en vivo o simplemente para entablar una charla vía texto o llamada se necesita la red digital del internet, sin acceso a esta herramienta tecnológica se detienen por completo las operaciones.

Figura 8. **Algunas deficiencias en los sistemas de información**



Fuente: elaboración propia.

Estas deficiencias son consideradas repetitivas, significativas y de relevancia ante cualquier cambio que se desea realizar en la industria privada, un factor que no se incluyo es el económico, determinante por la capacidad de adquisición en máquinas o equipos tecnológicos, licencias de programas o uso de programas gratuitos, con la sumatoria de estos demás factores se podría dar forma al panorama complejo que incorpora todo lo relacionado hacia los sistemas de información. Las empresas que no disponen del departamento de informática deberán tercerizar estos servicios considerando que los prestadores de servicios realizan su trabajo de forma eficiente, confiable y seguro, resguardando la integridad digital de la empresa en todo momento y a futuro.

1.4.2.3. Compatibilidad de sistemas

Emplear diferentes programas o softwares digitales compromete la ejecución, acciones y manejo de las operaciones en cualquier empresa, fácilmente un usuario puede comprometer su información al emplear dos dispositivos digitales que no sean compatibles en el tráfico de la información, haciendo esto a nivel exponencial en una empresa que dispone de más de 100 empleados, cada uno con un computador de escritorio asignado y por cada computador posiblemente 2 o 3 equipos digitales dentro de la misma oficina crea un nudo tecnológico que al mínimo error de conexión y comunicación podría dejar de funcionar.

Los técnicos y expertos en informática recomiendan que la base segura hacia la compatibilidad de los sistemas es emplear equipos dotados con sistemas operativos y capacidades comunes, no se aconseja comprar equipos con desarrollador tecnológico A que necesiten intercambiar información con equipos con desarrollador tecnológico B. Dentro de la simpleza es necesario comprar los equipos a un solo proveedor que garantice y respalde la instalación, uso, manejo y sostenimiento continuo de las operaciones. Se puede agregar a esto circuitos de programas integrados del mismo proveedor.

Maximizar la compatibilidad de los equipos, dispositivos digitales, máquinas de escritorio garantizaría que la empresa no incurra en inversiones continuas he innecesarias. Sostenerse en una línea de tiempo apegado a una marca X en los equipos de cómputo permitirá que los usuarios encuentren modelos amigables y con menor tiempo de asociación hacia las actualizaciones del ciertos programas que emplean para reducir los tiempos de capacitación, reduciendo estos tiempos claramente necesarios afectarían en cascada permitiendo mejorar los tiempos de reincorporación a las actividades cotidianas, menos tiempo de paros por

adiestramiento de personal, menos tiempo de retención en producción y menos costos asociados a la producción y planes de capacitación.

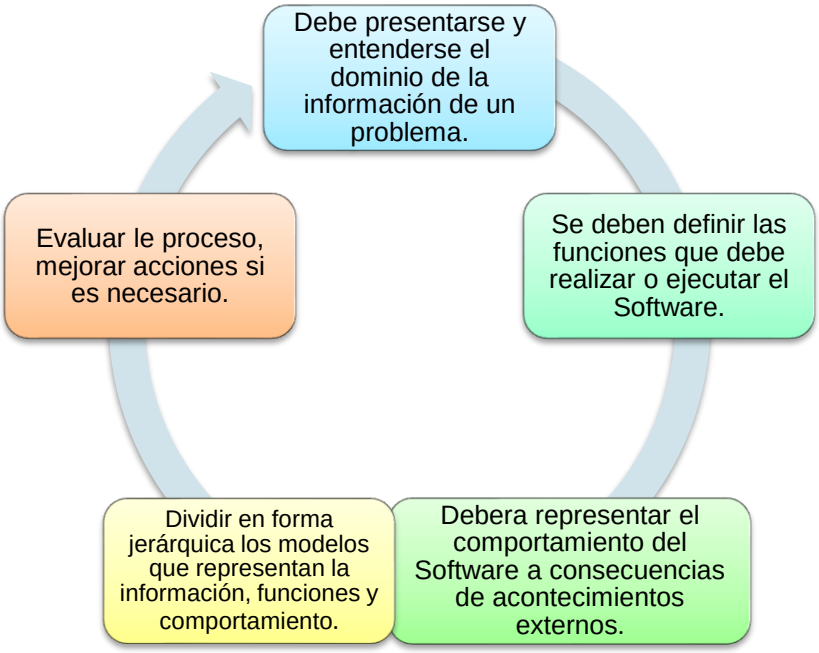
Los programas compatibles son útiles incluso cuando los sistemas no están integrados. El uso de programas compatibles asegura que diversos tipos de archivos como los documentos, las hojas de cálculo, los archivos y los correos electrónicos puedan ser compartidos por el personal en distintos lugares sin ninguna preocupación sobre su conversión o incapacidad para leer otros archivos. También se podría obtener incremento en la eficiencia con la compra de sistemas que otorguen compatibilidad entre dependencias e instituciones.

1.4.2.4. Análisis de la información

Para el reconocimiento del análisis informático se pueden emplear un sin de acciones por diferentes medios, que en síntesis es optar por el conjunto de procedimientos o programas relacionados de manera que juntos pueden llegar a conformar una sola unidad. Lo relacionado a la informática es materia confusa con miles de vertientes y aplicaciones. Dependerá del usuario o la empresa de lo que desea desempeñar o realizar, si es analizar información deberá establecer parámetros, si es sobre producción, ritmos de producción, eficiencias de los equipos, eficiencias de los operarios, control de temperaturas, medición de desperdicios entre algunos de tantos factores que pueden ser medidos.

La programación se basará en un ambiente multidisciplinario, donde cada uno de los interesados de la empresa proporcionaran los datos a ser analizados, los eventos realizados y las tareas asignados bajo ciertos niveles esperados en resultados finales, esto traducido a la producción total.

Figura 9. **Principios básicos para el análisis de la información**



Fuente: elaboración propia.

Los principios establecidos en la figura 9 fueron recolectados de diferentes autores, haciendo uso del lenguaje técnico que los desarrolladores tecnológicos emplean se fue modelando este círculo infinito de acciones, se denomina infinito por ser empleado constantemente y sin temporalidad, podría ser empleado hoy y mejorado mañana, pero al ser utilizado mañana podría proporcionar infinidad de datos mejorados y aun así podría ser mejorado desde el dominio la información que analizara determinado problema.

Cada proceso de análisis de información deberá iniciar con información esencial relacionada a la acción a evaluar, incorporando aspectos relevantes que permitan reducir los sesgos en el análisis culminando en los detalles de la implementación.

1.4.3. Accesibilidad a usuarios

Para los usuarios de las plataformas que se emplean en cada empresa deberán trabajarse bajo los principios de usabilidad e ingeniería de la usabilidad. La evaluación de la usabilidad, es la medida de la facilidad de uso de un producto o pieza de software. Por su parte, la ingeniería de la usabilidad es el proceso de investigación y diseño que asegura que un producto tenga una buena usabilidad.

Para cada usuario la empresa deberá crear un registro único con respaldo de bitácora de ingresos, acciones internas realizadas, traslados entre oficinas con registros magnéticos o algún método similar, limitar al usuario conforme las tareas y cargos asociados a su representación interna dependerá de los accesos o participaciones que puedan llegar a tener en la plataforma interna.

1.4.4. Gestión de permisos

Para la creación de perfiles de usuarios de equipo como invitados; estos pueden ser asociados a un grupo donde es posible administrarlos. Estas buenas prácticas resultan de utilidad en empresas. Actualmente se puede ver que a diario surgen nuevas amenazas que afectan a los sistemas operativos.

Un aspecto importante en el Sistema Operativo es el de los permisos en los perfiles. Como en Linux está el súper usuario *root,* deberá existir la posibilidad de contar con distintas sesiones de menor cantidad de privilegios; en Windows estas se pueden crear y establecer permisos para lo que cada uno necesita usar. Esto permite dejar el usuario Administrador solo para fines de administración del equipo como instalación de aplicaciones o actualizaciones, entre otros.

Para crear un nuevo perfil, se debe ingresar al Panel de Control y allí en el ícono “Cuentas de usuarios”. Una vez dentro se debe acceder a Administrar

cuentas y desde ahí se podrá crear una. Luego de crear las respectivas para cada usuario se podría iniciar a definir el tipo de permiso en diferentes directorios para autorizar o denegar acceso a escritura o solamente lectura de tareas asignadas.

Tabla IV. **Tipos de permisos principales en una empresa u organización**

Tipo de permiso	Descripción
Permiso directo	Se asignan directamente a un grupo de personas o de forma individual a cada usuario. Cuando se han otorgado los permisos necesarios pueden realizar diferentes tareas administrativas y si disponen de niveles adicionales de privilegios podrán incorporar asignación de tareas especiales para otros usuarios. Cada permiso directo puede ser editado con órdenes superiores y controles de mando por medición de resultados.
Permiso heredado	En el amplio espectro de la informática, se reconocen usuarios con permisos sobre algún dominio o carpeta, se ejecuta orden de heredar el permiso especial para todos los equipos del dominio o la estructura organizacional especifica. Cuando el grupo de usuarios tiene acceso a permisos sobre algún equipo del dominio compartido, todos los subgrupos y usuarios que forman parte integra a ese grupo heredan el permiso sobre el objeto del dominio. Cuando los grupos tienen permisos sobre un objeto del dominio, todos los subgrupos y usuarios que pertenecen al grupo heredan el permiso sobre el objeto del dominio. Es posible denegar permisos heredados a algunos tipos de objetos. Al denegarse permisos, se configuran excepciones para los permisos que los usuarios y grupos puede que ya tengan.

Continuación de la tabla IV.

Permiso efectivo	Los detalles de los permisos muestran los permisos directos asignados a un usuario o grupo, permisos directos asignados a grupos primarios y permisos heredados de objetos primarios. Además, los detalles de los permisos muestran si un usuario o grupo tiene asignada la función de administrador, la cual pasa por alto la comprobación de permisos.

Fuente: Informática. *Guía de seguridad*. https://docs.informatica.com/es_es/data-integration/metadata-manager/10-0/guia-de-seguridad/permisos/permisos-del-objeto-de-dominio/permisos-por-usuario-o-grupo/visualizacion-de-detalles-de-permiso-para-un-usuario-o-grupo.html. Consulta: 14 de marzo de 2021.

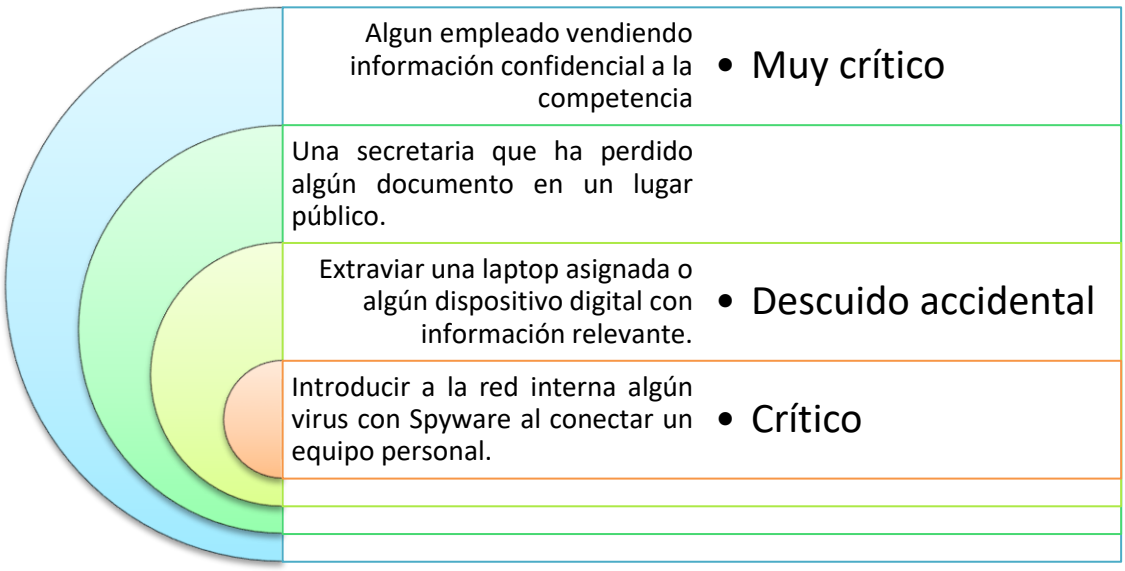
1.4.5. Precedentes de fuga de información

Para la informática y la seguridad en informática industrial, podría ser considerado como algún evento o incidente que se haya presentado a nivel interno o externo en la empresa, se deberá considerar que se ejecutó de forma intencional o por algún tipo de error humano pudo darse fuga a otras fuentes interesadas. En corporaciones destacadas por sus altos índices de éxito es frecuente comprometer los valores éticos de ciertos empleados que podrían comercializar información estratégica que ha marcado el diferenciador o la brecha entre las empresas competidoras y la firma a la cual representan.

La información expuesta puede ser de cualquier índole: un listado de empleados con datos personales, listado de salarios, base de datos de clientes o una fórmula o algoritmo secretos, por citar algunos ejemplos. Es difícil medir el impacto de la fuga de información, pero puede ser muy diverso, especialmente según la intencionalidad del incidente. En aquellos casos en que se trata de un

accidente no intencional, el impacto en la empresa dependerá de qué ocurre con el nuevo poseedor de esa información. Si se supone que un gerente de la empresa pierde una computadora portátil, el impacto puede ser nulo si quién la encuentra ignora la información que allí se contiene y formatea el sistema; o puede ser alto si el nuevo poseedor identifica los datos y los utiliza para publicarlos, comercializarlos o cualquier otra acción dañina.

Figura 10. **Eventos que podrían ser considerados como fuga de información**



Fuente: Informática. *Guía de seguridad*. https://docs.informatica.com/es_es/data-integration/metadata-manager/10-0/guia-de-seguridad/permisos/permisos-del-objeto-de-dominio/permisos-por-usuario-o-grupo/visualizacion-de-detalles-de-permiso-para-un-usuario-o-grupo.html. Consulta: 14 de marzo de 2021.

Este conjunto de eventos son los más conocidos, en la diversidad de acciones abordadas por cada empleado determinara el nivel de criticidad, que podría ser sesgado hacia un descuido o trabajar con intencionalidad, la empresa

deberá emplear protocolos preventivos para anticiparse a estos hechos que podrían comprometer por completo datos relevantes internos.

1.5. Seguridad y continuidad

El ingenio incorpora protocolos mínimos para impactar la seguridad informática en los procesos administrativos, algunos equipos no poseen licencias activas de antivirus, los accesos no son restringidos en ciertas áreas donde posiblemente se podría accesar a la base de datos que comprometan las acciones diarias. Es parte de la necesidad inmediata establecer protocolos adecuados en la continuidad de operaciones distribuidas. La continuidad que se realiza es escasa de algún software de control avanzado, se llevan registros de datos vaciados en hojas de control.

El beneficio con el ingenio es la poca rotación de personal dentro de las oficinas administrativas, al asignar un puesto se asigna un equipo de cómputo, este se encuentra conectado a la red interna de las instalaciones, pero no se encuentran en línea con los servidores de toda la empresa donde se podría intercambiar la información inmediatamente sin esperar ser cargada de forma independiente por cada usuario en distintos horarios.

La seguridad se ha visto comprometida con fuga de información, esta información conlleva datos históricos de cosechas, inversiones económicas realizadas, uso y empleo total de cuadrillas para corte de caña, costos de operación por uso de maquinaria pesada en la siembre de caña, lo relevante o destacado en esta información fugada es el comercializar con fórmulas propias establecidas para germinar eficientemente con el mínimo empleo de recurso en agroquímicos la caña de azúcar.

La red interna podría ser mejorada, reforzada, estableciendo limites hacia los usuarios, estos accesos pueden ser físicos y digitales, otorgando líneas de trabajo específicas para que no hagan uso de programas innecesarios acorde a las tareas asignadas.

1.6. Aseguramiento de procesos

Con la medición de resultados por quejas han logrado establecer los límites de aseguramiento de sus procesos internos y externos. Los programas internos evalúan esporádicamente los alcances sobre los objetivos y proyecciones trazadas, el epicentro del problema que se logra evidenciar es que se evalúa por departamento, no se han incorporado sistematizaciones o modelos de indicadores de eficiencia por separado a cada usuario asignado a una computadora y a tareas específicas.

Este problema radica por emplear software de baja capacidad de análisis, como se describe con anterioridad, emplear programas muy antiguos solamente hacen de su ejecución un proceso engorroso, invirtiendo demasiado tiempo en los analistas de los datos recolectados que por ser evaluación grupal no logran delimitar donde podría erradicar la debilidad puntual.

Los procesos se continúan ejecutando con problemas cotidianos, frisado de computadoras por exigir el rendimiento de su Ram con tareas que requieren rapidez y fluidez en la ejecución de las tareas asignadas, otros aspectos determinantes es la falta de capacidad técnica y operativa de los usuarios, algunos usuarios no logran trabajar amigablemente con la interfaz de ciertos paquetes de programas, especialmente si estos programas o su interfaz se encuentra en el idioma inglés. El obsoletismo se presenta con el interrumpido transido de datos hacia la matriz general de la empresa, se cargan datos a los

servidores en diferentes horarios, cuando se presentan problemas en el fluido eléctrico interrumpe estas acciones retrasándolos hasta por 48 horas.

1.6.1. Controles actuales

El ingenio a empleado he incorporado para el control de sus operaciones protocolos semi automatizados para el ingreso de su recurso humano, previamente a ser asignadas tareas específicas se les otorga su número interno supernumerario, se les crea usuario y código para utilizar las computadoras, cuando son contratados para un departamento específico se les asigna su computadora de escritorio personal conectada a la red interna, estos controles los lleva el departamento de informática. Los datos son procesos cada 28 días calendario, no se obtienen medición de resultados en vivo o a cada momento que pueda presentarse alguna brecha en el robo de información.

1.7. Distribución

Se han distribuido las tareas informáticas por cada puesto organizacional representado, el ingenio innovo al contratar personal previamente calificado que puedan presentar credenciales o certificaciones en materia de informática. Los trabajadores del nivel más bajo en la empresa tienen tareas asignadas para procesamiento de materias primas, manejo de inventarios, control de bodega de insumos, seguimiento de quejas administrativas por personal irresponsable.

Luego de esta línea de trabajadores ocupan supervisores, por cada supervisor están asignado 10 o 15 operarios, velando por el cumplimiento de las tareas asignadas, sin permitir que se interrumpa la continuidad de las acciones solo que sea por eventos naturales o perdidas en el fluido eléctrico.

En la parte superior de esta distribución se localiza el jefe de área, monitorea a los supervisores, se esfuerza por llegar a la meta de producción establecida, reduce los problemas con el traslado de ordenes operacional.

2. ANÁLISIS DE FACTORES DE RIESGOS

2.1. Departamento de seguridad y continuidad

El ingenio implementa acciones de evaluación para el análisis de riesgos dentro de sus instalaciones, para el trabajo de campo trabajan apegados a otro tipo de protocolos de seguridad, destacan algunas herramientas preventivas a cargo de supervisores de área y supervisores digitales, se nombran así por trabajar específicamente monitoreando cámaras en toda su jornada laboral.

Tabla V. **Herramientas empleadas para el control de seguridad en las oficinas administrativas**

Herramienta	Descripción
Check-list	Con un conjunto de formatos desarrollados para ciertas áreas o controles especiales identifican los riesgos que propician incertidumbres hacia los colaboradores en las oficinas. Son ejecutados o llenados por supervisores destacados en lugares claves para garantizar que se a diario se respetan los protocolos implementados por la empresa.
SWIFT	Emplean esta herramienta de control interno en aspectos críticos de trabajo, les permite anticiparse a algún posible riesgo y evaluación técnica. Por medio de esta herramienta lograron reducir incidentes que podrían suscitarse con aglomeraciones al utilizar las escaleras al salir de la jornada laboral. La demanda de ascensores es alta, por eso algunos empleados deciden utilizar las escalares auxiliares para llegar a planta baja, pero ocasionan alto tráfico al descender por los niveles del edificio junto a otros departamentos y demás personal administrativo.
Diagrama causa-efecto	Herramienta básica, sencilla y fundamental para la gestión de operaciones, en las oficinas administrativas la emplean para lograr encontrar las posibles causas que propician ambientes inseguros de trabajo con riesgos a la salud de sus colaboradores.

Continuación de la tabla V.

Análisis funcional de operatividad (HAZOP)	Para evaluar el rendimiento en los procesos administrativos, se conoce que este tipo de herramienta lo emplean en plantas industriales donde son transformadas materias primas, pero la administración del ingenio logro modelar el protocolo de tal forma que lo adapto para medir el rendimiento de cada tarea asignada a su personal administrativo. El clima organizacional favorece a la cultura de trabajo eficiente al mitigar cualquier foco que permita ocio y trabajo irresponsable con actitudes que comprometan la saludad de uno mismo y de sus colaboradores.

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

El departamento de seguridad de esta forma evalúa continuamente el ambiente laboral, algunas de esas herramientas son automatizadas o se llevan bajo control constantemente desde computadoras que están conectadas a servidores donde se cargan los resultados y parámetros necesarios que permitan analizar sobre situaciones fuera de lo normal para tomar alguna medida preventiva o correctiva.

Este departamento por ser totalmente dispensable trabaja en horarios y jornadas extendidas, caracteriza que al no encontrarse personal administrativo continúan monitoreando las instalaciones para prevenir algún incidente futuro por evento natural como un sismo o conato de incendio, cuando consideran pertinente detener operaciones por alguna fuente de peligro trasladan esta notificación a sus superiores inmediatos quienes evalúan la magnitud del posible evento y accionan de forma inmediata y preventiva.

2.1.1. Responsabilidad del área

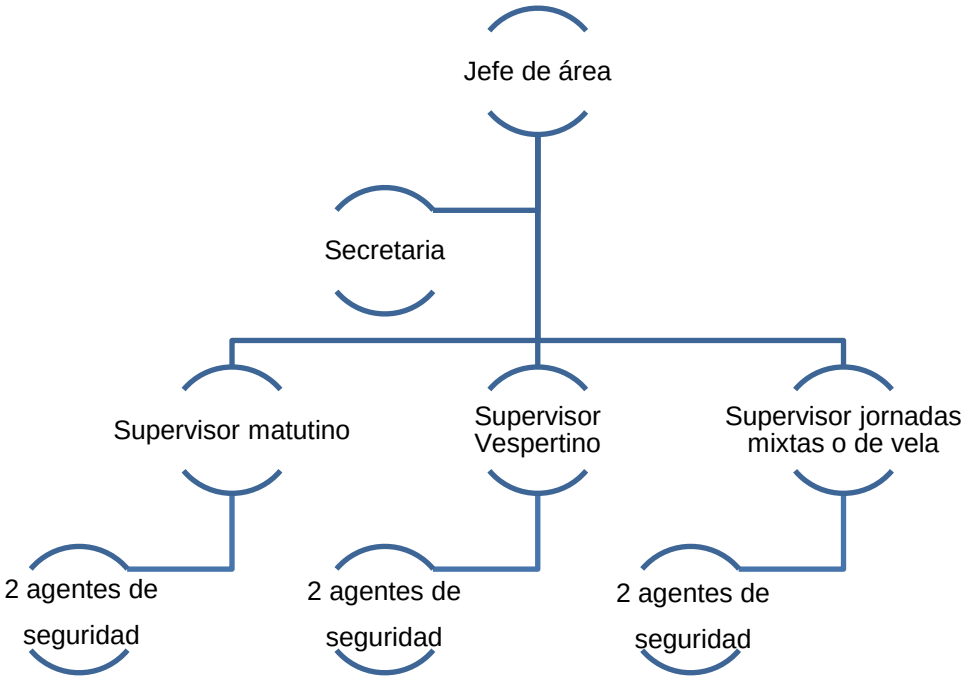
Destacan varias acciones y tareas asignadas a este departamento, lo fundamental es prevenir accidentes, responder activamente cuando se presente alguno y promover el ambiente de trabajo seguro libre de amenazas internas, proporcionar herramientas éticas de trabajo con trifoliares o correos internos compartiendo información necesaria para reforzar la conducta ética en el trabajo.

El departamento de seguridad tiene por función velar por que las instalaciones sean seguras y sin fuente de peligro en los caminamientos, gradas y techos, que las luminarias funcionen eficientemente, velarán por que se encuentren despejados los pasillos y corredores, que las puertas de emergencia estén libres de cualquier obstáculo en todo momento, deberán garantizar que se encuentran visibles todos señalamientos de salida de emergencia. Otra tarea asignada es validar que se disponga del punto de reunión al ser evacuado el personal administrativo, este punto de reunión también deberá permanecer despejado en todo momento.

2.1.2. Estructura organizacional del departamento

Se conforma por un total de 11 personas, el alto cargo está asignado a un jefe, tiene a su cargo una secretaria, 3 supervisores y 6 agentes de seguridad. Se rotan por turnos, 2 agentes quedan al resguardo del equipo de vigilancia todos los días, entregando el turno a las 6 de la mañana en jornada normal de trabajo, el jefe a cargo de esta tarea de seguridad evalúa cada acción o queja trasladada, evalúa los resultados obtenidos por las herramientas para el control de seguridad, diseña estrategias constantemente hacia sus empleados para optimizar el recurso disponible y el tiempo empleado para realizar sus tareas.

Figura 11. **Organigrama del departamento de seguridad**



Fuente: Departamento de seguridad. Ingenio Pantaleon.

Con el control de mando y traslado de tareas en forma vertical, desarrollan sus actividades cotidianas, el jefe de área dispondrá de estrategias necesarias que se deberán implementar a diario para garantizar que el clima organizacional en su estructura sea optimo, que no se presenten malos entendidos y que el personal trabaje acorde a sus oficios asignados.

La secretaria traslada a sus delegados toda la información relevante diariamente, programa la rotación de los agentes de seguridad para no desgastarlos y causarles estrés por trabajo continuo en jornadas extensas, se rotan aproximadamente cada quince días, los de la mañana pasan a la jornada nocturna, los de la jornada nocturna hacia la jornada especial de madrugada, los de la jornada especial hacia la jornada matutina. También es responsable por

llevar la agenda del jefe de área, trasladar y redactar los correos necesarios hacia otras dependencias externas.

Los supervisores se mantienen en constante movimiento, no solamente supervisan a los agentes de seguridad asignados a las oficinas, también prestan servicios auxiliares si es necesario hacia otras jefaturas, si es necesario el traslado de documentación importante ellos realizan estas acciones, los ciclos de medición de resultados es por cada 7 días, evalúan las deficiencias y debilidades en la semana operada, así emiten el debido informe al jefe de área para que considere oportuno tomar alguna cierta respuesta inmediata o a largo plazo para llamarles la atención.

Los agentes de seguridad trabajan constantemente evaluando su entorno, no solamente garantizan la prevención del riesgo ante algún evento de peligro hacia los trabajadores del sector asignado, también garantizan que los propios trabajadores del sector cumplan con el decoro necesario en las relaciones interpersonales y que no se presenten faltas al respeto entre colegas, velaran constantemente por que no se extravíen los equipos de cómputo y de oficina distribuidos en las áreas asignadas.

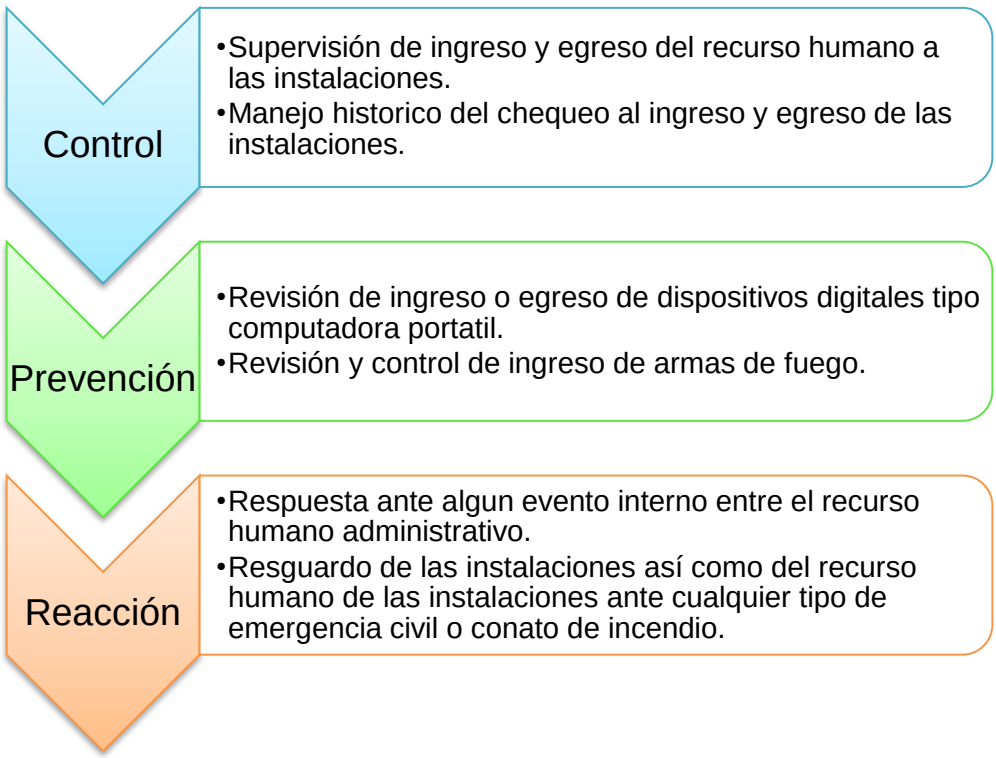
El trabajo en conjunto es de total sinergia, cada agente de seguridad puede optar hacer rondas en tiempos previamente asignados, es considerable que no deberán abandonar su puesto de trabajo por ningún motivo, siempre estará uno de ellos presentes, el personal administrativo considera oportuno la presencia de ellos dándoles respaldo a sus actividades desarrolladas constantemente.

El jefe del departamento de seguridad, evalúa constantemente a todo su personal asignado, ellos se encuentran comprometidos con la empresa.

2.1.3. Atribuciones

Para realizar y desarrollar sus funciones adecuadamente existe principalmente el compromiso hacia la empresa, si existe el compromiso todo el personal de seguridad realiza su trabajo eficientemente. Para el ingenio en las oficinas administrativas es representativa la participación desde el jefe de área hasta cada uno de los agentes, las quejas son mínimas y los resultados son aceptables.

Figura 12. **Atribuciones al departamento de seguridad en las oficinas administrativas**



Fuente: Departamento de seguridad. Ingenio Pantaleon.

2.1.4. Puntos críticos de la gestión actual

El sistema de análisis de peligros y puntos críticos empleados en las oficinas administrativas forman parte del control neuronal del ingenio, identificar los puntos críticos para esta gestión en espacial es trabajo en conjunto de supervisores y jefes de área, de acuerdo al control de los riesgos asociados al trabajo intermitente y los procesos en el manejo de información sensible de la empresa que podrían comprometer resultados mensuales y anuales en la producción total de azúcar hacia el mercado nacional o mercado extranjero.

Para garantizar que el recurso humano administrativo realice el trabajo asignado conforme lo requerido por sus superiores ha sido tarea compleja, la medición de resultados no es inmediata, deberán transcurrir temporalidades de 4 a 6 meses para medir el desempeño unitario o en conjunto por cada departamento. La administración actual emplea pasos estructurados de un protocolo para la determinación de los puntos críticos.

Tabla VI. **Pasos para la determinación de los puntos críticos**

Acción	Descripción del proceso
Identificación de peligros	Los supervisores de los departamentos que conforman el organigrama de la empresa trabajan en conjunto para desarrollar el listado de peligros que pueden ser introducidos, controlados o aumentados en las instalaciones o en algunos procesos administrativos en las oficinas. Emplean estratégicamente las siguientes actividades: • Actividades de revisión para cada paso del proceso (fase intermedia y trabajos terminados) • Equipos de oficina y herramientas utilizadas. • Desarrollo del trabajo final (verificando si cumple con los requerimientos establecidos al ser programada los desempeños administrativos propuestos)

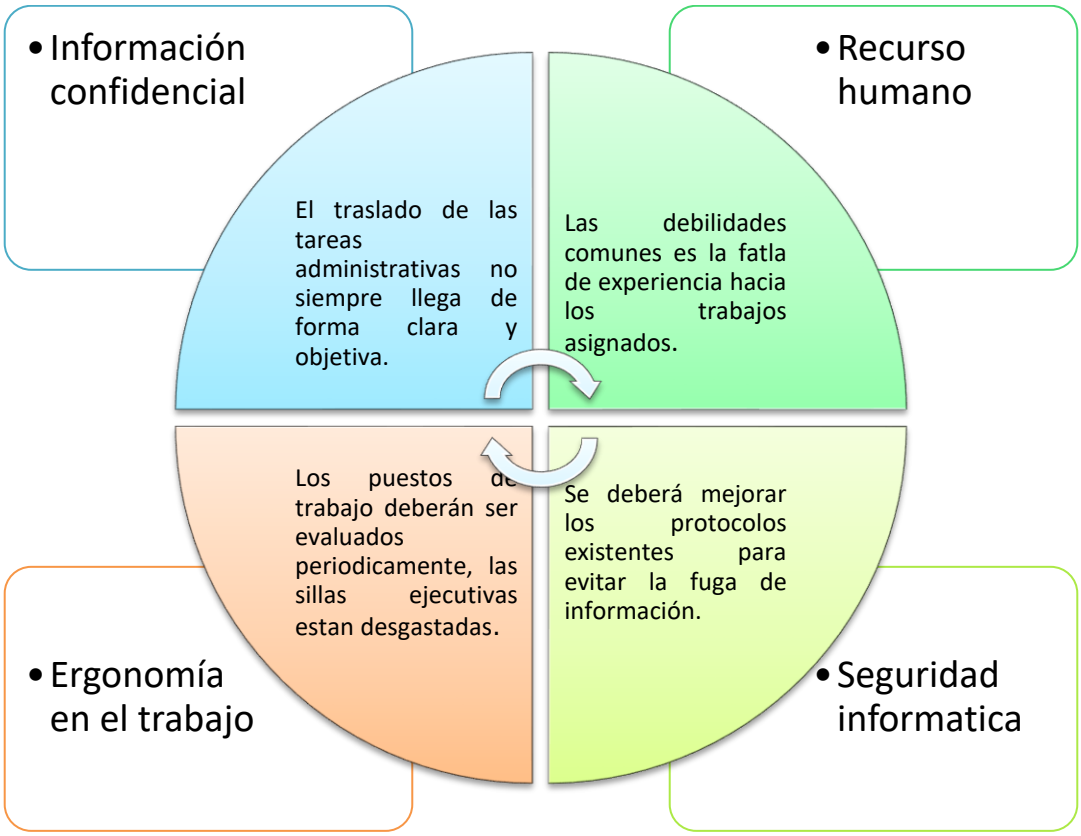
Continuación de la tabla VI.

Evaluación de peligros	Los supervisores en mesa de trabajo multidisciplinario deciden cuales pueden ser los posibles peligros que representa trabajar en las oficinas administrativas, para ello consideran aspectos y valoraciones representativas que pueden afectar la continuidad del trabajo bajo límites de estrés o fatiga. • Ergonomía en el trabajo. • Severidad del daño ante algún accidente (magnitud, duración de la enfermedad, secuela) • Probabilidad de ocurrencia (datos epidemiológicos, experiencia en prevención de riesgos de salud ocupacional, literatura técnica) • Consecuencias de enfermedades contagiosas en entornos cerrados. • Efectos de cansancio crónico a corto y mediano plazo. • Factores que propician la mala conducta laboral en el recurso humano.
Determinación de puntos críticos de control	Aplicar análisis continuo con el contexto de algunos parámetros contenidos en normas HACCP, así delimitan como poder eliminar, reducir o impedir el peligro asociado hacia los trabajos en las oficinas administrativas. Inician trabajando siempre en mesas multidisciplinarias con los supervisores de cada área con la determinación si el riesgo identificado podría ser completamente mitigado o controlado, con el uso de algún protocolo de prerrequisito. De esa forma evalúan cada uno de los riesgos asociados a la gestión actual.

Fuente: Comité administrativo multidisciplinario. Ingenio Pantaleon.

Para la óptima gestión administrativa en la medición de resultados emplean procesos y subprocesos, los resultados obtenidos por el comité administrativo son sólidos, intercambian los focos donde se obtienen debilidades que comprometan la continuidad de las labores, no solamente se miden aspectos técnicos en el recurso humano, a nivel informático monitorean constantemente que no se presenten brechas en la información o extracción de datos relevantes.

Figura 13. **Resumen de los puntos críticos en la gestión actual**



Fuente: Dirección general. Ingenio Pantaleon.

Se evidencia que los puntos críticos en la gestión actual no es responsabilidad de un solo departamento administrativo, el compromiso es múltiple para obtener resultados positivos, reducción de problemas y minimización de brechas que ocasiones fallas repetitivas administrativas.

2.2. Funciones

Lograr determinar los actos inseguros y las posibles condiciones peligrosas que se presenten o se encuentren en la ejecución de los trabajos administrativos

en las oficinas del Ingenio es en si el conjunto de funciones del departamento de seguridad, su fortaleza radica en la prevención de cualquier tipo de eventualidad, ante algún evento inoportuno deberán corregir las circunstancias peligrosas, mitigar el riesgo o controlar cada uno de los factores que dieron parte al potencial peligro, erradicando continuamente así los focos que darían paso a cualquier circunstancia de peligro.

El grado de peligrosidad es en cierto aspecto de incertidumbre, la elocuencia con que los trabajadores se presentan a sus puestos de trabajo se observa sin alteraciones en su conducta laboral, cuando alguno de sus colaboradores muestra indicios de alteración o acciones de agresión conductual, es abordado inmediatamente por los agentes de seguridad asignado a esas oficinas.

Otras funciones aparte de la prevención de incidentes o actos inseguros es garantizar el resguardo las instalaciones, proteger la información confidencial del Ingenio, así como sus activos, mediando el clima laboral responsable entre el recurso humano sus superiores y el manejo de las instalaciones, que sea en permanencia responsable sin obtener beneficios por actos deshonestos al retirar equipos valiosos.

Estas funciones de supervisión, vigilancia, prevención y resguardo de las instalaciones con los equipos contenidos en ella es actividad diaria, estas funciones garantizan la continuidad en las operaciones de la gestión administrativa, sin los protocolos empleados daría paso al desorden total.

2.2.1. Servicios

Los servicios básicos como parte del departamento de seguridad es resguardar los bienes de la empresa, supervisar el comportamiento del recurso humano, tomar de datos de ingresos y egresos a las oficinas administrativas, rendir informes semanales o mensuales de hechos suscitados. El más importante, respaldar a la empresa y el personal que trabaja diariamente con la protección total.

2.2.2. Contingencia

Ante alguna amenaza o evento critico que se pueda presentar emplean un protocolo de contingencia, este protocolo se trasladara en el siguiente diagrama de evolución.

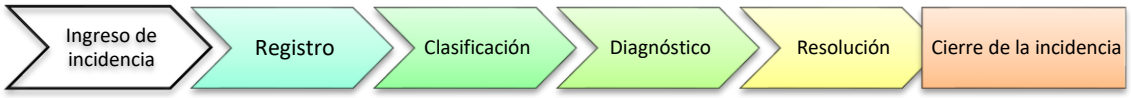
Figura 14. **Secuencia de respuesta ante alguna emergencia**

Fuente: Departamento de seguridad. Ingenio Pantaleon.

2.2.3. Gestión de incidencias

Los supervisores y personal asignado a las tareas de seguridad interna, realizan diferentes tareas al momento de presentarse algún evento inesperado. Los supervisores de cada departamento tienen asignada esta tarea, ante la respuesta inmediata de uno de ellos alguno de los trabajadores deberá tomar su cargo y realizar esas tareas en la gestión de incidencias.

Figura 15. **Diagrama de la gestión de incidencia**



Fuente: Departamento de gestión de operaciones. Ingenio Pantaleon.

El diagrama en la figura anterior representa como se realiza una gestión, las gestiones dependerán de la ocurrencia del evento, no se presentan reportes diarios de incidencias, hecho menos como llegadas fuera de horario normal de ingreso de trabajo no considerado como incidencia.

Tabla VII. **Descripción de las etapas en la gestión de incidencia**

Actividad	Descripción
Ingreso de incidencia	Se llena el formulario digital disponible en el sistema interno de la empresa indicando el motivo, la acción suscitada y el por qué se está gestionando.
Registro	El registro se efectúa en la red interna asignando un número de evento para el seguimiento del mismo.
Clasificación	Se clasifica según la tipicidad que se haya suscitado, si es por emergencia, por algún tipo de queja administrativa o por algún incidente externo.

Continuación de la tabla VII.

Diagnóstico	Se evalúan las causas ingresadas en la gestión inicial, según el departamento donde fue ingresada la gestión es el personal asignado para evaluar los acontecimientos, comúnmente es el departamento de recursos humanos que evalúa estas gestiones, asigna el personal necesario para delimitar responsabilidades y emitir los juicios correspondientes con las sanciones necesarias.
Resolución	Luego de realizar la investigación necesaria, evaluar la participación de una o varias personas en los hechos ocurridos emiten la resolución acerca de las acciones necesarias para que se dé la pronta solución, incorporando acciones preventivas y responsabilizar individualmente a quien sea necesario.
Cierre de la incidencia	Se da por concluida la gestión al notificar a las partes involucradas de lo resolución obtenida, se da por finalizado en el sistema, pero queda la bitácora para futuras fuentes de consulta.

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

Estas acciones fueron descritas por el departamento de recursos humanos, se respetará la jerarquía interdepartamental al evaluar acontecimientos asociados a otros departamentos si ocurriera así algún evento inesperado.

2.3. Descripción de la maquinaria

Las computadoras asignadas son de tipo escritorio ejecutivas con cuerpo rígido, incluye monitor para computadora de 22 pulgadas, las capacidades de operación son de 1 Terabyte de almacenamiento interno, 12 Gigas de memoria Ram, procesador I7 con disco duro sólido. Estos equipos se conectan a la red interna con restricción de usuarios a ciertas páginas de navegación, la red dispone de conexión a otros equipos de oficina, los protocolos de seguridad en

esta red interna son bajos, podrían ser víctimas de ciberataques o robo de información confidencial, destaca en el Ingenio que cada usuario consigna el registro de acciones diarias, pueden asociarse los movimientos en la red de forma inmediata, la debilidad es que no se encuentran conectados en tiempo real a los servidores corporativos.

2.3.1. Sistemas operativos

Las computadoras asignadas están configuradas con licencias de software Windows, la red interna denominada Artnet es usada bajo licencia anual, otros sistemas adicionales fueron desarrollados por petición y objetivos especiales del Ingenio, son utilizados para control automatizado de ingreso y egreso del personal administrativo, así como el tráfico interno donde se encuentran puntos de acceso y control de tarjetas magnéticas.

2.3.2. Equipos

Los equipos asignados varían según el puesto ocupado o las tareas asignadas, algunos comparten recursos tipo impresoras o *scanners.*

Tabla VIII. **Equipos disponibles en las oficinas**

Puesto delegado	Equipo disponible
Colaborador común, supervisor y jefe de área	Computadora de escritorio
	Impresora
	Scanner
	Teléfono de escritorio
	Destructora de papel
Jefe de área	Computadora tipo portátil

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

2.4. Descripción de los procesos

Para garantizar que las tareas asignadas sean efectivamente realizadas, el ingenio implementa diferentes protocolos de supervisión y administración. Dentro de estos procesos se ejecutan controles de mando superiores delegando tareas y atribuciones según el rol del puesto, la mayoría de procesos evaluados fueron administrativos donde se obtiene bajo nivel de incertidumbre por tareas diferenciadoras, las tareas que se ejecutan cotidianamente en las oficinas administrativas son exclusivamente en trabajo de escritorio, solamente los agentes de seguridad y sus supervisores realizan rondas esporádicas dentro y fuera de las instalaciones, no se obtuvo acceso total a las tareas asignadas por puestos desarrollados.

2.4.1. Administración de accesos

El trabajo bipartito del departamento de recursos humanos y el departamento de informática garantiza el resguardo de los usuarios junto a los accesos asignados, previo a ser autorizado el usuario de un nuevo integrante a la red de trabajo interno se filtran las credenciales de seguridad del mismo, si no ha pertenecido a algún grupo delictivo, si no ha participado o ha estado involucrado en acciones de robo o similares penadas por la ley, si la persona es mentalmente estable, si está dispuesto a firmar la cláusula de confidencialidad para preservar toda la información que por sus manos pueda circular.

Si el departamento de Recursos Humano da el visto bueno ante estas evaluaciones preventivas de cada personal contratado o por contratar asigna el proceso de apertura de usuario al departamento de informática, este departamento incorpora los datos generales del contratado, impresiones dactilares, fotografía reciente, atributos dentro de la empresa, accesos de transito

otorgados dentro de las instalaciones, asignación de horarios de almuerzo, entre algunos de diferentes variables consignadas.

Los accesos deberán ser validados por el jefe de área a donde está asignado el nuevo empleado, de esta forma todos los ya contratados fueron participes de este proceso para trabajar con su usuario, contraseña y tarjeta electrónico de accesos.

2.4.1.1. Coordinador de seguridad

Su roll es preventivo y de monitoreo, administra protocolos de accesos informáticos, puntos de control del personal cuando ingresan a las instalaciones, distribuye tareas a los agentes de seguridad por cada turno, prevale la prevención y minimización del riesgo ante eventos de peligro que puedan comprometer la seguridad en las instalaciones.

2.4.1.2. Coordinador control interno

Constantemente evalúa datos obtenidos por programas digitales que evalúan las acciones de todo el personal distribuido por áreas en las oficinas administrativas. Verifica que los resultados sean muy cercanos a las proyecciones estimadas por sus superiores, con la participación multidisciplinaria efectúa evaluaciones inmediatas cuando alguna persona no está cumpliendo con las tareas asignadas o presenta constante abandono de su puesto de trabajo asignado.

Distribuye tareas a los supervisores de las áreas asignadas de supervisión, esperando resultados constantemente, se miden los resultados por el alcance de metas ejecutadas, y miden la eficiencia en los tiempos presentes de los

colaboradores con el mínimo índice de abandono de su puesto de trabajo, traslada las quejas a los superiores inmediatos para que ellos accionen de manera que indiquen los protocolos por departamento asignado.

2.4.2. Gestión de protección

La protección del resguardo de las oficinas administrativas, el equipo disponible y su recuso humano es tarea continua del departamento de seguridad y seguridad informática. La interconexión en distribución de tareas automatizadas entre departamentos permite que el Ingenio optimice los recursos disponibles garantizando el clima organizacional con respaldo y reacción ante cualquier eventualidad.

Se trabajan en reuniones semestrales con jefes y supervisores de los departamentos interesados en la gestión, se presentan ideas que mejoren la protección de personas y recursos tangibles como no tangibles, se proyectan supuestos panoramas que podrían dar paso a alguna reacción negativa entre los trabajadores, se prioriza la salud humana, luego de eso la información interna que podría llegar a ser vulnerabilizada, le preceden los equipos de cómputos, las instalaciones oficinistas y por último punto los bienes o pertenencias de los colaboradores.

Toda gestión inicia con la descripción del futuro panorama que podría darse en función de determinadas causas negativas, se evalúan las causas clasificándolas de peligrosas, agresivas o inesperadas naturalmente, se priorizan las causas peligrosas derivadas por agresión conductual, paralelamente se trabajan en la prevención informática que podría ocurrir al conectar dispositivos externos a la red interna, donde el departamento de informática diseña cortafuegos para evitar estas acciones.

2.4.2.1. Coordinador de seguridad

Para asignar el coordinador de seguridad es sometido a votación por los jefes de las áreas participantes en la gestión de protección, evalúan diferentes aspectos relevantes colocando puntuación, el que obtenga mayor puntuación de un listado de 10 personas como mínimo podrá ser asignado como el coordinador de seguridad.

Figura 16. **Atributos evaluados a la persona asignada como coordinador de seguridad**

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

La pirámide que emplea el departamento de recursos humanos gestiona diferentes niveles cualitativos y cuantitativos para poder optar a este cargo se deberán cumplir cada uno de los 7 niveles de la pirámide, se asignan valoraciones internas en el proceso de clasificación, solamente se obtuvo acceso a este tipo de información no se logró obtener información clasificada de la toma de decisiones internas en la fase de selección y reclutamiento de esta persona, la pirámide constituye características físicas y psicológicas optimas que la persona indicada deberá contener. Se inicia el reclutamiento a nivel interno, de no encontrar al indicado la plaza pasa a nivel externo para recibir propuestas de futuros candidatos.

No solamente se evalúan los perfiles obtenidos, para este reclutamiento en la fase pre final son sometidos a diferentes evaluaciones físicas y psicométricas, se hace interacción con un grupo pequeño de personal asignado para recrear algún evento de emergencia, comúnmente es un conato de incendio con dirección de desalojo y puesta en resguardo de estas personas, se simula un herido para medir el nivel de estrés y respuesta del futuro candidato, de los posibles candidatos que cumplen con el perfil de la pirámide son seleccionados 3 para la última evaluación y simulación.

2.4.2.2. Coordinador control interno

El protocolo de selección es similar al coordinador de seguridad pero con menos atributos y habilidades consignadas, su evaluación es sesgada hacia la administración de recurso humano, su roll es validar que las tareas de prevención de riesgos sean ejecutadas oportunamente, evalúa al personal de seguridad y presta auxilio a tareas administrativas al recurso humano que requiera apoyo en problemas menores, por citar alguno; cuando un empleado no puede registrar su acceso con la tarjeta electrónica.

2.4.2.3. Analista de seguridad

Resguarda los controles y registros históricos de cada evento que sale de lo considerado como normal, garantiza que los empleados cumplen con sus patrones de comportamiento normales sin presentar algún tipo de peligro a sus demás compañeros de trabajo o hacia las instalaciones de la empresa.

Este analista trabaja con proyecciones en la prevención de riesgos asociados a las malas acciones interpersonales del conjunto de áreas asignadas, no solamente evalúa los patrones de comportamiento diarios que apoyado en programas con histogramas de frecuencia ejecutan protocolos de predicción sobre toma de decisiones unitarias o grupales, el analista de seguridad trabaja independientemente para no sesgar la toma de decisiones según el criterio creado por los análisis previos realizados.

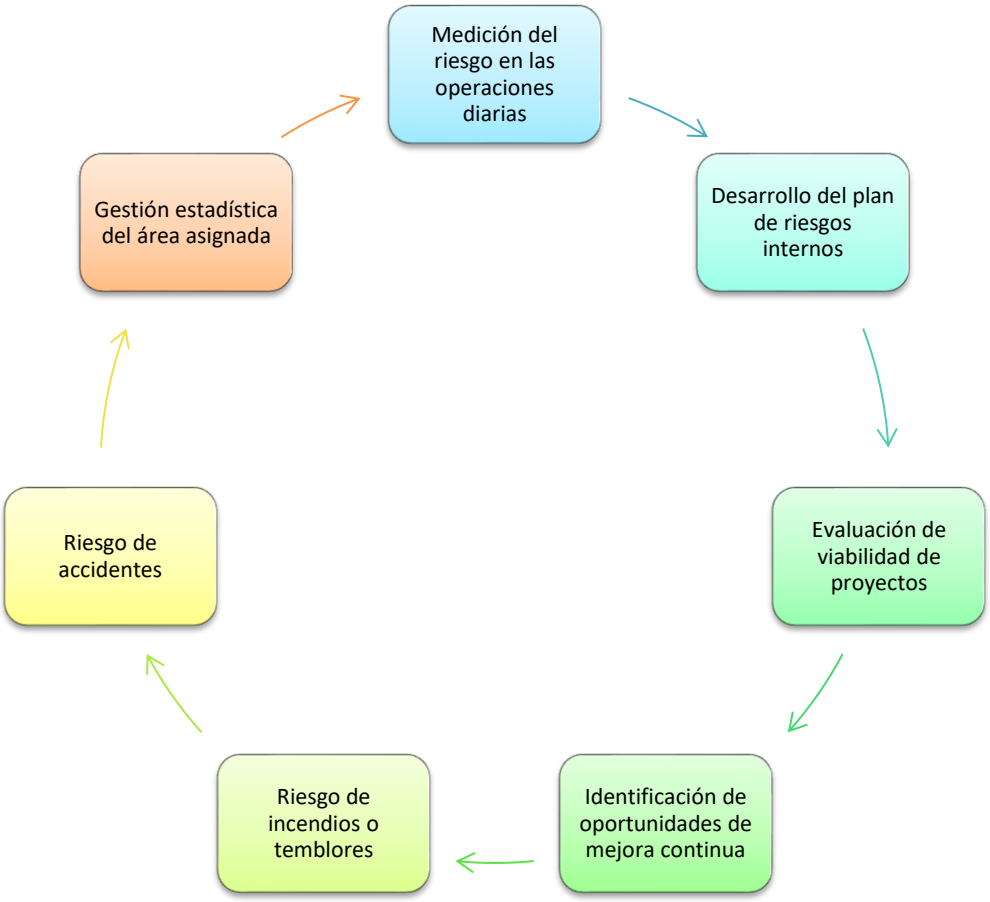
2.5. Análisis de riesgos

El Ingenio separa el tradicional analista de riesgos financiero con el analista de riesgos de seguridad ocupacional con atributos y alcances de riesgos informáticos, esta acción ha sido relevante para la empresa ofreciendo el diferenciador hacia lo cotidiano, se desarrolla de esa forma para otorgar tareas de prevención, seguimiento y resolución de problemas que puedan darse en las actividades cotidianas.

En la atribución y delimitación de tareas para este cargo asignan diferentes parámetros, el perfil de la persona responsable a cargo de estas tareas deberá someterse a un conjunto de filtros y etapas que permitan otorgar al personal idóneo, recordando que su acción erradica en la prevención, no se permiten las

ocurrencias de eventos que comprometan los procesos administrativos de la empresa y la gestión de operaciones se detenga por actos inesperados.

Figura 17. **Funciones asignadas al análisis de riesgos**



Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

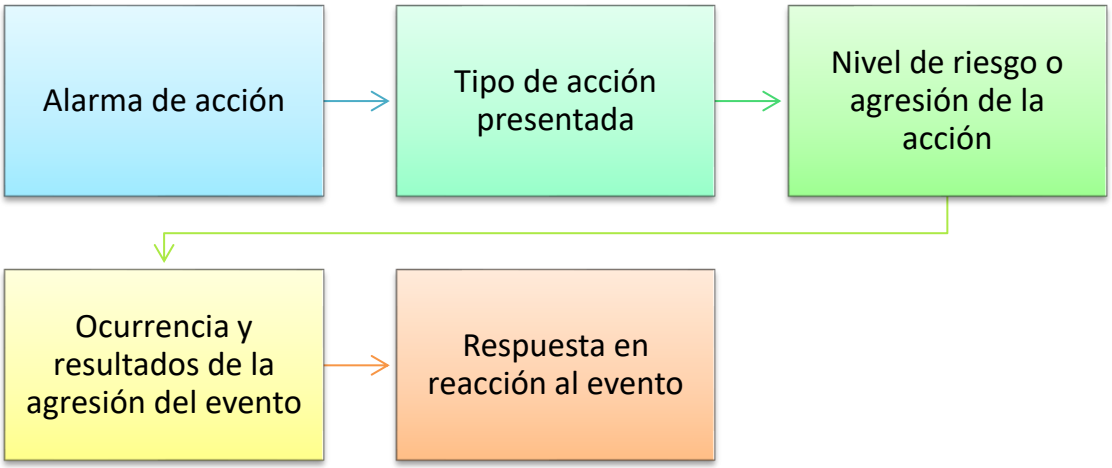
El departamento de recursos humanos describió el diagrama presentado en la figura anterior, inicia el proceso de estas funciones asociadas al análisis de riesgo con la medición del riesgo en las operaciones diarias, se otorga prioridad al recurso humano para estas acciones.

2.5.1. Identificación de eventos

Los eventos podrían estar asociados a malas prácticas en el trabajo, según información descrita por los supervisores difícil que se presenten eventos que comprometan la seguridad informática o la salud humana de los colaboradores, los protocolos de prevención con charlas de capacitación por el departamento de recursos humanos cumplen su función. Los eventos pueden ser identificados por el tipo de efecto provocado, no se conocen reportes internos de violencia interna, los reportes constantes son relacionados por fallas en los sistemas de computación o por equipos que no encienden por las mañanas.

Utilizan un diagrama interno para describir el evento o darlo por ocurrido si está siendo presente.

Figura 18. **Protocolo de identificación de eventos**

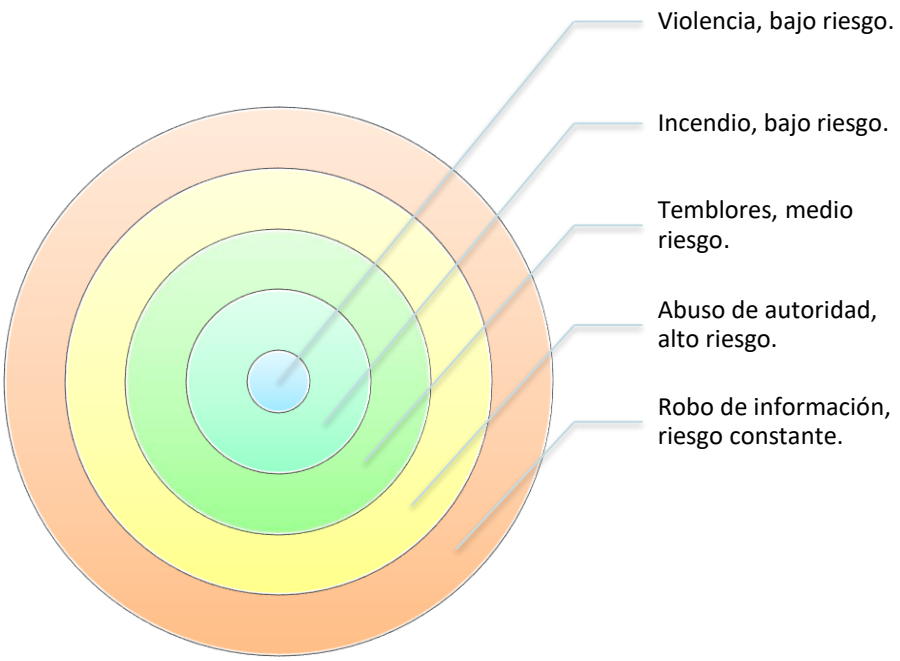


Fuente: Departamento de seguridad. Ingenio Pantaleon.

2.5.1.1. Eventos

Los eventos que podrían dar pauta a respuesta o reacción inmediata se valoran por el nivel de peligrosidad o por los alcances que puedan comprometer la salud de los colaboradores, otros eventos que son monitoreados es el robo de información interna.

Figura 19. **Eventos clasificados en la empresa**



Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

Los eventos según el departamento de recursos humanos se valoran por la probabilidad que ocurra desde bajo riesgo hasta riesgo constante, según esta empresa el riesgo latente y continuo es que se extraiga información confidencial para ser vendida a la competencia.

2.5.1.2. Factores influyentes

Las malas prácticas laborales asocian mayormente a los factores influyentes en los eventos que se han presentado. Las estadísticas representan que por descuidos o errores humanos se presentaron incidentes de baja valoración, no se ha presentado algún evento de violencia o robo de información.

Según el departamento de recursos humanos influye en las acciones hacia la toma de decisiones de su recurso humano por estar sometidos a niveles elevados de estrés, algunos pueden ser influenciados por su nivel de endeudamiento, otros por ingesta de licor, los factores académicos evidencian que las personas trabajan apegados al reglamento interno sin entorpecer las actividades asignadas, los cargos de rango inferior con poca preparación académica han mostrado ser susceptibles ante propuestas que comprometan sus principios y valores éticos hacia la empresa.

2.5.2. Análisis de matriz de riesgos

El departamento de recursos humanos lidera la evaluación de los posibles riesgos que podrían ocurrir en las instalaciones, trabajando paralelamente se encuentra el departamento de seguridad, otros departamentos influyen en que se cumplan las debidas acciones preventivas para garantizar que los colaboradores sin importar el rango o puesto ocupado obtengan el clima organizacional optimo donde se resguarda y garantiza su salud física y mental. Los supervisores son constantemente evaluados y capacitados para mantenerse a la vanguardia de riesgos influyentes o acciones interpersonales que podrían comprometer la intención de mala fe entro los propios compañeros de trabajo, se respetan las jerarquías y puestos asignados.

Tabla IX. **Matriz de riesgos en la prevención de actos inseguros**

CONSECUENCIAS	PROBABILIDAD					
		Raro	Poco probable	Posible	Muy probable	Casi seguro
	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

Para el departamento de recursos humanos es efectivo establecerse constantemente en los rangos bajos de probabilidad de ocurrencia, para ese rango existen todos los protocolos de prevención con los puestos distribuidos en personas de supervisión y control ya descritos. Cuando se presentan actos de riesgos medio se acciona con formatos de corrección y prevención, evaluando los hechos que llevaron a que sucediera estos eventos. No se han presentado actos inseguros donde se podrían localizar con consecuencias catastróficas y probabilidad casi segura.

Mensualmente se evalúan los resultados obtenidos donde pueden ser considerados niveles de riesgos que no se pueden dejar pasar por alto, la prevención es parte integral de los valores del Ingenio. La matriz no es validada solamente hacia el recurso humano que trabaja en la gestión de operaciones, también es desarrollada y aplacada al personal de seguridad, con mayor objetividad por ser los únicos en portar armas cortas dentro de las instalaciones. Se les asignan este tipo de armas para responder ante cualquier posible evento que comprometa la salud física individual o colectiva del área asignada para el resguardo total, la prevención será efectiva con tasa del 0% de eventos suscitados, si este valor cambia la prevención no es efectiva.

2.5.3. Riesgos operativos

Riesgos operativos como tal no se presentan, el trabajo es exclusivamente de oficina, no hay peligro o riesgo de caídas por trabajos en alturas, tampoco se efectúan trabajos pesados, el único riesgo operativo presente es el cansancio crónico y las posturas ergonómicas inadecuadas por prolongados tiempos de trabajo.

2.5.4. Grado de exposición de riesgos

La exposición al riesgo operativo es casi nula, las tareas asignadas son exclusivamente de escritorio, utilizando equipos de computación, exposición al choque eléctrico podría ser una causa casi finita en que pueda ocurrir. Se logró evidenciar que las conexiones y conectores son seguros.

2.6. Análisis de protocolos actuales

Los protocolos muestran algunas debilidades, el compromiso de los supervisores se nota desgastado y con baja participación. Los protocolos empleados son una década de antigüedad, no presentan acciones ante escenarios futuros que no fueron contemplados al diseñar estas acciones preventivas.

La mayor debilidad se presenta en el protocolo de seguridad del departamento de informática, los usuarios pueden acceder a información interna sin dejar registros de su revisión, copia y guardado en dispositivos móviles, se deberán incorporar acciones preventivas para garantizar que la información en los servidores del Ingenio no sea copiada sin los debidos permisos de superiores que administran y resguardan dicha información.

2.6.1. Manejo de accesos

El departamento de informática es quien asigna los usuarios y claves los accesos a la red interna es vulnerable, todos los empleados que dispongan de una computadora de escritorio conectada a la red interna pueden acceder a información clasificada que no es de importancia hacia las tareas asignadas o el trabajo programado.

2.6.2. Manejo de permisos para visitas y consultores

Otro factor que maneja el departamento de informática, la recepcionista envía por correo los datos de las personas que visitan las instalaciones asignándoles un permiso especial y temporal, este permiso es creado y autorizado por el departamento de informática, que en un lapso menor a un minuto digita los recursos necesarios para autorizar el ingreso habilitando una tarjeta electrónico temporal con accesos a ciertas áreas de interés.

2.6.3. Manejo de internet

La red interna permite navegar en internet sin restricciones, no se presentan protocolos de seguridad o programas antispyware que garanticen los ataques externos al extraer información sensible de cada puesto de trabajo donde es accesado vía web. El departamento de informática ha presentado varias propuestas para limitar el uso de la navegación libre de los trabajadores, pero se han opuesto algunas autoridades dividiendo la votación para llegar a un punto en común donde se permita limitar ciertas paginas o accesos restringidos desde la web interna, por lo que se trabaja expuestamente a cualquier tipo de ataque cibernético o robo de información confidencial.

3. SISTEMA DE GESTIÓN ADMINISTRATIVA

3.1. Administración de roles y perfiles

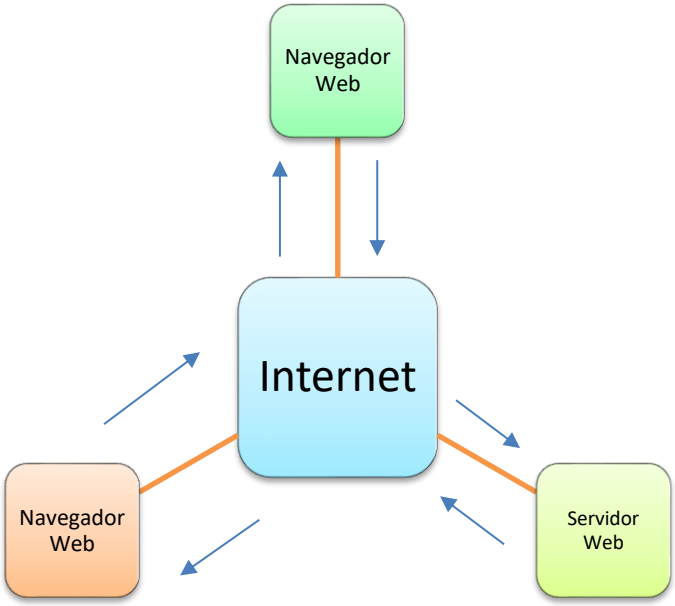
Antes de presentar el diseño propuesto para la administración de roles es conveniente introducir un poco de contenido acerca del modelo de gestión que podría ser utilizado en las oficinas administrativas del Ingenio, por diferentes aspectos en desarrollo, monetarios y accesibilidad a licencias de propiedad.

Para la administración eficiente se plantea incorporar el desarrollo tecnológico relacionado con la arquitectura web. Se describe como una aplicación de carácter informático que puede ser ejecutado en el medio WEB conocido como arquitectura WEB que permite a múltiples usuarios disponer de un canal de comunicación utilizando el internet como medio hacia un servidor WEB.

Los usuarios que puedan accesar algún navegador especifico trasladan sus peticiones vía HTTP hacia el servidor WEB que automáticamente responde a cada solicitud. Dentro del servidor quedan resguardadas las diferentes aplicaciones WEB que pueden ser empleadas en la red interna de comunicación con diferentes servicios hacia los usuarios conectados. Dentro del servidor WEB se concentran las cargas emitidas de datos en el tráfico diario generado por el trabajo cotidiano. Diferentes desarrolladores informáticos comparten la idea que en la mayoría de los usuarios industriales el uso del navegador prediseñado e instalado sirve únicamente para mostrar información interna (modelo de cliente

ligero)[3] dentro de este navegador no se desarrolla ningún tipo de procesamiento que relacione información confidencial o información crítica de la empresa.

Figura 20. **Arquitectura web**



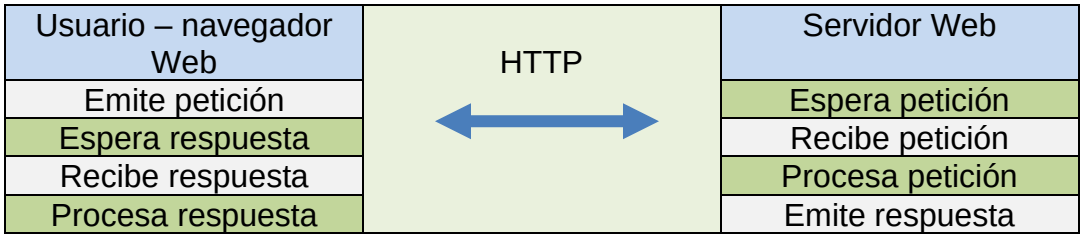
Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Este modelo básico pero eficiente permitirá comunicarse en cualquier tiempo en vivo entre *n* puntos de control, cada navegador deberá ser configurado desde el servidor a través de la red local de internet. Acá iniciaría el proceso de creación y autorización de usuarios. En el intercambio de datos con arquitectura

[3] MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Web genera un modelo de comunicación entre cada usuario independiente y el servidor empleando un navegador conectado al servidor la comunicación se genera mediante el uso de protocolo HTTP.

Figura 21. **Comunicación web**



Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Según la imagen anterior, el usuario de interés podrá interactuar con las diferentes aplicaciones Web que disponga el Ingenio a través del navegador. Acá inicia el desarrollo de la gestión administrativa, se proveerá de un usuario identificado para cada colaborador, este usuario consignará una única contraseña, para cada colaborador se le asignará una sola computadora, esta computadora podrá tener comunicación Web con otros equipos de interés según los cargos asignados.

Los resultados inmediatos son captados en la base de datos del servidor, cada petición es enviada y alojada con la red neuronal o aplicación Web. Normalmente se puede hacer uso de bases de datos extensas que han sido almacenadas con toda la información relevante hacia el trabajo que se debería estar desarrollando. El servidor procesará cada petición esta petición es analizada bajo condicionamientos previamente establecidos por los altos mandos

y jefes de área, luego de resolver la petición otorga la respuesta al navegador que representa a un usuario.

Dependerá de cada permiso establecido según la jerarquía de participación en el modelo efectivo para los accesos de usuarios de bajo rango, mandos medios, supervisores y jefaturas con el acceso total hacia los demás.

Para la propuesta en la gestión administrativa se podría incorporar el módulo SUM Server, este módulo de servidor es ejecutable de aspecto consola no presenta interfaz de multi usuarios, este tipo de servidor se ejecutará en modo *batch* con las aplicaciones necesarias. Puede ser desarrollado en lenguaje Visual Basic o con tecnología Microsoft .Net empleara el sistema gestor de base de datos SQL Server para crear y autorizar los respectivos accesos hacia la información necesaria.

Para este módulo SUM Server podría llegarse a ejecutar multi tareas correspondientes a infinitas peticiones de cada usuario autorizado con acceso, serán generadas desde el módulo on line SUM Web.

Tabla X. **Gestiones que se podrán realizar desde el servidor SUM Server**

Nombre de la gestión	Descripción
Gestionar el alta hacia cada usuario	Para esta acción o determinada activada se desarrolla la incorporación de nuevos usuarios al sistema.
Gestión para la asignación de determinados perfiles	Dentro del servidor se gestiona la acción y asignación de perfiles específicos a cada usuario existente dentro del sistema. Los permisos son restringidos para quien realiza esta acción.

Continuación de la tabla X.

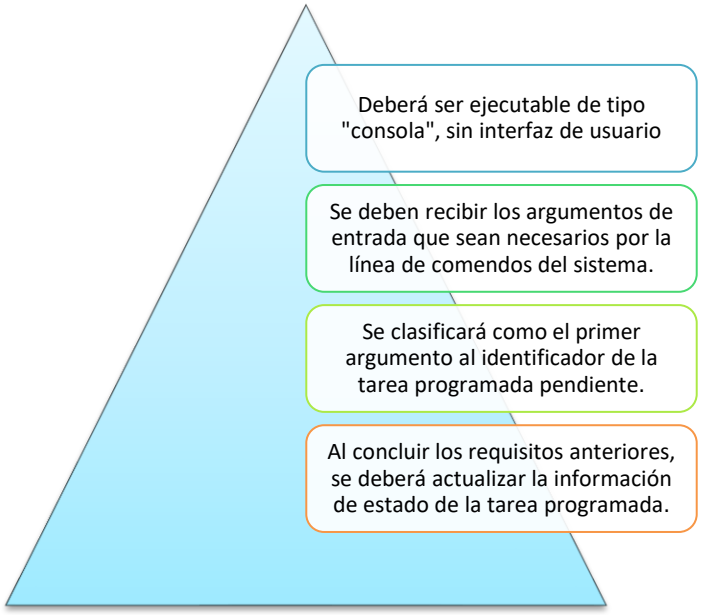
Gestión para la eliminación de usuarios	La gestión estaría diseñada para eliminar usuarios ya establecidos en el sistema (servidor), se hace eliminación definitiva, se eliminan sus atributos, accesos y permisos otorgados, únicamente se resguarda el historial de los accesos he interacción dentro del sistema.
Gestión de tareas programadas y peticiones.	Dentro de esta actividad se deberán actualizar los estados o permisos, las fechas y resultados de las peticiones de cada usuario ejecutadas así como las tareas que fueron programadas a dichas peticiones.

Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Una de diferentes garantías de ciberseguridad es porque el módulo de servidor no se encuentra interconectado o integrado hacia algún sistema externo con accesos compartidos. Cuando se da inicio a esta aplicación es a través del sistema externo de planificación de tareas (STM), este es responsable de gestionar las infinitas tareas planificadas y programadas. El protocolo se basa con diferentes requisitos que pueden ser detallados según las necesidades del Ingenio.

Para los requisitos del servidor SUM al integrarse en funciones en la empresa, deberá ser invocado el modulo Server siempre que se plantee alguna tarea programada con la correspondencia hacia el subsistema de planificación de tareas del entorno de trabajo. Cada requisito deberá ser debidamente completado, de no ser así fallará la operación restringiendo el acceso hacia las siguientes tareas.

Figura 22. **Requisitos de SUM Server para la integración de tareas**



Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Cuando se da inicio al módulo SUM Server, recibirá la totalidad de los argumentos que fueron enviados hacia la entrada por cada línea de comando dentro del sistema. Para ello se deberá respetar el protocolo de sintaxis de invocación evitando cualquier error de redacción que dará por fallida la tarea.

Tabla XI. **Aspectos complementarios al desarrollo de la integración de tareas al servidor SUM Server**

Acción y tarea	Descripción o composición
Formato de sintaxis	○ Ruta de asignación y posible nombre del fichero ejecutable. ○ Identificador de cada tarea programada. ○ Identificador de alguna acción a ser ejecutada (nuevo usuario, asignación de perfil a usuario y eliminación de usuario) ○ Nombre de usuario solicitante. ○ Contraseña de tipo cifrada del usuario solicitante. ○ Tipo de argumento en función de la posible acción a ejecutarse.
Descripción de cada argumento de entrada para incorporación de usuarios.	○ Nombre del usuario que solicita esta función. ○ Nombre completo del usuario que será creado. ○ Contraseña nueva totalmente cifrada del usuario que será creado.
Descripción de argumentos para asignar el perfil de cada usuario.	○ Identificador del posible perfil a ser asignado. ○ Nombre de usuario de asignación. ○ *True/False* para eliminar o continuar los permisos previos del usuario de asignación.
Descripción de argumentos para realizar las entradas al eliminar un usuario.	Nombre del usuario que será eliminado.

Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

La administración de roles y perfiles se basará por el tipo de tarea necesaria a incorporarse, si es por reclutamiento o incorporación de un nuevo usuario o perfil se delimitará por un conjunto de procesos y fases establecidas, si es por eliminación de un usuario o por asignar el tipo de perfil.

Tabla XII. **Procesos para la administración y creación de un nuevo usuario**

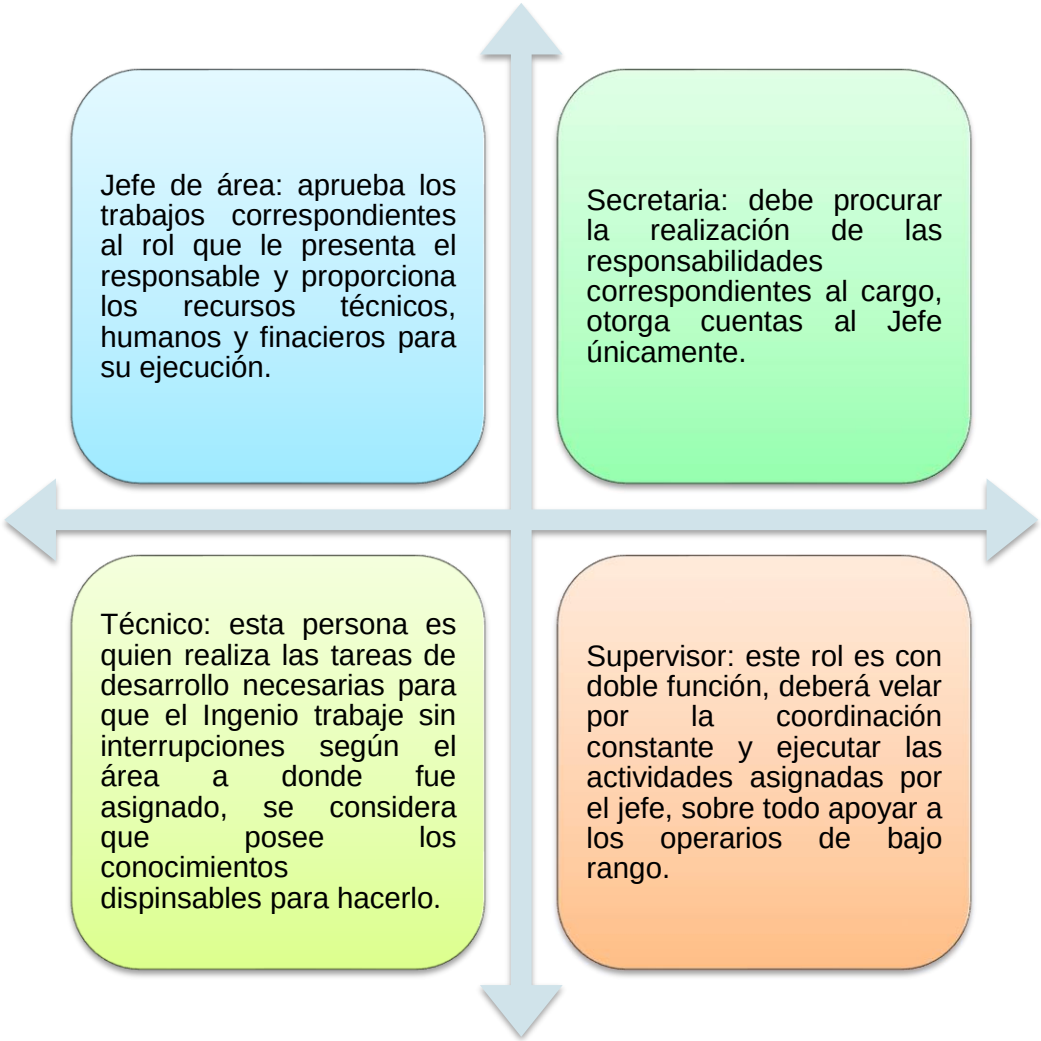
Acción en el proceso	Descripción y alcance
Tipo de acción	Crear usuario.
Responsable	Gerente y jefe de área.
Objetivo	Crear un usuario en el sistema.
Descripción	Se deberá crear el registro de un nuevo usuario que generó la acción de solicitud.
Precondiciones	Recepción del perfil y roll con parámetros específicos para la creación de un nuevo usuario.
Postcondiciones	Usuario creado.
Flujo normal	• El usuario invoca el módulo SUM Server a través de los comandos establecidos con los siguientes parámetros: o Ruta del fichero que será ejecutado. o Identificador de la tarea programada a ejecutar. o Identificador de cada acción a ejecutar. o Nombre del usuario solicitante. o La contraseña que ha sido cifrada del nuevo usuario solicitante. o Nombre del usuario que será creado. o Confirmación de contraseña. o Nombre completo del usuario que ha sido creado y registrado. o Asignación de roll dentro del organigrama empresarial. • Ingresa el software para comprobar el número de argumentos que fueron recibidos en las entradas recibidas como las acciones a ejecutar. • El sistema otorga la validación con permiso de acceso y contraseña del usuario solicitante. • El sistema reconoce el identificador del departamento al cual será asignado el usuario solicitante, se asigna el departamento de destino. • El sistema empleando la arquitectura informática crea el nuevo usuario de tipo no especial en el departamento destino, se exceptúa de esta regla los altos cargos o rangos superiores. • El sistema actualiza los campos de petición: estado OK, fecha y hora de actualización de estado y marcar como no visible. • El sistema ejecuta otro comando final, actualiza el estado con fecha y hora que fue incorporado, limita con base a las descripciones del perfil el conjunto de tareas y permisos programados.
Fin del proceso	El usuario ya aparece registrado con limitaciones según su roll en la oficina.

Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

La administración podrá ser dirigida con las herramientas de este servidor, podrían ser automatizadas las tareas diarias y programarse evaluaciones periódicas para cuantificar los avances y resultados previos, no dependerá el manejo de las operaciones solamente a esta herramienta tecnológica, la participación constante de directores junto a jefes de área en concordancia con los supervisores asignados, podrán medir constantemente las acciones tomadas por cada persona en forma individual, este crecimiento va de la mano con la revolución digital con uso de la automatización. Administrar el recurso humano con nuevas herramientas digitales será la tarea a superar.

Con la necesidad de establecer los roles se podrían presentar las responsabilidades, tareas y asignación de recursos entre los roles y los puestos de trabajo, para altos mandos, rangos intermedios y operadores de bajo nivel. Se dispondrá de cómo pueden participar para cada puesto en estos tres rangos para la asignación de su rol según el nivel de responsabilidad.

Figura 23. **Roles, responsabilidades y puestos de trabajo propuestos**



Fuente: elaboración propia.

3.1.1. Actualización y perfiles

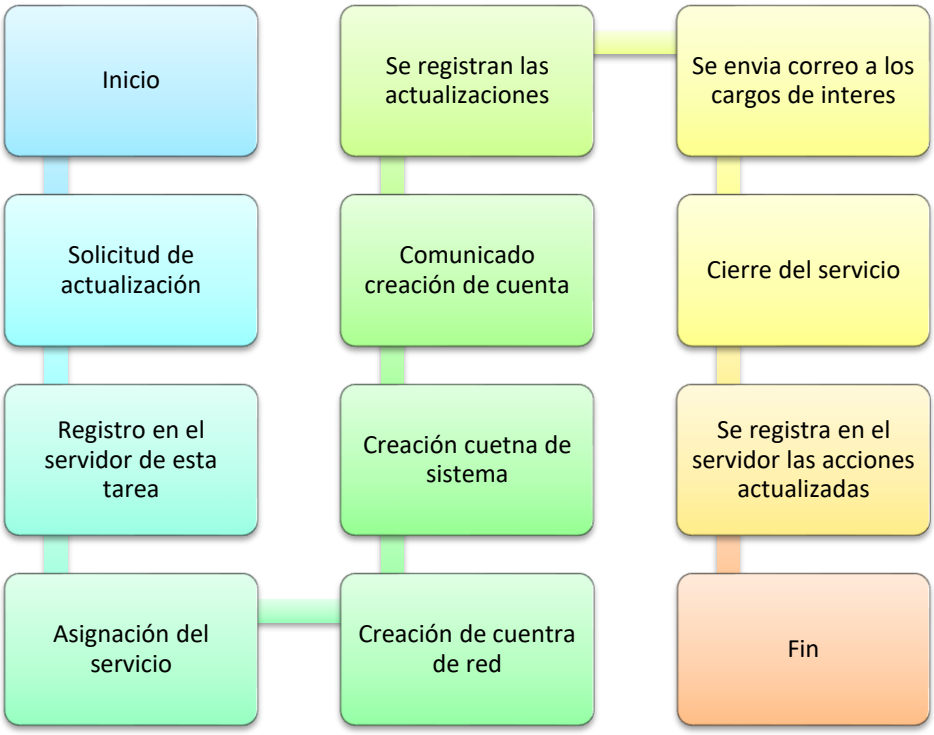
Se deberá crear la solicitud específica, la cual será autorizada exclusivamente por el jefe de área o jefe de departamento. Se asignará la especificación de cuentas, roles y privilegios hacia algún nuevo sistema de

información que será utilizado. Bajo los privilegios cedidos por el jefe de área acciona el supervisor para asignar el nuevo perfil y rol esperado con privilegios estructurados para dicho usuario de interés.

Se deberá llenar la solicitud del usuario claramente para dar la actualización conforme el perfil deseado, donde no se dupliquen puestos o funciones, dentro del sistema se deberán realizar los cambios específicos. Se deberá guiar por el documento de roles que está bajo el resguardo del departamento de recursos humanos y los permisos otorgados según el jefe de área. El supervisor dejara registrado en el software del servidor el tipo de actualización según el perfil del usuario de interés y los privilegios asignados nuevamente.

Luego de esto se deberá colocar la solicitud en estado concluido y finalizado. El supervisor de área debe enviar el correo interno hacia los departamentos involucrados o de interés con la actualización de cierto perfil de usuario vía correo electrónico en la Web interna explicando el por qué se dio este tipo de acción, quien fue quien lo autorizo. Los supervisores cuando pretendan realizar estas acciones deberán anotar cada detalle de la actualización donde se originó la causa y el motivo que lo origino, si estas causas fueron por sanciones, por traslados horizontales, por crecimiento dentro de la empresa o por ganar ascensos según la plaza ocupada. Cada uno de estos detalles deberá quedar registrado en el servidor para ser evaluado en correlación a las actividades desarrolladas y la evaluación de resultados recientes.

Figura 24. **Evolución de actualización de perfiles**



Fuente: ALARCÓN ÁVILA, Rodrigo. *Implementación de un modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos.* http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2694/Trabajo%20de%20grado.*pdf?sequence=1&isAllowed=y.* Consulta: 22 de mayo de 2021.

Las actualizaciones variaran en el tiempo de trabajo, según información histórica del Ingenio es poco frecuente realizar este tipo de acciones. Dependerá de promociones por puestos internos, despidos o causa de muerte de sus colaboradores. Las directrices diseñadas para ejecutar las labores cotidianas no representaban atrasos operativos, el problema radicaba en los protocolos de protección y comunicación entre los técnicos que realizan las labores constantes

hacia los supervisores y el manejo total de información por los jefes de área, el diseño podría mejorar la toma de decisiones a futuro.

3.1.2. Levantamiento de puestos

Esta tarea se realizará por los supervisores, de forma presencial en cada puesto, se comparará con el manual de perfiles y roles que posee el departamento de recursos humanos, se podrán realizar incorporaciones que destaquen el trabajo eficiente para el tipo de puesto en análisis. No se podrán realizar cambios sin antes evaluarlos con el jefe de área. Este levantamiento consistirá en anotar cada una de las actividades que realiza el técnico, desde que se le fue asignado usuario y perfil. Luego podrá hacerse la comparación de lo ya diseñado versus lo que realiza. De esta acción se propiciará mejoras inmediatas.

3.1.3. Análisis de los procesos

Cuando el Ingenio da por hecho implementar nuevos procesos para la gestión administrativa, su primer paso será definir la estructura organizacional con las funciones y responsabilidades que garantice la ejecución de las tareas y actividades desarrolladas. La designación del personal a estas nuevas tareas es activamente necesario a tal punto crítico de no entregar o delegar las responsabilidades para cierto perfiles o usuarios no se podrá obtener el alcance esperado y la efectividad requerida.

El recurso humano se podrá ir definiendo en los procesos administrativos dependiendo del tamaño del departamento de interés, otro factor crítico es considerar el alcance previamente definido dentro del proyecto enfocado en la gestión de asignación de usuarios, roles y perfiles que garanticen resguardar la información confidencial con los procesos internos establecidos. El proyecto por

sí solo no tomará forma sin el compromiso de los jefes de área, las tareas no podrán ser ejecutadas sin el compromiso de los supervisores.

Existen diferentes actos inseguros al implementar los procesos establecidos, en el campo de la informática todo el panorama futuro es incierto, desde pasar el techo económico propuesto para incorporar esta propuesta y los resultados ralentizados al emigrar hacia la nueva tecnología, deficiencias en el uso de la plataforma Web como la falta de experticia se los usuarios al iniciar a trabajar en este modelo.

Figura 25. **Riesgos en los procesos propuestos**

Fuente: elaboración propia.

3.1.4. Roles y responsabilidades

Los roles estarán establecidos por cada departamento de interés, el acompañamiento se dará con el departamento de recursos humanos quienes poseen la base de datos de todos los colaboradores de la empresa con el historial de crecimiento interno, las responsabilidades ya fueron divididas y segmentadas, la máxima autoridad por departamento es el Jefe de Departamento, lo precede la secretaria oficinista, que es la responsable de trasladar la información constante a los supervisores y los técnicos de bajo rango, para este estudio se les denomina técnicos a todo el personal que labora con diferentes tareas productivas administrativas en el uso de una computadora de escritorio.

3.1.5. Comité de riesgos

Se deberá crear este comité con la finalidad de estudiar las amenazas internas y amenas ante algún posible ciberataque externo. Se enfocará en analizar y tomar decisiones conjuntas, se podrán guiar y apoyar con la matriz de riesgos consignada en la tabla IX. Este comité podrá trabajar en sentido multisectorial y transversal hacia todas las actividades de la empresa donde se permita evaluar constantemente con permisos otorgados por la alta dirección.

Se podrá conformar por un equipo multidisciplinario, con la participación de recurso de bajo rango, supervisores y jefes de área, por cada departamento de influencia podrán participar como mínimo 2 técnicos y como máximo 5 para participar deberán poseer reputación impecable sin faltas a sus labores, se incorporarán 1 o 2 supervisores por cada departamento y de forma remota pero siempre informados cada jefe de departamento o jefe de área.

Tabla XIII. **Funciones del comité de riesgos**

	Tipo de función y alcance
•	Deberán determinar cuales podrán ser los límites de tolerancia que podrán evitar los escenarios de peligro y riesgo. A nivel informático visualizarán cuales podrían ser las acciones inseguras que comprometerían la información de la empresa.
•	Se deberán proponer el desarrollar los planes de contingencia. El comité deberá establecer las acciones a tomar cuando se presente algún evento que compromete la salud de sus colaboradores. Se deberán comprometer para fortalecer el uso de las nuevas herramientas tecnológicas y trabajar para diseñar los protocolos de prevención al navegar en el nuevo servidor.
•	Se priorizará en fomentar la cultura corporativa ante los riesgos frecuentes.
•	Deberán establecer canales de recepción y comunicación para compartir la información de todos los departamentos que conforman el comité de riesgos. De esa forma se recepcionará información constante en tiempo en vivo sobre los peligros que se están enfrentando ante determinada eventualidad.
•	Procurar que la misión y visión paralelamente a los objetivos estratégicos del Ingenio para que sean afines hacia las medidas propuestas y dispuestas para mitigar eventuales contingencias.
•	Determinar los focos de riesgo que constantemente asedian a cada departamento, se deberán analizar por separados los límites que deberán ser respetados por otros departamentos.

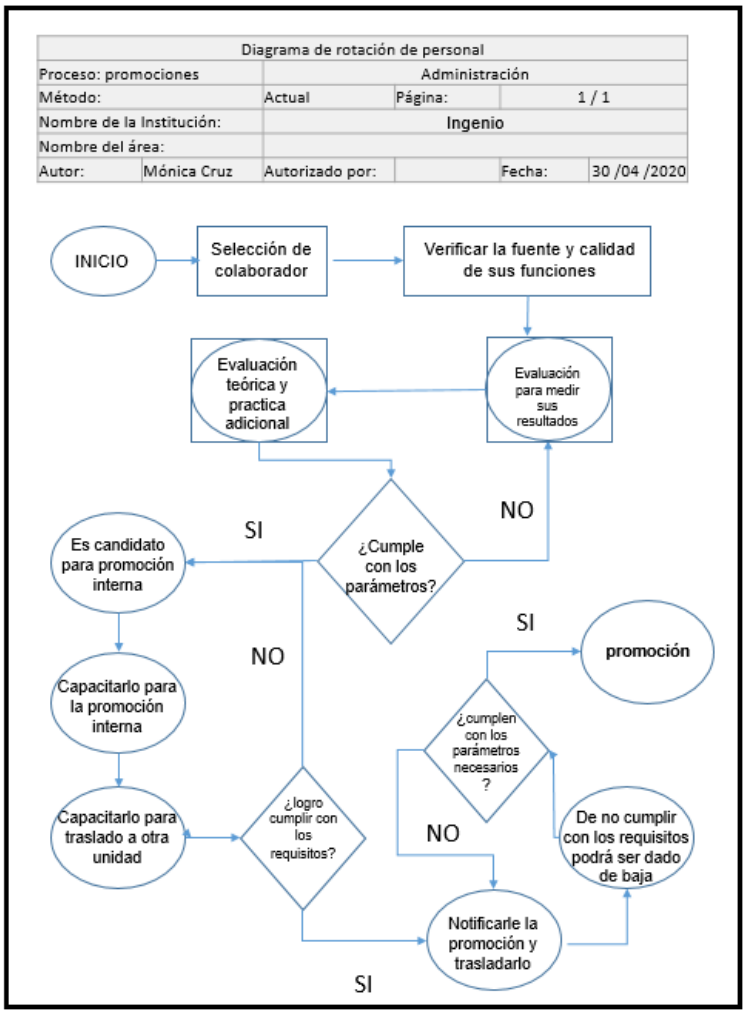
Fuente: elaboración propia.

El comité de riesgo por ser un grupo multidisciplinario deberá programar las reuniones de trabajo para medir los alcances y problemas que se han suscitado en un determinado tiempo luego que inician sus acciones. Se les deberá autorizar el uso de alguna oficina especial de trabajo donde puedan trabajar sin ruidos externos y factores que interrumpan las reuniones.

3.1.6. Procedimiento para altas, bajas y cambios

Actualmente recursos humanos emplea herramientas funcionales para la promoción, cambios o bajas de sus colaboradores, podría incorporarse a ese modelo un diagrama que mejore la relación en la toma de decisiones.

Figura 26. **Diagrama de procedimiento para promociones internas de los colaboradores**



Fuente: elaboración propia, empleando Visio 2016.

El monitoreo constante sobre los avances de las tareas asignadas de cada colaborador es trabajo compartido, por cada departamento involucrado en la gestión de administración implementan registros cualitativos donde los parámetros medibles son aspectos cotidianos acerca de su desempeño, valorización hacia su puesto y alcances de metas establecidas, otro aspecto relevante que destaca en el Ingenio es la evaluación del clima organizacional para obtener métricas del comportamiento social dentro de los grupos seleccionados de trabajo, esta herramienta destaca para organizar por preferencias compartidas a ciertos elementos que pueden mejorar la producción en determinada distribución física en su departamento de trabajo.

Tabla XIV. **Medición de resultados del último trimestre del año 2020**

Actividad	Medición de resultados
Tareas asignadas	0,95%
Valorización de su puesto	0,85%
Alcance de metas globales	0,96%
Relaciones sociales	0,72%
Clima organizacional	0,66%
Percepción del lugar asignado	0,70%

Fuente: Departamento de recursos humanos. Ingenio Pantaleon.

Los datos de la tabla XIV demuestran debilidades en ciertas actividades de análisis, el departamento de recursos humanos indico que el número 1 sería la meta alcanzada, el clima organización en general demuestra la mayor debilidad, en relación a eso recursos humanos indico que ese valor se compone por la sumatoria de por lo menos 5 variables medibles dentro de las oficinas, parte de este compromiso limitado en la evaluación denotaba que el uso de complejos sistemas de computación afectaban a sus colaboradores.

Figura 27. **Mapeo de actividades evaluadas en el último trimestre del año 2020**

Fuente: elaboración propia, empleando Microsoft Excel 365.

La responsabilidad del departamento de recursos humanos podrá influir en los puestos asignados, previo a realizar alguna promoción deberán someter estos datos hacia impulsar mejoras inmediatas que permitan mejorar la gráfica, en la figura 27 se aprecia que la percepción hacia el puesto de trabajo asignado es débil y que su clima organizacional es de igual o menor aceptación.

Con las promociones de puestos dependerán de los roles asignados y los perfiles impuestos por las diferentes personas que influyen al determinar cuáles son las tareas a realizar y cuáles son los resultados esperados, estas personas no podrán trabajar dando lo mejor de sí en un entorno que no es propicio para explotar sus fortalezas y habilidades. Es relevante lograr establecer los mecanismos que comprometan el trabajo en equipo donde los supervisores no solamente evalúen y ejecuten órdenes directas, donde la salud ocupacional

pueda ser relevante, así como los resultados de la producción esperada para cada nuevo ciclo de tiempo.

3.2. Monitoreo de seguridad

Está actividad está diseñada para proteger la información confidencial ante las amenazas internas o las amenazas externas. El conjunto de actividades de seguridad informática internas se centrará en los colaboradores sin distinción de perfil, puesto o rol asignado, la red informática junto al servidor también formarán parte de estas acciones, se fundamentará toda acción maligna que comprometa la información y los sistemas operativos que dispone para desarrollar las actividades diarias en la gestión administrativa.

El monitoreo de la red interna abarcará el rendimiento total desde los colaboradores de bajo rango hasta las jefaturas incluyendo las estaciones de vigilancia de los guardias de seguridad. Este desempeño de monitoreo es empleado para crear datos del rendimiento de la red, otro aspecto que se evalúa continuamente es el comportamiento típico o atípico del recurso humano. Con estos datos obtenidos se puede medir la eficiencia del tiempo que este recurso humano gasta en sitios no relacionados con el trabajo, cuantas veces accedieron a sus cuentas personales y redes sociales o simplemente cuanto fue el tiempo que estuvieron interactuando con el programa de interés que se les ha asignado para desarrollar su trabajo cotidiano.

Fortalecer el esquema del monitoreo otorga a la empresa el manejo de paquetes de datos constantes, por medio de estos paquetes de datos se pueden diseñar esquemas de necesidades de mejoras continuas hacia el sistema de seguridad. La diversidad con el avance informático es poder realizar multitareas al mismo tiempo, combinando monitoreo con evaluación y mejoras.

“Las personas asignadas a desempeñar estas tareas realizarán pruebas por el método de penetración”[4], con la intención de encontrar brechas de la seguridad en el servidor y la red interna. Se conoce que personas que se dedican al robo de información realizan este tipo de actividad por afuera de la red especialistas en seguridad informática utilizan el mismo recurso. Este tipo de pruebas de penetración es realizado de forma aleatoria sin proyectar un punto final en la red. No se reporta a los colaboradores o altos cargos que se lleva a cabo para no limitar su participación en cualquier acción negativa que podrían estar realizando. Generalmente al realizar las pruebas de penetración internas son incluidas las características internas de las medidas de seguridad informática, los evaluadores intentan violar la red de las computadoras de los colaboradores y evaluar las posibles brechas en la seguridad interna.

Cuando se obtienen reportes de infracciones de seguridad, sin discriminar falsas alarmas o falsos positivos, se procederá a implementar el procedimiento de seguridad distribuyendo el reporte a la autoridad superior inmediata. Estos informes deberán incluir una explicación clara de lo que sucedió, en que momento ocurrió, como fue la respuesta de seguridad ante el incidente, qué persona de seguridad lo descubrió y cuáles fueron las medidas abordadas para resolver el asunto. Este tipo de acciones deberá ser una rutina común para la seguridad en la gestión administrativa del Ingenio con el constante monitoreo de redes y monitoreo de seguridad física para proporcionar al Ingenio datos estadísticos que permitan mejorar los procedimientos de seguridad y su eficiencia ante la exposición accidental o intencional.

[4] MAGIO, Sasha. *Actividades de monitoreo de seguridad interna y externa*. https://techlandia.com/actividades-monitoreo-seguridad-interna-externa-info_194844/. Consulta: 15 de junio de 2021.

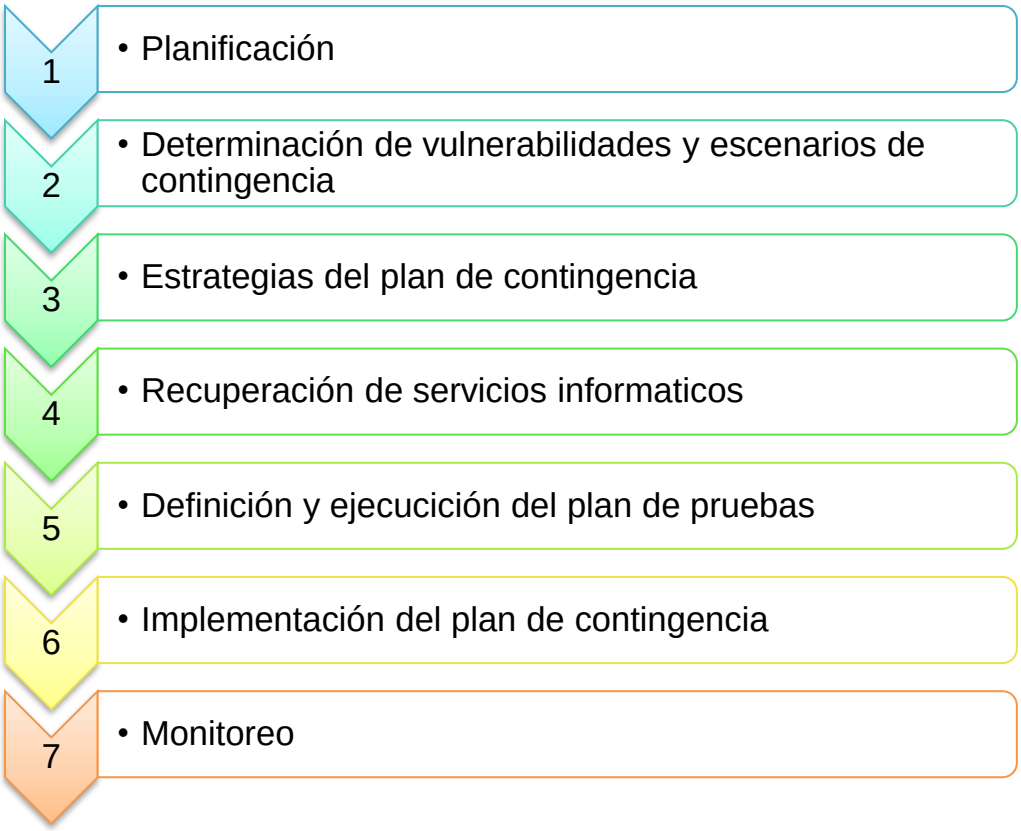
3.2.1. Plan de contingencia

Para el Ingenio implicará el análisis de los posibles riesgos a los cuales podrían estar expuestos sus equipos de computación, equipos periféricos y equipos conectados de forma remota a la red interna por donde se pueda obtener alguna brecha de acceso a su información. Para el departamento de seguridad o seguridad informática corresponderá aplicar las medidas de seguridad y protección para estar siempre preparados en afrontar contingencias y desastres por diversos tipos de acciones.

El alcance del plan de contingencia estará relacionado con la infraestructura de la red informática, así como todos sus procedimientos relevantes asociados al servidor interno y su plataforma tecnológica. La infraestructura tecnológica se conforma por software, hardware y elementos periféricos que complementan el traslado de información o datos críticos para el funcionamiento del Ingenio. Todos sus procedimientos relacionados y relevantes a la red informática, serán contemplados como las tareas que el recurso humano realiza frecuentemente al interactuar con la Web interna generando data critica, generación de reportes, consultas específicas y envíos de correos internos.

La orientación del plan de contingencia radica en establecer el adecuado sistema de seguridad lógicas y física en la prevención del riesgo de desastres informáticos o perdida de información clasificada, de tal forma que se puedan establecer las medidas destinadas a respaldar y proteger la información contra los daños producidos por ciberataques, daños naturales o daños específicos por el hombre en general. Para el Ingenio la información que se maneja en las oficinas administrativas representan uno de sus principales activos con rasgos invaluables económicamente, la prevención es la herramienta básica a utilizar.

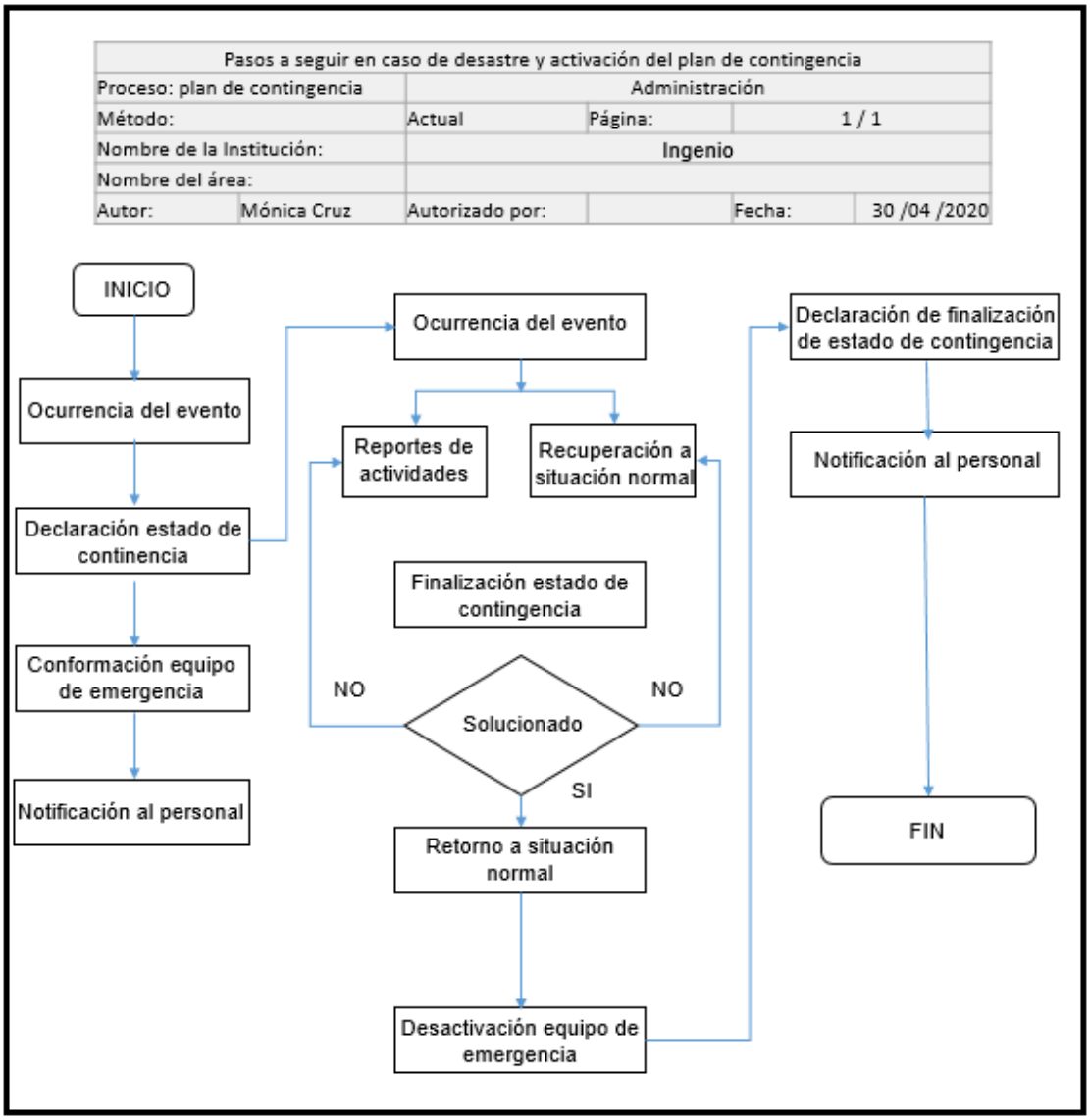
Figura 28. **Fases del plan de contingencia**



Fuente: elaboración propia.

Se deberán desarrollar las 7 fases propuestas para planear, desarrollar e incorporar el plan de contingencia, se indicarán aspectos relevantes en la propuesta se desconocen aspectos internos que podrían comprometer las acciones cotidianas en el Ingenio. Se considera que para la creación de este plan sería importante contar la participación de todos los departamentos involucrados en el cruce de información, cada representante de cada departamento podría aportar datos o rasgos críticos que permitirán tomar acciones preventivas y emergentes al suscitarse algún evento que vulnere la seguridad informática o física de los equipos como del servidor.

Figura 29. **Pasos a seguir al presentarse un desastre y la activación del plan de contingencia**



Fuente: CIFCO. *Plan de contingencia equipo informático*. https://www.studocu.com/en-us/document/navarro-college/computer-organization/plan-de-contingencia-para-equipo-informatico-2014-r2/17908576. Consulta: 15 de junio de 2021.

El diagrama servirá al personal a cargo de implementación del plan de contingencia para poder guiarse, trasladar la información al recurso humano sería importante para que tengan conocimiento de lo que pueda estar realizándose ante algún evento que comprometa la seguridad informática.

3.2.2. ISO 27001

La Norma internacional fue emitida con el fin y descripción de cómo gestionar la seguridad de la información dentro de las empresas. Se presenta el esquema que podrá incorporar el ingenio con una serie de controles y actividades basadas en la Norma ISO 27001.

Tabla XV. **Actividades y controles a implementar basados en la Norma ISO 27001**

Control	Establecimiento de control	Actividades a implementar
Política de control del acceso	Difundir la información de la política de seguridad respecto a la política de control de acceso. Se propone eficientizar las políticas de control de acceso incorporando el bloque automático, horarios de registros.	La difusión de las nuevas políticas podrá ser realizada por el departamento de recursos humanos. Incorporar bloqueo automático luego de 4 minutos de inactividad es lo recomendado.
Registro de usuarios	Modificar la gestión de creación de cuentas de usuario según el rol y perfil en donde se establezcan los permisos de cuentas, autorización de permisos y bloqueos, registro de contraseñas y derechos de accesos, se deberá establecer la definición de responsabilidades y retiro definitivo de algún usuario.	Cada empleado debe poseer un ID único en el directorio activo. El departamento de recursos humanos deberá informar a través de correos internos cualquier novedad que se presente con el recurso humano sobre ingresos, retiros, vacaciones o bloqueos.

Continuación de tabal XV.

Gestión de privilegios	Para la modificación en el sistema sobre la creación de cuentas de usuario deberá realizarse desde el servidor en la carpeta raíz por el jefe de informática bajo supervisión de alta gerencia. Por cada ID incorporado o creado para cada empleado se deberá automatizar los privilegios, permisos, mapeos de acciones diarias. Deberá ser aprobado y puesto en ejecución al incorporar el nuevo servidor en la empresa. Deberá ser incorporado y establecido en las auditorías internas la revisión de los privilegios de los usuarios dentro de todos los subsistemas de la empresa.	Se deberá ejecutar el procedimiento necesario para la creación de cuentas de usuarios. Con la debida verificación del cumplimiento de las responsabilidades del jefe de informática en calidad y seguridad. Se deberán realizar auditorías internas para revisar los privilegios de los usuarios dentro de cada uno de los sistemas de la empresa. Cada jefe de área deberá enviar la solicitud de rol y permisos que tendrá cada uno de sus colaboradores según las tareas asignadas y perfil correspondiente.
Gestión de contraseñas para usuarios	Todas las cuentas según la Norma contarán con el manejo seguro de las contraseñas con la limitación de súper usuarios en casos que no sean requeridos y eliminar usuarios de funcionarios que sean de otros departamentos.	Para la seguridad del usuario en control de su privacidad y el manejo de su información, se deberán cambiar las contraseñas por cada culminación de mes, se incorporarán 8 caracteres que deberán incluir como mínimo 4 letras. Otras aplicaciones de dirección se autenticarán con otro tipo de niveles de seguridad.

Continuación de tabla XV.

Uso de contraseñas	El departamento de recursos humanos deberá divulgar las políticas de seguridad relacionadas al uso y dominio de las contraseñas de seguridad, realizando campañas de concientización para el uso y manejo adecuado con la prevención de no intercambiar usuarios y contraseñas con sus compañeros de trabajo.	Se deberán ejecutar campañas de prevención para hacer uso de razón y conciencia a los colaboradores de la empresa en resguardar sus contraseñas celosamente y no intercambiarlas por estricta confidencialidad y responsabilidad limitada.
Procedimiento de ingreso seguro	Se establecerá controles con limitaciones sobre intentos permitidos al inicio de la sesión. Se deberán incorporar monitoreos sobre las cantidades de intentos fallidos según el usuario y el equipo de cómputo. Otra herramienta esencial será limitar los horarios de inicio de sesión.	Se deberá ejecutar como política de control activo para los bloqueos por ingresos fallidos. Recursos humanos deberá trasladar las acciones previas y estás nuevas reglas en los procesos agregados a los usuarios.
Identificación y autenticación de usuarios	Tendrá que verificarse los usuarios genéricos en aplicaciones o dispositivos periféricos dentro de la Web o red física, para realizar el mapeo y seguimiento sobre las acciones de cada usuario en tiempo real. Los perfiles de supervisores no deberán gestionar tareas normales o regulares, deberán ser específicos en las solicitudes internas.	Cada colaborador deberá ser autenticado por el directorio raíz del servidor. Cada permiso de acceso de estos colaboradores será administrado desde el departamento de informática.

Continuación de tabla XV.

Sistema de gestión de contraseñas	La Norma establece que se deberá incorporar la gestión de contraseñas con características y especificaciones únicas que individualicen a cada usuario y puedan ser gestionados por separados. Se deberán considerar los siguientes aspectos: ID único por usuario, dar permisos de selección y cambio de contraseña, agregar selección de contraseña segura, imponer cambios de contraseña temporales dentro del servidor, conservar el historial como registro de contraseñas previo para emplear alguna ya utilizada, garantizar que se emplean por lo menos cuatro letras en la contraseña con sistema cifrado. Se deberán fortalecer las políticas de seguridad hacia los controladores del servidor.	En las políticas de control interno de seguridad se deberán incorporar y establecer los requerimientos de las contraseñas.
Tiempo de inactividad de la sesión	Según la Norma que se deberán evaluar los tiempos de manejo de tiempos de inactividad según los programas de mayor uso con las tareas asignadas. Se podrá monitorear todo tipo de acción que represente amenaza a la empresa y los cierres de sesión fuera de los rangos de horarios activos.	El control de tiempos de inactividad para las aplicaciones, se coordinará con los diferentes supervisores de aplicaciones la implementación de dichos controles.

Continuación de tabla XV.

Restricción del acceso a la información	Para las políticas de control del servidor deberán fortalecer las acciones preventivas, desarrollar acciones según las auditorías de prevención en riesgo de información.	Incorporar políticas de prevención de delitos informáticos, ejecutar auditorías internas constantemente.
Fuga de Información	No se permite fuga de información con la implementación de sistemas de prevención de seguridad y auditorías constantes que permitan encontrar brechas y violación en accesos remotos o periféricos.	Incorporar dispositivos adicionales de seguridad en la red periférica y redes externas a las instalaciones.
Aprendizaje debido a los incidentes de seguridad de la información	Se deberá crear el procedimiento de control de registro de incidentes reportados acerca de brechas de seguridad identificando los eventos e incidentes que corrompieron la seguridad informática o vulneraron algún equipo físicamente. Se deberá establecer un canal de comunicación ajeno al conocimiento de los demás usuarios para asegurar la respuesta inmediata de manera ordenada y eficaz.	Existe cierto margen de incertidumbre acerca de lo que podría suceder y de ejecutar reactivamente el protocolo de seguridad.
Controles de auditoría de los sistemas de información	Las auditorías internas serán la prioridad para la empresa, se coordinarán acciones de prevención en los sistemas de información y el resguardo del servidor a instalar.	Se debe incorporar el manual de auditoría interna y acciones preventivas o correctivas en el proceso de evaluación y mejora.
Protección de las herramientas de auditoría de los sistemas de información	Para los registros de auditoría se deberán incorporar controles de prevención debidamente revisados y auditados constantemente por el personal del departamento de informática con restricciones especiales hacia accesos al servidor.	El departamento de calidad o de seguridad será el responsable de definir los accesos a los registros de auditoría.

Continuación de tabla XV.

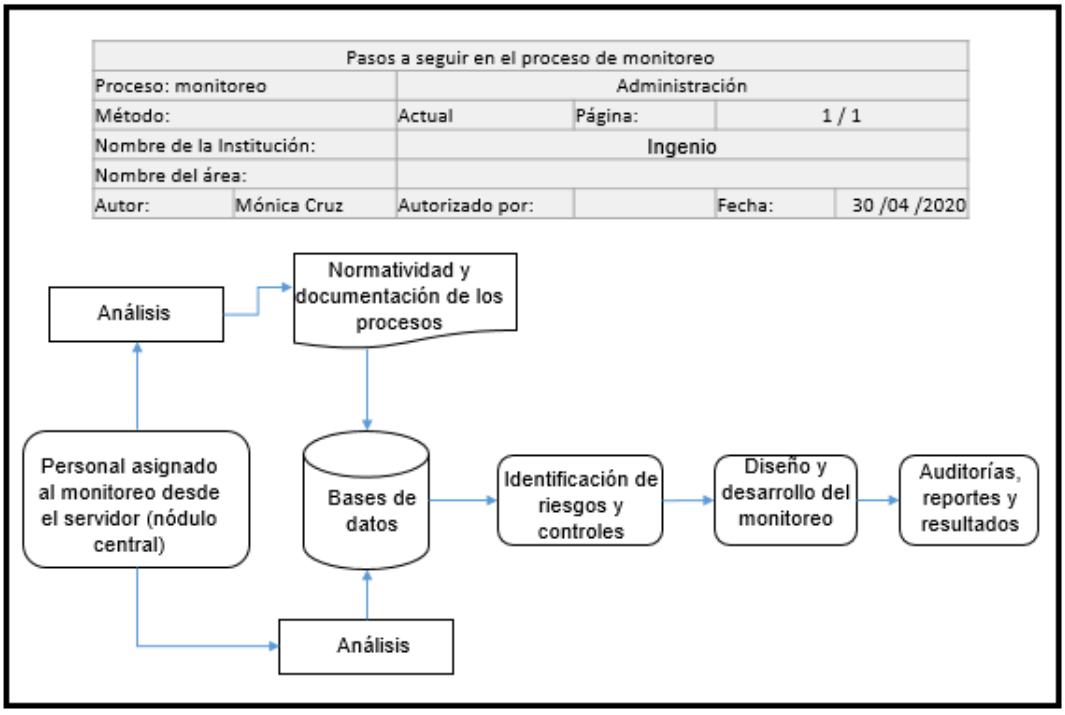
Acuerdos sobre confidencialidad	Se deberán programar revisiones sobre la existencia o diseño de cláusulas de confidencialidad por cada colaborador con contratos vigentes. La necesidad de los acuerdos deberá ser valorada en equipo multidisciplinario de acuerdo a los niveles de acceso a información clasificada por perfil y usuario asignado.	En los contratos vigentes y contratos futuros de contratación será adicionada la cláusula de confidencialidad definida por las autoridades del Ingenio.
Retiro de los derechos de acceso	La Norma sugiere establecer en el procedimiento de Gestión de cuentas de usuario la eliminación de derechos de acceso inmediatos. Se deberá tramitar con herramientas internas del servidor desde el departamento de informática. Se deberá realizar la verificación previa al departamento de recursos humanos y con el jefe del departamento de donde proviene la solicitud.	Dentro del servidor se podrá ejecutar esta acción, eliminando todo registro activo, acceso y permisos. Se deberán guardar los registros históricos sobre la bitácora de la interacción en el servidor desde que fue contratado hasta que fue dado de baja.

Fuente: ALARCÓN ÁVILA, Rodrigo. *Implementación de un modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos.* http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2694/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y. Consulta: 22 de mayo de 2021.

3.2.3. Procesos de monitoreo

Se podrá centralizar la información en el departamento de informática, se asignará personal capacitado del departamento de seguridad para acompañar las acciones preventivas constantemente. El proceso se diseña según los alcances esperados al ser implementado el uso de un nuevo servidor interno.

Figura 30. **Proceso de monitoreo**



Fuente: elaboración propia, empleando Visio 2016.

Realizar el monitoreo es parte fundamental de la prevención en incidentes y brechas de seguridad, las alertas deberán ser programadas desde la parte interna del servidor, la programación será fundamental para destacar cuales

podrán ser las actividades que hacia la empresa representen acciones graves que comprometen información crítica o procesos de producción.

3.2.4. Tecnología para implementar

La tecnología será complementada por el servidor Sum Server, los protocolos de monitoreo, el plan de contingencia y todos los procesos establecidos con la propuesta de la Norma ISO 27001.

Con el uso de nueva tecnología incurrirán nuevos retos y nuevos desafíos. El personal deberá ser capacitado previamente al incorporar las herramientas tecnológicas y administrativas para el resguardo de información, el departamento de recursos humanos se fortalecerá con trabajo en equipo y apoyo del Departamento de Seguridad y de Informática.

La tecnología es compleja, estandarizar los procesos de accesos, creación de usuarios, manejo de contraseñas, editar el rol según el perfil para cada colaborador es tarea extensa, por eso en el transcurso de la propuesta idóneamente se considera trabajar en mesas multisectoriales incorporando a cada jefe y supervisores de los departamentos de incidencia para que en conjunto logren diseñar los protocolos, accesos, criterios de evaluación, modelos y patrones de conducta dentro del nuevo recursos tecnológico.

A este nuevo recurso se deberá incorporar programas de seguridad informática, buses periféricos físicos que permitan reducir accesos inoportunos sin autorización, la información nuevamente se plantea como el recurso invaluable para el Ingenio, por lo cual deberá ser respaldada 24/7, el personal mejorara exponencialmente la experiencia en el uso de estas herramientas, las tareas asignadas les serán menos dificultosas de poder realizarlas.

3.2.5. Capacitación de personal

Previo a diseñar el plan de capacitación se trabajó con la detección de necesidades, no se ejecutó algún sistema de evaluación por que el programa a implementar será nuevo, al igual que la interfaz del usuario y todo lo relacionado a los accesos, resguardo y navegación dentro del sistema. Para la propuesta se empleó el ciclo de la capacitación.

Figura 31. **Ciclo de la capacitación**

Fuente: CHIAVENATO, Idalberto. *Administración de recursos humanos.* p. 369.

Se hace acá una pausa, para indicar que el presente trabajo de graduación es una propuesta, dentro del ciclo de capacitación se ejecutan los pasos 1 y 2, como parte de la propuesta quedará en total discreción del Ingenio adquirir el

Servidor, así como el Software he incorporar todos los procesos diseñados. El proceso 3 y 4 no tendrá participación en el desarrollo de la tesis.

Para la estructura del plan de capacitación se considera una breve introducción sobre el software, manejo de los usuarios, protocolos de monitoreo y supervisión para que el recurso humano tenga sobre aviso que son constantemente monitoreados, gestión de cuentas, gestión de usuarios, consultas al sistema y operaciones dentro del sistema, se les realizará la plática introductoria con una persona del Departamento de Seguridad, una persona representante de recursos humanos y un representante del Departamento de Informática.

Tabla XVI. **Estructura del plan de capacitación**

TEMA	DURACIÓN	MODALIDAD	FACILITADOR
Introducción	1 hora	Presencial	Recursos humanos
Descripción de módulos	1 hora	Presencial	Informática
Inicio de sesión	1 hora	Presencial	Proveedor de servicios
Gestión de cuentas	30 minutos	Presencial	Proveedor de servicios
Gestión de usuarios	30 minutos	Presencial	Proveedor de servicios
Operaciones del sistema	1 hora y 30 minutos	Presencial	Proveedor de servicios
Consultas del sistema	1 hora y 30 minutos	Presencial	Informática
Gestor administración	1 hora y 30 minutos	Presencial	Informática

Fuente: elaboración propia.

El proveedor de servicios formará parte de la capacitación, son quienes deberán preparar al recurso humano a poder crear sus usuarios, indicar cuales son los parámetros para las contraseñas, introducirlos al manejo y uso de los nuevos programas, todos esto en trabajo con recursos humanos e informática.

3.3. Mejora de comunicación

La comunicación podrá realizarse eficientemente, sustituyendo los protocolos que implementaban con anterioridad donde se presentaban retrasos, perdidas de datos y control de tareas. Los supervisores velaran por el adecuado uso he implementación de las nuevas tecnologías dando paso a reducir los tiempos en que se pueda enviar un conjunto de acciones hacia diferentes usuarios con la finalidad de procesar con las indicaciones especificas asignadas.

Los usuarios trabajarán en línea en todo momento, eso permite que los supervisores junto al personal de seguridad informática puedan observar en tiempo en vivo todas las actividades que se están desarrollando, implementar los protocolos dentro del sistema cuando un usuario deja más de 4 minutos de inactividad es otro punto crítico que podría mejorar los resultados en la comunicación entre el usuario final, los supervisores y los analistas de riesgo.

Los datos recabados a cada minuto sirven para analizar la producción, los correos internos por problemas informáticos serán trasladados con mayor eficiencia, las quejas por bajo rendimiento podrán ser redactadas casi a diario, la medición dentro del propio clima organizacional podrá ser ejecutado al concluir cada jornada. De esta forma se podrá mejorar el medio de comunicación interna entre los usuarios finales como una sociedad única, entre los usuarios finales y sus supervisores para aclarar dudas en las tareas asignadas y entre los jefes de área con sus supervisores y sus usuarios finales asignados.

3.3.1. Resumen ejecutivo de problemas continuos

Para los supervisores será importante emplear el modelo homogéneo para presentar este tipo de resumen, que sea corto, claro, breve y conciso, deberá incluir aspectos relevantes asociados al problema que se presentó y cuáles fueron las acciones correctivas incorporadas.

Tabla XVII. **Estructura y modelo del resumen ejecutivo por problemas**

Contenidos	Resumen
Se definirá cuáles fueron los problemas que se presentaron, se clasificará por nivel de agresión en fallas y cuáles fueron los medios utilizados para su corrección.	Se deberá presentar la investigación realizada con los pasos seguidos hacia el problema que se presentó, se deberá incorporar cuales fueron los alcances dentro de la investigación del problema, quienes fueron los responsables y la consignación de los usuarios pertinentes.
Nivel de agresión o peligrosidad	Opinión personal
Indicar cuales fueron los sectores afectados, cual fue el nivel de profundidad de la falla, los posibles motivos y sujetos que dieron pauta a que existiera el evento. Si podrían existir asociados externos a la empresa o si la brecha se dio en algún dispositivo periférico.	Redactar con palabras personales cuales fueron los resultados obtenidos luego de realizar la exploración, evaluación y tareas de contingencia, dejar en todo momento algún análisis que mejore la situación y prevé el mismo evento a futuro.
Mensajes relevantes	Conclusiones
Destacar dentro de este informe si se presentaron alarmas previas a existir el evento o si el personal de seguridad paso por alto el protocolo de respaldo y supervisión continua.	Emitir las conclusiones con juicios técnicos sin comprometer al usuario por malas relaciones interpersonales dentro del trabajo.

Fuente: elaboración propia.

3.3.2. Revisión de documentación

La documentación previa a ser aprobada deberá ser sometida a diversos filtros de aceptación, cada supervisor redactará las peticiones necesarias acorde a las necesidades que se presenten en su grupo de trabajo, el recurso humano de forma independiente emitirá sus peticiones a cada supervisor de área.

El conjunto de supervisores asignados deberá analizar los documentos que fueron redactados por los colaboradores de bajo rango, esperando encontrar información relevante acorde a los puestos asignados. Se descartarán solicitudes que no puedan cubrir el rango de jerarquía dentro de la empresa. Estos documentos luego de ser evaluados por los supervisores trasladarán la información sintetizada a sus jefes de área, quienes la emitirán y transformarán en índices de producción a los altos mandos o Junta Directiva.

Dentro del proceso de revisión de documentos se deberán identificar las necesidades de actuación de los documentos internos al proceso de esa forma los supervisores informarán a sus jefes de los procesos. La actualización es asociada a la creación, modificación y anulación de documentos.

Se deberá asignar un supervisor responsable por cada 5 colaboradores de elaborar la propuesta o modificación de los documentos internos. Cada propuesta será realizada conforme las normas y reglamentos internos, se presentará dentro de la Web interna al correo institucional del supervisor asignado donde se citará la totalidad de los cambios realizados. La revisión técnica deberá disponer de temporalidad y vigencia desde su ingreso, revisión, informe de resultados y divulgación de los mismo con un tiempo no mayor a 2 horas por cada caso ingresado.

3.3.3. Correo de notificación de incidencias

Esta acción se incorpora desde el Servidor, empleando la Web interna se deberán enviar los correos necesarios ante cualquier eventualidad, no solamente cuando se presenta algún problema o evento que detenga las operaciones dentro de las oficinas administrativas. El correo emitido deberá llevar copia a los destinatarios dentro de su jerarquía de trabajo. Cada colaborador en la dirección de correos indicará cual es el asunto que promueve la necesidad de enviar el mismo, e incorpora la dirección de su supervisor inmediato y jefe de área.

3.3.4. Informes estandarizados

Para cada informe se deberán incorporar datos y aspectos relevantes donde se pueda demostrar e identificar cual es el área de trabajo asignada y cuáles fueron las tareas programadas. Dentro de este informe se puede colocar la jornada de trabajo y quien es su supervisor inmediato.

Tabla XVIII. **Estructura del informe estandarizado**

Nombre completo		Código interno o usuario
Fecha:	Puesto asignado:	Hoja _/_
Supervisor	Recibido por:	
Descripción de las tareas:		
Alcances y resultados obtenidos:		
Notas especiales:		

Fuente: elaboración propia.

3.3.5. Manual de comunicación de informes

El manual de comunicación interna y externa tendrá como fin el lograr estructurar el sistema de comunicación estandarizado para el Ingenio, reduciendo así el cruce de información, emisión de información innecesaria, aprovechamiento del tiempo de trabajo y el rendimiento de los colaboradores.

El desarrollo y compromiso del manual de comunicación exige la participación de los supervisores, jefes de área y de todo su recurso humano. Luego del diseño estará bajo responsabilidad del departamento de recursos humanos e informática de llegar a implementarlo, antes de ser implementado se deberá otorgar la capacitación necesaria para poder familiarizar a los usuarios.

Se deberán incorporar aspectos cotidianos del clima organizacional, comunicación interna actual entre cada trabajador y sus supervisores y por cada supervisor con su jefe inmediato. Los informes son piezas fundamentales en el avance en medición de resultados de los procesos establecidos acorde a la programación diaria, semanal, mensual, trimestral y semestral.

La propuesta del manual de comunicación deberá incluir componentes relevantes que solamente la empresa conoce y tienen conocimiento del desempeño en cada área de interés. Por eso se indicarán solamente y como pueden incorporarse al ser previamente aceptados para su ejecución.

Tabla XIX. **Componentes del manual de comunicación**

Componente	Descripción y alcance
Situación	Se deberá identificar con los jefes de área cual sería la secuencia lógica que mejoraría el desempeño de la comunicación actual, se debe incorporar el diseño único desarrollado por ellos mismos que contenga los aspectos relevantes que simplifiquen el documento que será enviado conteniendo la información deseada por cada informe.
Objetivo	Se deben definir los objetivos según lo que se desea lograr, incorporando una estrategia para cada objetivo.
Público	Se deberán definir los roles dentro del manual, donde se clasifique los alcances por rol o perfil. Si es colaborador de bajo rango sus permisos serán distintos a los de un supervisor, de la misma forma entre un supervisor y el jefe de área.
Estrategias	Por cada objetivo se diseñará una estrategia, es acá donde se prevé la necesidad de los representantes de las áreas de influencia para destacar un objetivo por cada representante. Así se esperaría diseñar el manual homogéneo que cumpla las necesidades de todos los sectores de interés.
Mensajes	Los mensajes que serán desarrollados en el manual deberán ser claros, de fácil comprensión sin palabras rebuscadas o textos complejos. Esto se empleará para acompañar las estrategias y cumplir con cada objetivo diseñado.
Tácticas	Serán las acciones debidamente detalladas que se diseñarán y llevarán a cabo para cumplir con el objetivo trazado.
Cronograma de incorporación	Las fechas serán proyectadas según las estrategias con sus tácticas planteadas. Se debe incorporar fecha de inicio y fin del mismo.
Presupuesto	La cuantificación será abordada por el tiempo empleado de los represented dejando detenidas las tareas ya asignadas, por lo que se presume duplicar la carga de trabajo para ellos y recurrirían en jornadas extendidas de trabajo representando costos de participación.
Evaluación	Luego de concluir la fase de diseño, análisis y pruebas, podrán ser evaluados resultados.

Fuente: elaboración propia.

El manual de comunicación futuro, podrá ser la expansión del modelo actual por el cual la empresa realiza estas acciones de enviar los informes. Se emplean herramientas digitales para el envío, hace falta incluir la estructura de dichos informes propuesto en la tabla XVIII. Así es como se espera incorporar el manual que beneficie relativamente el desempeño del trabajo de los colaboradores.

3.4. Manual de accesos

Para el uso del servidor SUM Server se propone incorporar el manual del usuario del fabricante. Este mismo describe que dentro del sistema de acciones de la aplicación para la gestión de usuarios será necesario incorporar una plataforma digital de preferencia GEXTEL.

Tabla XX. **Descripción de las actividades del manual de accesos**

Sección de interés	**Acción**	**Descripción**
Servidor	Acceso al sistema de gestión de usuarios	Se deberá acceder al menú principal desde el sistema corporativo con la previa identificación dentro del sistema. Luego de ingresar se podrá visualizar la aplicación de gestión de usuarios.
	Gestión de usuarios	Dentro de la aplicación permite a los administradores gestionar los usuarios dentro del sistema con la distinción que solamente pueden acceder a los usuarios relacionados a su departamento de trabajo. Se pueden realizar las siguientes gestiones: • Alta de nuevos usuarios • Baja de usuarios • Asignación de perfiles predefinidos a usuarios. • Bloqueo/desbloqueo de usuarios. • Cambiar contraseña de usuario. • Consultar permisos de portafirmas. • Visualizar permisos de usuarios.

Continuación de la tabla XX.

Acciones diferidas	Alta usuarios nuevos	Por medio de esta acción se permitirá crear el usuario previamente incluido del domino de red. Luego de ser reconocido el usuario, se procederá a incluir la contraseña de aplicación. Al aceptar el alta del usuario podrá aparecer en la lista de peticiones con tarea en estado pendiente.
	Baja de usuarios	Con la interfaz del software podrá realizarse fácilmente, será necesario seleccionar en la lista de usuarios existentes el usuario para el cual se desea tramitar la baja y pulsar el botón eliminar usuario. Previo a dar de baja a un usuario, se deberán contar con los permisos físicos en carta membretada y firmas originales de los jefes de áreas interesados, se recomienda que la carta de solicitud de baja de usuario deba ir firmada por el jefe del departamento de recursos humanos con la justificación de quienes solicitaron el proceso deseado.
	Asignación de perfiles a usuarios	La acción para asignar perfiles a cada usuario, permitirá asigna el perfil por cada usuario, reasignar perfiles y añadir permisos especiales a usuarios existentes. Se deberán diferenciar dos tipos de perfiles; perfiles que contengan permisos básicos por cada departamento y perfiles especiales que contengan permisos especiales a los usuarios existentes, estos permisos especiales podrán ser asignados a los supervisores y sobre ellos asignar permisos especiales a los jefes superiores. Para asignar perfiles por cada usuario, será necesario seleccionar por separado cada usuario, seleccionándolo desde la lista de usuarios en el servidor. Luego de ser seleccionado se deberá seleccionar el perfil que se desea asignar, luego de ser seleccionado el perfil en el cuadro de la descripción del perfil aparecerá todas las características del perfil seleccionado.

Continuación de la tabla XX.

Acciones *on line*	Bloqueo / desbloqueo de usuarios	Para bloquear un usuario desde el servidor se deberá seleccionar dentro de la sección de usuarios existentes y pulsar el botón bloquear usuario. Aparecerá el recuadro de confirmación presionando la pestaña de aceptar. Luego de bloquear al usuario no le será permitido acceder a las aplicaciones a las cuales tenia permisos. Para desbloquear un usuario se deberá seleccionar dentro del conjunto de usuarios existentes, se deberá seleccionar y pulsar la pestaña desbloquear usuario. Previo a ser desbloqueado aparecerá una alarma de aceptación o cancelación, al pulsar aceptar se dará por concluido el proceso de reincorporación del usuario con sus permisos específicos.
	Cambio de contraseñas	Para esta acción se deberá solicitar permiso al técnico de informática, quien ingresará a seleccionar el usuario que desea cambiar su contraseña, luego presionará la pestaña de cambio de contraseña, al elegir esta opción aparecerá en la pantalla el usuario indicado y los campos de nueva contraseña con el espacio de repetir contraseña y la confirmación de la misma.
	Permisos portafirmas	Podrá ser ejecutado con la selección de cada usuario que se desea asignar permisos dentro del cuadro de usuarios existentes y pulsando el botón de permisos de portafirmas.
	Permisos grupos	Con la implementación de esta herramienta, se podrá conocer al momento cada permiso o grupo asignado por cada usuario.
	Consulta descripción de perfil	Se podrá conocer la característica de cada perfil, será necesario seleccionar el perfil deseado y aparecerá la descripción dentro del recuadro de descripción de perfil, su contenido se visualizará en el recuadro de permisos que otorga el perfil en el que mostrará la lista de grupos asociados a ese perfil.

Fuente: MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y. Consulta: 15 de mayo de 2021.

Con la implementación del manual de accesos se podrán diversificar las herramientas tecnológicas y de trabajo, se podrán reducir tiempos en ejecución y programación de tareas según los perfiles de los usuarios.

3.4.1. Informes estandarizados

Estos informes deberán incluir información clara, objetiva y directa, donde se demuestren porque se autorizaron los diferentes accesos en un determinado tiempo.

Tabla XXI. **Informes estandarizados para el control de accesos**

Nombre completo		Código interno o usuario
Fecha:	Puesto asignado:	Hoja _/_
Supervisor	Recibido por:	
Descripción de las tareas:		
Alcances y resultados obtenidos:		
Notas especiales:		

Fuente: elaboración propia.

3.4.2. Tipos de controles

Los controles asociados al manual de accesos también deberán estar constituidos dentro de la propuesta del uso de la Norma ISO 27001. Estos tipos de controles serán de prevención y reacción ante la vulnerabilidad o presentarse alguna brecha que exponga información crítica de la empresa. Se deberán robustecer los controles en el manejo de permisos y credenciales de autoridad,

los propios jefes de áreas deberán ser monitoreados para evitar que actúen con falta de ética y responsabilidad ante el cargo representado.

Figura 32. **Resumen de controles a incorporar según la Norma ISO 27001**

Fuente: elaboración propia.

3.4.3. Plan de manejo de la administración de controles y protocolos

Su importancia se fundamentará en la necesidad de monitorear permanentemente la gestión relacionada a la gestión del riesgo, eventualmente

se proyecta la efectividad de los controles diseñados y mejorando los establecidos. Se tendrá en cuenta que cualquier miembro dentro de la empresa estará expuesto constantemente a ser corrompido para extraer información crítica o exponer ciertos documentos o procesos internos que destaquen de la competencia. Este tipo de actividad es difícil de detectar por lo cual se deberán atender lineamientos y actividades esenciales que permitan administrar eficientemente los controles con sus gestiones diseñadas.

Tabla XXII. **Esquema del plan de manejo de la administración**

Acción con precedencia
Se deberá analizar el nivel de riesgo residual y definir el tratamiento a implementar con la ejecución de los controles preventivos ya descritos y los seguimientos continuos en brechas internas, será necesario generar un reporte que consolide la información que destaco en el proceso de gestión del riesgo.

Se deberá iniciar el registro del riesgo identificado, luego se deberá especificar el tipo y clase de riesgo, se procederá a transcribir la causa raíz o causa priorizada, así como el nivel de probabilidad e impacto quedado luego de valorar los controles que determinaron el riesgo residual.

Luego de la fase de determinación del riesgo, se deberá analizar qué tipo de estrategias de supervisión se implementarán, esto para contrarrestar las causas raíz para colocarlas en las actividades de control de los formatos y sobre su contenido se pueda establecer la opción viable del tratamiento correspondiente.

Se procederá a relacionar el soporte por el cual se evidenciará el cumplimiento de cada actividad, se consignará quien fue el responsable de implementar este proceso de control relacionando el cargo y el usuario, se consignará el tiempo empleado en el que se cumplió la actividad y la periodicidad de ejecución.

Continuación de la tabla XXII.


Al concluir las actividades de control establecidas para reaccionar a las causas de riesgo, se deberá relacionar la acción de contingencia a ser implementada, pero esto se deberá analizar las estrategias que mitiguen las disrupciones o brechas de seguridad. Se deberán seleccionar las estrategias que comprometan o empleen el menor tiempo de reacción.

En la última fase del plan se deberán formular los indicadores de riesgo que participaron en el evento, esto con la finalidad de medir el impacto de las actividades y protocolos de control, se estudiaran cada una de las acciones implementadas en este proceso del plan de manejo de la administración.

Fuente: elaboración propia.

El complemento de este plan de manejo se verá influenciado y proyectado por las acciones previstas por el Ingenio, se deberán mejorar o robustecer las existentes, la plataforma ideal es en función a los manuales y programas de organización ya previstos, el departamento de recursos humanos con la gestión de administración será trabajo por los sectores que conforman la estructura organizacional en las oficinas administrativas, dentro de este organigrama se emplearan la jerarquía de atributos y puestos. Por cada departamento será esencial que proponga información que pueda eficientizar las acciones de trabajo del departamento de informática sobre aspectos internos del manejo y operación de la información, las tareas preventivas deberán destacar en todo momento de la mano con el monitoreo y la supervisión de los usuarios y perfiles de trabajo.

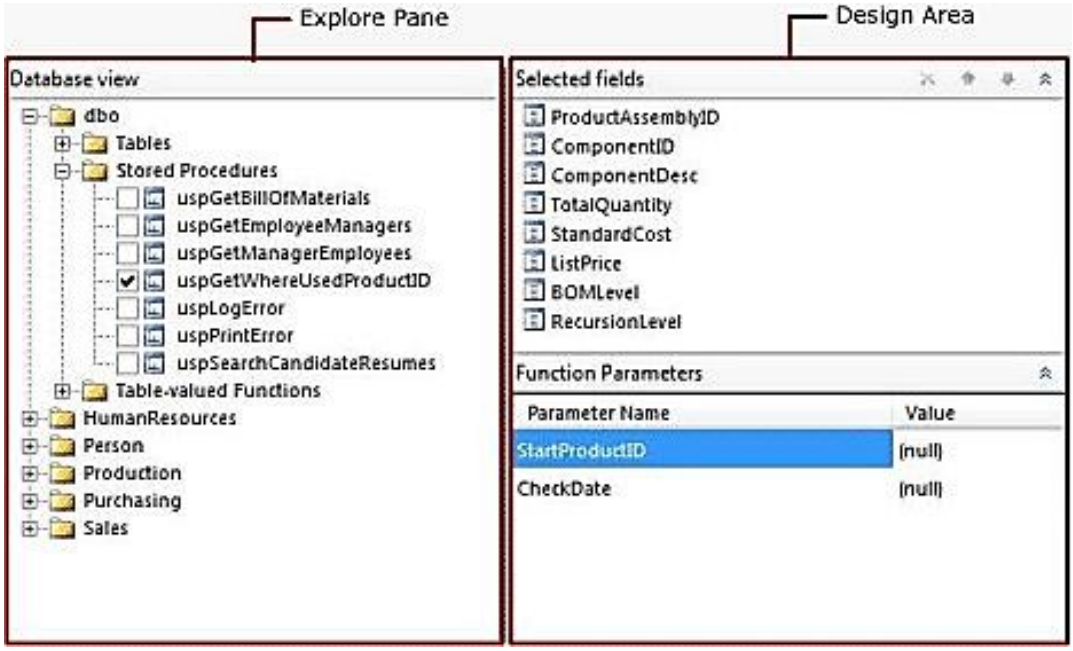
3.4.4. Definición de accesos

Los accesos serán definidos por el tipo de rol y usuario para el departamento donde se consignarán a trabajar. Por cada usuario será definido un único acceso tal y como lo establece la Norma ISO 27001 y el manejo de información según el servidor SUM Server.

3.4.5. Manual de bloqueos de desbloqueos de usuario

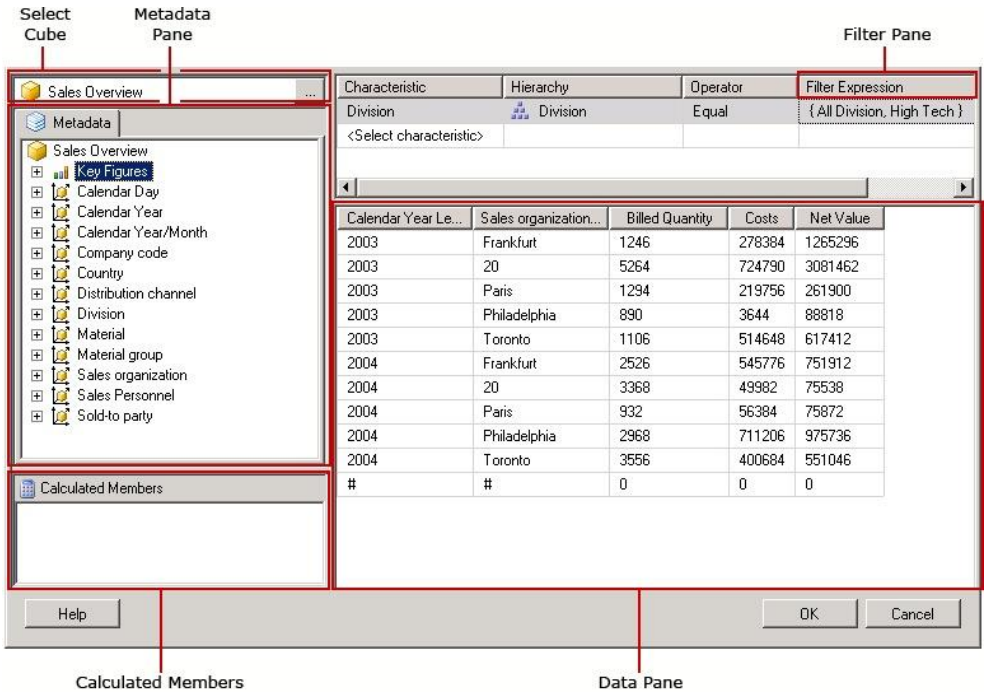
Parte de estas acciones están descritas en la tabla XX dentro de las acciones *on line* incorporadas a las actividades del manual de accesos.

Figura 33. **Interfaz de bloqueo de usuario**



Fuente: Microsoft. *Tipo de comando Text*. https://docs.microsoft.com/es-es/sql/reporting-services/report-data/graphical-query-designer-user-interface?view=sql-server-ver15. Consulta: 15 de agosto de 2020.

Figura 34. **Interfaz de desbloqueo de usuario**



Fuente: Microsoft. *Tipo de comando Text*. https://docs.microsoft.com/es-es/sql/reporting-services/report-data/graphical-query-designer-user-interface?view=sql-server-ver15. Consulta: 15 de agosto de 2020.

Para el bloqueo del usuario se seleccionarán una serie de pasos sencillos, dentro del servidor se encontrará esta acción, el detalle completo esta ya descrito en la tabla XX.

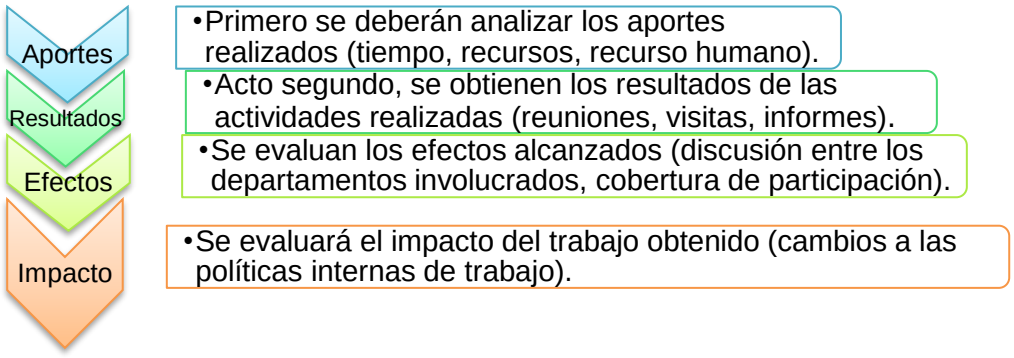
3.5. Plan de incidencias

El plan de incidencia es conocido como una serie de componentes o pasos que permitan contribuir a precisar y definir cada problema, objetivo, acciones y recursos necesarios que permitan en conjunto promover el cambio en las políticas internas.

En la parte administrativa del Ingenio deberán ser discutidos diferentes temas relacionados a la gestión administrativa y los ciclos de planificación. Estando ya comprometidos con esos temas se podrá proceder a diñar el plan de incidencia que incorpore los aspectos importantes de cada departamento que puede comprometer la seguridad laboral visto de diferentes ángulos, el primero es mitigar y reaccionar ante la presente brecha y fuga de información, el segundo resguardar la integridad física de todos los colaboradores. Para los análisis futuros se considerarán las actividades de incidencia requerirán disposición de personal capacitado.

Se considera que la ejecución de las tareas de monitorio y las evaluaciones del impacto obtenido en la incidencia de manera frecuente es algo difícil de predecir, sin los debidos protocolos de monitoreo es difícil darse cuenta de alguna ocurrencia o evento que vulnere la seguridad interna. Las tareas de incidencias serán realizadas por alianzas interdepartamentales. Con la distribución de estas tareas será un poco complejo medir la efectividad de cada departamento, pero siempre deberán mantener cierto límite de eficiencia.

Figura 35. **Niveles estimados de participación segmento por fases de monitoreo y evaluación**



Fuente: elaboración propia.

Tabla XXIII. **Matriz del plan de incidencias**

Objetivos	Actividades	Objeto	Indicadores	Plazo	Responsable	Revisión
Monitoreo de usuarios conectados.	Validar que los usuarios se encuentren conectados	Valoración del tiempo efectivo de trabajo	Producción estimada según proyecciones	Lo necesario según la proyección	Supervisor de informática o supervisor por área	Jefe de área
Monitoreo de ingresos en horarios establecidos	Validar los accesos al sistema	Reportar los accesos tardíos	Jornadas de trabajo, menos tiempo efectivo de trabajo	Justo en el horario de ingreso de los colaboradores	Supervisor de área asignado	Jefe de área
Concordancia de accesos según programas de cómputo asignados.	Monitorear que los colaboradores utilicen exclusivamente los programas necesarios para realizar el trabajo y tareas asignadas.	Medir la eficiencia en el trabajo y el tiempo efectivo de interacción.	Tiempo efectivo laborado, eficiencia por tareas asignadas, cumplimiento y rendimiento de metas.	Podría asignarse de manera permanente con resumen semanal, mensual, trimestral y semestral.	Supervisor de área asignado	Jefe de área
Uso y ejecución de tareas según programación.	Monitorear el cumplimiento de las metas	Medir el desarrollo del trabajo realizado por los colaboradores	Tiempo efectivo laborado, eficiencia por tareas asignadas, cumplimiento y rendimiento de metas.	Diario	Supervisor de área asignado	Jefe de área
Uso de equipos de cómputo y equipos periféricos asignados.	Monitorear que los colaboradores no hagan uso de otros equipos	Obtener métricas de traslado internos no permitidos al recurso humano.	Cumplimientos de tareas asignadas.	Diario	Supervisor de área asignado	Jefe de área

Continuación de la tabla XXIII.

Ingresos al sistema interno para crear copias en dispositivos móviles.	Monitorear fugas de información y copias no autorizadas	Establecer quienes podrían actuar de forma negativa y peligrosa hacia el Ingenio	Nivel de seguridad y resguardo de información confidencial	Diario y constante	Supervisor de área asignado	Jefe de área
Control de accesos remotos desde otro equipo no asignado.	Monitorear fuga de información y copias no autorizadas	Monitorear que personal podría representar amenazas al Ingenio	Nivel de seguridad y resguardo de información confidencial	Diario y constante	Supervisor de área asignado.	Jefe de área

Fuente: elaboración propia.

La matriz propuesta pretende cubrir los aspectos relevantes del Ingenio, en materia de prevención y ejecución de protocolos que garanticen la seguridad informática. No será importante únicamente la seguridad informática, se proyecta que con el empleo del plan de incidencias se obtengan indicadores de eficiencia y calidad, monitoreando constantemente a todo su recurso humano con el aprovechamiento del servidor para garantizar que se encuentren en su puesto de trabajo conectados a la red y trabajando en las tareas que les fueron asignadas.

3.5.1. Procedimiento de documentación de las incidencias

Los incidentes serán registrados y documentados por el personal de informática, con cada evento se creará el archivo histórico contemplando la zona de ocurrencia o el departamento donde fue localizado, por el medio de automatización al emplear nuevo recurso digital se podrá establecer cuál fue el usuario que origino el error o si fue error informático en cierto punto de red. Se

deberá consignar la hora y fecha del evento, agregando cuales fueron los efectos primarios en daños obtenidos o daños colaterales luego de que se presentara esa falla.

Tabla XXIV. **Procedimiento para documentar una incidencia**

Acción	Descripción
Obtener los datos del usuario afectado	Anotar el nombre completo del colaborador que presento el problema con su código de usuario, ubicación, email interno y número de teléfono.
Identificar el IP o equipo	Dentro del sistema obtener la dirección IP o nombre del PC asignado, esos datos serán necesarios para de que equipo se está analizando el problema. Diferenciar los equipos periféricos, anotando si el problema es por una impresora o fotocopiadora.
Evaluar si el equipo pertenece a la red interna	Definir si el equipo se encuentra agregado a la red o si esta fuera del dominio de red y trabaja a través de la conexión a internet. Describir si ese equipo que fue reportado posee red a internet en el caso de ser un factor importante. Anotar si posee conexión VPN.
Describir el problema claramente	Se deberá realizar la descripción detallada del problema. Se deberá anotar los pasos que el usuario reprodujo hasta el momento que se presentará el error.
Añadir captura de pantalla al informe	Capturar una imagen y agregarla al reporte para complementar el reporte de incidencia.
Evaluar si es el único afectado	Medir el alcance del problema por el cual se definirá y condicionará la posible solución que deberá ser aplicada. Delimitar si el problema que se presentó es en una sola computadora o podría estar afectando a otros compañeros dentro de la oficina.
Preguntar si ha realizado cambios importantes a su computadora	Se deberá preguntar al usuario que reporto el incidente si ha instalado algún nuevo programa o realizado algún cambio en la configuración en los últimos días, eso podría ser útil para identificar los orígenes del problema que se presentó.
Comparar con el historial de reportes o eventos ocurridos	Se deberá consultar sobre eventos anteriores y ocurrencias que podrían haber determinado las posibles causas de las ocurrencias sobre incidencias.
Preguntar cuáles han sido las pruebas realizadas últimamente	Se deberá indicar cuales fueron las pruebas que ha realizado el usuario. Serán datos relevantes que ayuden a identificar y acotar los problemas o el problema que se haya presentado.

Fuente: elandroide. *9 claves para documentar correctamente una incidencia.* https://elandroidefeliz.com/9-claves-para-documentar-correctamente-una-incidencia-informatica/. Consulta: 6 de julio de 2021.

La documentación será incorporada a un sector especial dentro del nuevo servidor que garantice que la información es debidamente resguardada y podrá ser empleada nuevamente a futuro

3.5.2. Controles para evitar incidencias

Para el sector informático es basto y extenso desarrollar las estrategias infinitas que permitan accionar por medio de controles estandarizados que permitan mitigar y evitar incidencias. El Ingenio trabaja con plataforma ya establecida sobre protocolos que garanticen la seguridad, resguardo y respaldo de la información sensible que comprometería a la empresa con su entorno al sustraer archivos.

Los controles permitirán fortalecer las acciones ya implementadas que posiblemente se dupliquen y deban ser descartadas, se presume que al proponer el conjunto de acciones marcando los puntos débiles o los aspectos relevantes permitirá mejorar cada nivel de seguridad y la eficiencia del personal a cargo de esta tarea, las tareas relevantes de controles y vigilancia se ha descrito y establecido hacia el departamento de informática, pero será el trabajo en equipo de los supervisores de área con el monitoreo sobre el trabajo que se pueda desarrollar constantemente donde se plantee la primer barrera de seguridad hacia el recurso humano, no solamente pueden ocurrir incidencias humanos, podrán presentarse eventualmente problemas con equipos de cómputo o problemas internos dentro de la propia red de trabajo.

Tabla XXV. **Conjunto de controles que podrían reducir el evento de una incidencia**

Tipo de control	Acción recomendada para implementar el control
Controles básicos	Actualizar el inventario de todos los dispositivos incluso los periféricos que fueron autorizados y no autorizados.
	Actualizar el inventario del Software que fue autorizado y o el Software que fue sometido a actualizaciones y el Software que dejo de ser autorizado.
	Crear la gestión de monitoreo continuo sobre las posibles vulnerabilidades.
	Monitoreo de los privilegios sobre los administradores de cada área o departamento.
	Diseñar la modelo de configuración segura e encriptada del hardware y software en los equipos de cómputo, computadoras portátiles, equipos periféricos y dispositivos móviles.
	Monitoreo de las actividades de mantenimiento, establecer el análisis sobre las acciones de logeo utilizando las auditorías internas.
Controles fundacionales	Se deberá diseñar el modelo de protección para el correo electrónico interno y de la misma forma fortalecer el programa de seguridad en el navegador Web interno.
	Contratar o comprar software de tipo malware.
	Diseñar el control y limitación de los puertos de red, implementar los protocolos y servicios establecidos en la Norma ISO 27001.
	Fortalecer en el departamento informático la capacidad de obtener la recuperación de datos.
	Establecer configuración segura de los equipos de cómputo, equipos periféricos y equipos de red, empleando conmutadores, enrutadores y cortafuegos.
	Implementar la defensa de tipo borde.
	Monitorear constantemente la protección de datos críticos.
	Restringir y configurar el control hacia los accesos basado en necesidades de conocer el perfil y rol del usuario.
	Implementar el control de accesos ejecutando protocolos inalámbricos, donde se deberá establecer mayor nivel de criticidad por la exposición constante hacia afuera de las instalaciones.
	Mantener constantemente el control y monitoreo de las cuentas de todos los colaboradores sin distinción de nivel participativo en cada departamento.

Continuación de la tabla XXV.

Controles organizacionales	Se podrá implementar el programa de concientización y modelo de capacitación continua en niveles de seguridad informática.
	Implementar herramientas y protocolos de seguridad del Software raíz de aplicación incorporado al servidor.
	Gestionar el protocolo de respuesta y gestión inmediato ante la presencia de cualquier incidente.
	Realizar pruebas de penetración según el diseño planteado, ejecutar y replicar los ejercicios que permitan encontrar eventualmente brechas al sistema.

Fuente: elaboración propia.

Estos controles podrán fortalecer la gestión administrativa, permitirán proyectarse ante alguna incidencia o foco de sectores débiles en la ejecución de tareas diarias. El personal a cargo de ejecutar estas tareas deberá permanecer constantemente comprometido con su rol dentro de la organización, si la tarea es de monitoreo deberá desempeñar eficientemente su tarea, lo mismo sucederá con el personal de informática y el Departamento de seguridad, evitar incidentes será la clave central en la nueva gestión administrativa, con el compromiso de todos sus colaboradores.

3.5.3. Ciclo de Deming

Adaptado a las necesidades donde prevalecerá se seguridad informática, la prevención y minimización de brechas donde se pueda cometer algún delito hacia la empresa. Otro factor que destacará será el lograr incorporar hacia el Ingenio en sus oficinas administrativas el uso y adecuamiento del nuevo servidor con el Software que mejorara la rapidez con la que se ejecutarán las tareas y traslados de informes internos.

Figura 36. **Ciclo de Deming**

Fuente: elaboración propia.

3.5.4. Factores para prevención de incidencias dentro de la gestión administrativa

La gestión administrativa estará diseñada para programar la prevención, minimización de riesgos y mejora continua para lograr emigrar al uso he implementación de nuevos sistemas digitales, el Software que se prevé emplear mejorara sistemáticamente las operaciones cotidianas, el traslado de información y el intercambio de paquetes de datos que han sido monitoreados

constantemente. Para el Ingenio se podrán resumir un conjunto de factores con riesgo de incidentes a los cuales se les deberá prestar mucha atención.

Tabla XXVI. **Factores para prevención de incidencias dentro de la gestión administrativa**

Factor	Alcance y sector de prevención	Descripción
Procesos	El conjunto de eventos inter relacionados con los posibles errores hacia las actividades que deberán de realizarse el servidor del Ingenio.	Inexistencia de procedimientos estandarizados.
		Errores de autorización y errores de grabación.
		Errores internos de las auditorías y el envío de la información crítica.
		Inexistencia y falta de programas de capacitación con los temas relacionados a la interfaz del usuario con el nuevo Software.
Recurso humano	Salud y seguridad en el trabajo, analizando las posibles intenciones de robo o fraude.	Robo de activos de la oficina.
		Comportamiento anti ético de los colaboradores.
		Fraude interno (sustracción de información o dispositivos digitales con información de la empresa)
Recursos tecnológicos	Eventos que se podrán relacionar hacia la infraestructura tecnológica y la red interna.	Daño hacia el equipo de cómputo y equipos periféricos.
		Caída del Software y aplicaciones.
		Caída de red interna.
		Errores en los programas utilizados diariamente.
Daños hacia la infraestructura	Eventos que podrán ser relacionados hacia la infraestructura física del Ingenio.	Incendios.
		Derrames de líquidos.
		Sismos o temblores.
Eventos externos	Incidentes externos que podrían comprometer la seguridad interna.	Robos internos por propios colaboradores.
		Suplantación de usuario o de identidad.
		Vandalismo y atentados hacia las oficinas desde el exterior.

Fuente: elaboración propia.

Estos factores destacan dentro de un amplio panel que promoverían acciones de riesgo dentro y fuera de las oficinas del Ingenio, se presentaron las de mayor participación y relevancia que podrían propiciar la vulnerabilidad y riesgo hacia el control interno de la red y hacia la cultura organizacional de sus colaboradores.

3.6. Ciclo de vida de eventos de seguridad

El uso y empleo de herramientas tecnológicas expone en cierto grado la vulnerabilidad ante hechos delictivos o ciberdelitos que comprometen a cada empresa. Utilizar un servidor propio con aplicaciones diseñadas específicamente para el desarrollo de tareas específicas permitirá que se presenten servicios hacia la empresa enviando mensajes de eventos de seguridad. El departamento de seguridad y el departamento de Informática recibirán diariamente un sinfín de quejas, las quejas provienen de eventos que para los cortafuegos o los protocolos establecidos podrían representar alguna alerta o alarma, se podrán diferenciar los eventos surgidos dentro de la Web, problemas por mal interacción de los usuarios o acciones de sabotaje.

Figura 37. **Ciclo de vida de un evento de seguridad**

Fuente: TERUEL, Amneris. *El ciclo de vida de un evento de seguridad*. https://www.helpsystems.com/es/blog/el-ciclo-de-vida-de-un-evento-de-seguridad. Consulta: 15 de abril de 2021.

Se podrá adaptar este ciclo de vida hacia los eventos que puedan llegar a darse, los protocolos de prevención son robustos, las propuestas de intervención y proyección de las fuentes que podrán delimitar debilidades en el servidor, el uso del software y comportamiento de los colaboradores. Este ciclo se

comportará bajo los protocolos de prevención y reacción ante la vulnerabilidad del software o de alguna computadora y dispositivo periférico.

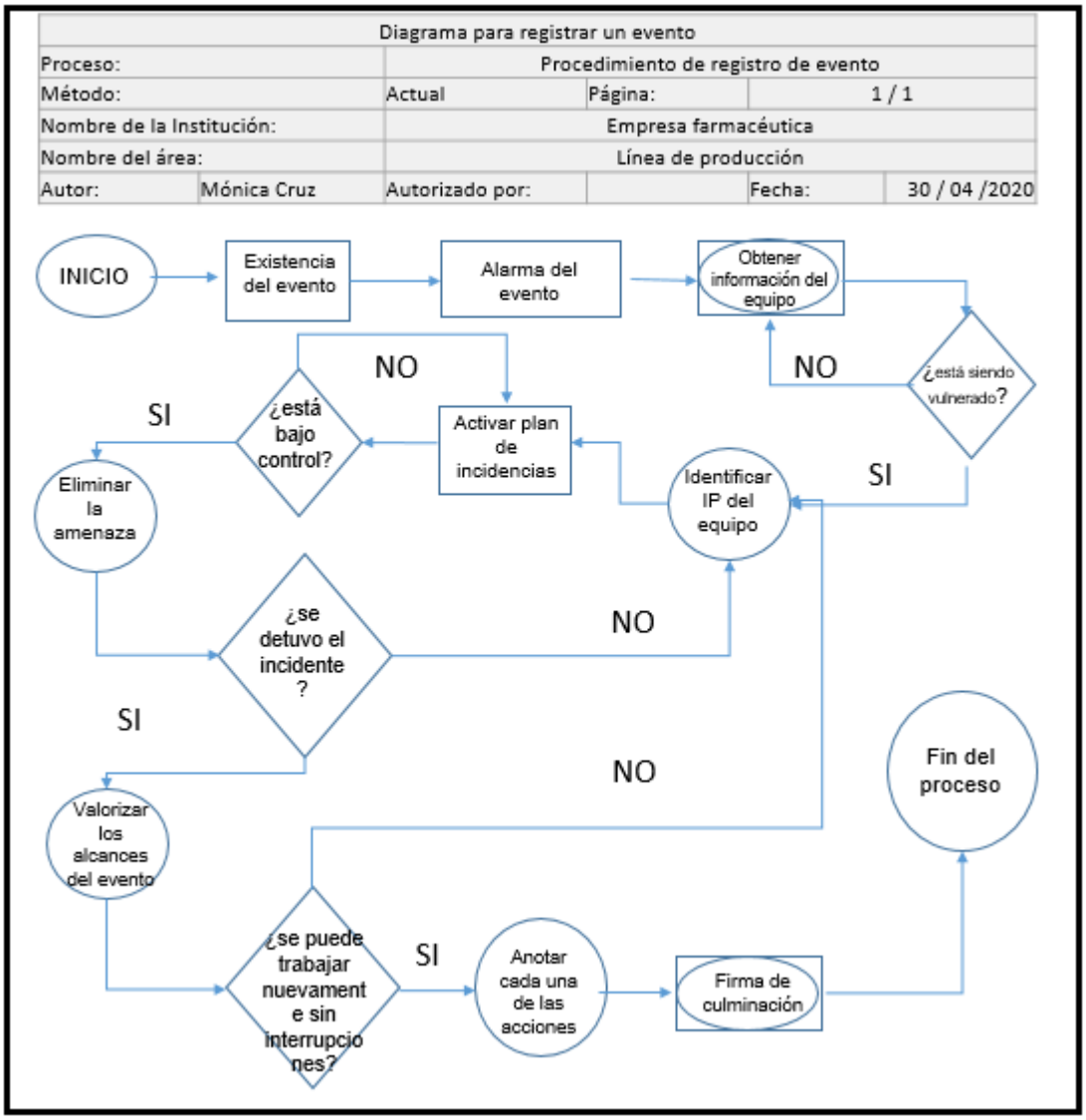
3.6.1. Detección del evento

El Software cortafuegos podrá marcar una alarma del evento encontrado, se trasladará un mensaje directo al supervisor asignado en el departamento de informática para que evalué el nivel de la brecha o el nivel de amenaza que está representando al servidor.

3.6.2. Procedimiento de registro del evento

En el departamento de informática será registrado todo el proceso sobre el evento que se está presentando, se deberá guardar el historial de acciones tomadas y el nivel de respuesta dentro del servidor ante cada acción.

Figura 38. **Procedimiento para registro de un evento**



Fuente: elaboración propia, empleando Visio 2016.

El presente diagrama podrá servir para los usuarios dentro del departamento de informática o de las áreas de interés, para poder actuar ante algún evento que se pueda presentar.

3.6.3. Evaluación de los diferentes eventos

Los eventos se diferenciarán por la fuente en que se describió la señal de alerta, dividiendo únicamente en eventos internos del sistema o eventos externos con brechas hacia el sistema por equipos periféricos o usuarios conectados en dispositivos remotos.

3.6.4. Resolución y recuperación

Para la resolución y recuperación podrá ser ejecutada y puesta en práctica la matriz del plan de incidencias contemplada en la tabla XXIII, adecuando cada fase de ese protocolo hacia la resolución del problema o de las fallas que se presentaron. La respuesta deberá ser inmediata por los representantes del departamento de informática, si un supervisor de cualquier área distinta a informática logra darse cuenta antes, deberá reaccionar con el mismo protocolo de respaldo y reacción. La recuperación de cualquier tipo de información sustraída o eliminada de ciertos sectores de la Web, podrá ser recuperada desde la fuente o raíz del servidor. Ante cualquier ataque al servidor podrá tenerse los programas cortafuegos ya que al ingresar a su sistema raíz podrá ser saboteada toda la información allí guardada sin presentar copia digital o copia física.

3.7. Proceso de inspección

La inspección quedo a cargo del departamento de informática, este tipo de monitoreo quedo establecido a ser realizado diariamente, el proceso de inspección se sustenta en la figura 35 promoviendo los niveles de monitoreo y evaluación en la prevención de incidentes de seguridad.

3.7.1. Gestión de servicios corporativos

La gestión iniciara con la definición y presentación del servicio que se desea desarrollar o incorporar, este tipo de gestión deberá ser firmado y aprobado por el jefe de área, se enviara por correo digital interno a cada departamento de interés con una copia simple sin intención. Los servicios corporativos comúnmente adoptan funciones que permitan mejorar la relación de trabajo de sus subordinados, mejorando las herramientas de trabajo, otorgando permisos especiales a ciertos sectores de la red interna o sobre aspectos en claves de accesos a dispositivos periféricos.

3.7.2. Gestión de servicios de seguridad

Este tipo de gestión se podrá realizar cuando se evalúe alguna brecha que pueda representar vulnerabilidad hacia cierto sector informático en el Software, Web interna o hacia el servidor. Para el desarrollo de estas actividades será importante limitar al departamento de informática con la alta gerencia, no podrá participar algún otro tipo de departamento, porque para ellos escapa las responsabilidades, conocimientos y configuraciones internas de la red.

La gestión iniciara con el desarrollo de la propuesta, se incluirán los objetivos, motivos y alcances previos, además se incorporará el diseño completo de la gestión, contemplando cambios o reforzamientos hacia ciertos procesos ya establecidos. No se permitirán realizar pruebas sin antes ser presentado, evaluado y aprobado por alta gerencia. Al ser incorporada cualquier gestión que involucre cambios sensibles en la interfaz de los usuarios deberán preparar la debida capacitación indicando cuales fueron los cambios mínimos o mayores para evidenciar así que el departamento de informática se compromete con la seguridad de sus funciones establecidas.

3.7.3. Ingeniería de servicios de seguridad

Esta acción es reconocida como la prevención hacia cualquier evento que pueda suceder dentro de la empresa. Para el desarrollo de la gestión administrativa se consideró implementar aspectos contenidos en la Norma ISO 27001 y los protocolos de incidencias, se incorpora el monitoreo y el uso de herramientas como cortafuegos, adquirir un nuevo sistema operativo no será tarea fácil, pero la garantía será en el respaldo de la información.

El contexto de la ingeniería se podrá visualizar al incorporar lo que represente una propuesta, ejecutar los programas periféricos de resguardo y los protocolos de seguridad en función de la prevención de incidentes, se suma a esto el proceso capacitación y ambientación de los usuarios con la interfaz, y se concluye con la adecuada segmentación de los usuarios con su perfil idóneo y el rol dentro del sistema informático. Se consideraron los aspectos de permisos y credenciales para asegurar que no existan duplicidad de tareas o compadrazgos que eviten exponer hechos fraudulentos.

3.7.4. Operación de los servicios de seguridad

La operación está a cargo del personal de informática, no se ha establecido un numero especifico de colaboradores para estas tareas, pero se podrán guiar por el número de usuarios que se conectarán a la red más la sumatoria de las computadoras y equipos periféricos. Se podría dar la proporción de 10/1 donde se presentaría por cada 10 usuarios o dispositivos con acceso a la Web interna se podrá asignar un supervisor de servicios de seguridad. Se establece esta relación por el alto flujo de datos que serán enviados desde antes de iniciar las labores hasta dar por concluida la jornada de trabajo, sin despreciar todo tipo de evento que pueda presentarse.

3.7.5. Monitoreo de seguridad

El monitoreo se llevará desde las oficinas de informática, el departamento de seguridad tendrá asignado otro tipo de monitoreo por cámaras. Para esta sección se puede especificar que el monitoreo en la red se realizará conectado indefinidamente a la red interna, con las herramientas provistas por el SUM Server se podrán obtener datos en tiempo en vivo, con las diferentes configuraciones sobre el rol de los usuarios se podrán obtener los datos que proporcionen información del trabajo que puedan estar realizando o si se encuentran desperdiciando su tiempo de trabajo esperado.

3.7.6. Inteligencia de seguridad

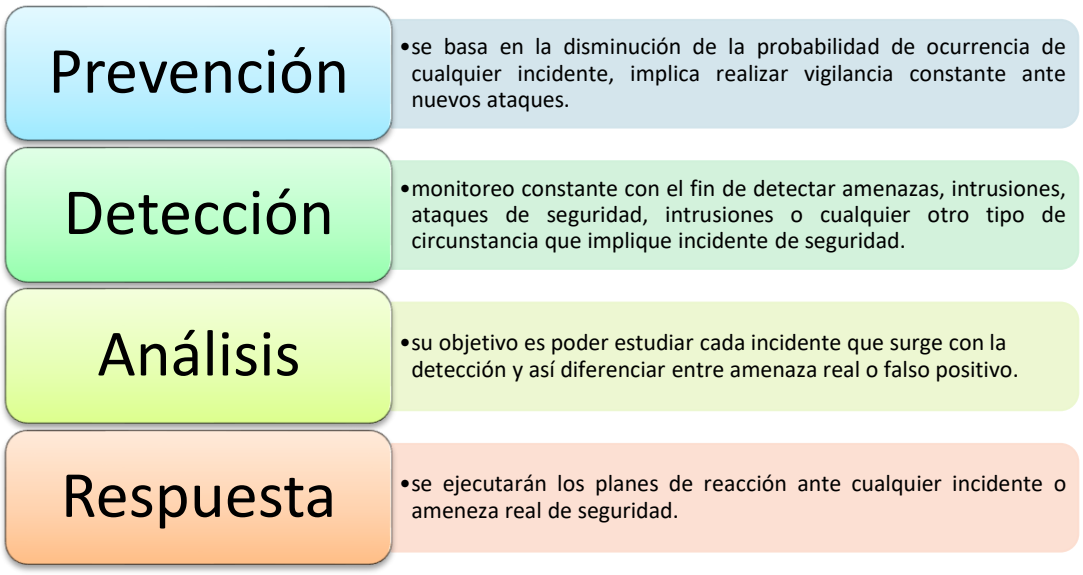
La arquitectura de la red interna permitirá evaluar sobre índices de comportamiento de los usuarios, dicho de otra forma podrá enviar alertas cuando algún usuario permanezca por más de cuatro minutos de inactividad, se podría emplear algún protocolo de suspensión de labores temporal, que permita enviar los reportes constantes hacia los colaboradores reincidentes, donde se transcurra en un día normal de trabajo y con tres alertas de inactividad se bloquee su terminal y las preferencias otorgadas a su usuario, para que pueda actuar el supervisor inmediato del área y le levante queja por incompetencia hacia su puesto de trabajo.

Esta fase será critica, deberá ser evaluada por los jefes de áreas, se podrán atribuir aleatoriamente que la inactividad podría representar ejecución propia de las tareas asignadas, donde tendrán que dedicar mayor parte de su tiempo para leer documentos y no redactar únicamente. La inteligencia de seguridad brindará el respaldo necesario siempre y cuando la configuración y detalle de aspectos críticos sean claramente planteados y establecidos.

3.8. Planteamiento de un centro de operaciones de seguridad (SOC)

Se conoce como una unidad de tipo centralizada dentro de las oficinas administrativas de una organización, su objetivo es dedicarse exclusivamente a controlar y supervisar los temas tácticos como los operativos asociados hacia la seguridad informática. Este centro de operaciones realiza el conjunto de labores orientadas al monitoreo, defensa de los activos de la información y el aseguramiento por medio de equipos tecnológicos con personal especializado que puedan monitorear en tiempo real cada uno de los eventos generados por la red de infraestructura tecnológica del Ingenio ejecutándose las 24 horas del día y los 7 días de la semana.

Figura 39. **Funciones importantes del SOC**



Fuente: MORALES GONZÁLEZ, Carlos Andrés. *Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana*. http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y. Consulta: 15 de abril de 2021.

Tabla XXVII. **Servicios característicos del centro de operaciones**

Tipo de servicio	Descripción del servicio
Detección y gestión de vulnerabilidades	Servirá para identificar las debilidades que pueda poseer el Ingenio, para ello se deberán realizar auditorías de forma automática y periódica, dirigidas hacia diferentes puntos de la infraestructura tecnológica de las oficinas administrativas con el fin de identificar debilidades y determinar acciones correctivas que eliminen cada vulnerabilidad.
Monitorización continúa de la seguridad	Consistirá en la observar constantemente los controles de seguridad que fueron propuestos he implementarlos con el objetivo de detectar incidentes de seguridad. Se deberá apoyar en diferentes herramientas que proporcionen información completa en tiempo real de los estados de niveles de seguridad del Ingenio.
Centralización, tratamiento y custodia de *logs*	Para el manejo y gestión del volumen de *logs* generados por diversos dispositivos conectados a la Web, se requerirá el uso del sistema SUM Server que permitirá correlacionar los diversos eventos de seguridad para detectar las situaciones sospechosas o poco comunes. Esos *logs* podrán ser almacenados para consultas posteriores y así poder investigar eventos acaecidos.
Programas de prevención	El centro de operaciones trabaja con la filosofía de prevención de incidentes que puedan violentar la seguridad a través de la vigilancia constante de nuevas amenazas y con la implementación de distintos controles preventivos que minimicen el riesgo de aparición de incidentes de seguridad.
Asesoría de seguridad	Los profesionales en seguridad informática podrán apoyar a los miembros de alta dirección en la toma de decisiones de seguridad de la información, apoyando la dirección en la toma de decisiones sobre la seguridad de la organización, por eso el SOC deberá disponer de personal con el conocimiento especializado en sistemas informáticos y comunicaciones, expertos en seguridad física y lógica, abogados especializados en temas de informática y auditores de seguridad, por último pero de igual relevancia, poder contar con analistas de malware.
Respuesta de resolución	Ante cualquier tipo de incidente o evento de seguridad, el SOC deberá activar los planes de solución para neutralizar la amenaza, considerando el nivel de criticidad del ataque y la criticidad de los activos comprometidos, así como el impacto sobre los mismo.

Fuente: MORALES GONZÁLEZ, Carlos Andrés. *Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana*. http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y. Consulta: 15 de abril de 2021.

3.8.1. Planta física

La infraestructura física que soportará el SOC se podrá acomodar en el centro de cómputo principal o en dentro del departamento de seguridad si existiese de espacio y capacidad física. El diseño será acorde a los requerimientos del proveedor del equipo de cómputo y el proveedor del servidor, se considerarán las capacidades de las instalaciones.

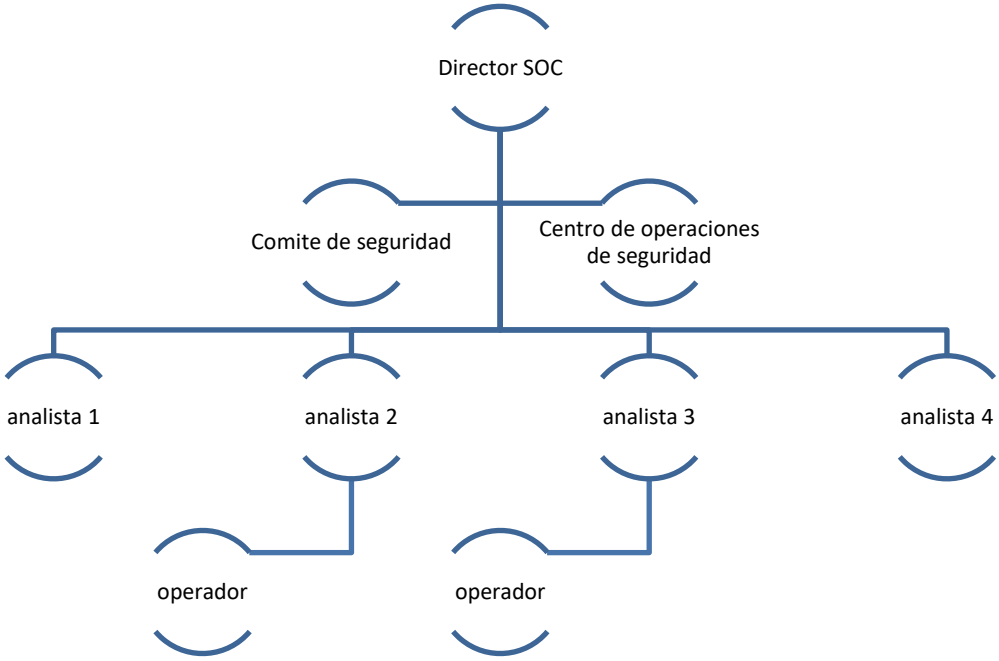
3.8.2. Área de la distribución principal

Para las dimensiones del área de distribución se deberán contemplar los equipos ya descritos, el acondicionamiento artificial o natural para evitar altas temperaturas, otro factor relevante que podrá determinar el área es directamente proporcional a la cantidad de personal asignado, no se podrá emplear espacio físico menor a 24 metros cuadrados para garantizar que de forma ergonómica puedan encontrarse diariamente por lo menos 3 personas dentro de esas instalaciones con aire acondicionado.

3.8.3. Organigrama

Se desarrolla la propuesta acorde al tamaño de las operaciones proyectadas para las oficinas administrativas.

Figura 40. **Organigrama propuesto para el SOC**



Fuente: elaboración propia.

Para el organigrama en el SOC se propone incorporar un Director, su comité de seguridad el espacio físico para el centro de operaciones, a un mismo nivel los analistas de riesgos y dos operadores, los analistas uno y cuatro podrán funcionar como supervisores y personal de apoyo directo hacia el comité de seguridad, los informes serán redactados por los operadores hacia los analistas dos y tres, quienes enviarán sus resultados al comité de seguridad.

3.8.4. Distribución de responsabilidades

Para el personal a contratar o capacitar dentro del ya existente en el departamento de informática, se deberán apegar a un mínimo planteado en el organigrama para realizar y desempeñar las actividades esperadas.

Tabla XXVIII. **Distribución de responsabilidades según el puesto ocupado**

Puesto	Descripción de su responsabilidad
Director	Será el encargado y responsable para llevar a cabo la planeación, coordinación toma de decisiones estratégicas para la correcta operación del centro de operaciones de seguridad y de cada servicio que esta pueda brindar al Ingenio, garantizará la disponibilidad de los recursos necesarios para otorgar la atención de eventos críticos, especialmente sobre los que puedan resultar en daños o pérdidas irreparables de la información o infraestructura, llevará a cabo la toma de decisiones necesarias para garantizar la continuidad de las operaciones por turnos o jornadas extendidas en horarios de 7 x 24 x 365 según los ritmos demandantes de la empresa, dará el visto bueno de las solicitudes que sean necesarias escalar, brindará los lineamientos y procedimientos para la generación de reportes sobre determinados procesos y definirá las líneas de acción en caso de presentarse contingencias internas.
Analista de seguridad	Será el encargado de apoyar en la interpretación y tomar decisiones sobre algún evento que tenga calidad de actividad sospechosa, falto positivo o tipo de incidente de seguridad, podrá cambiar la calidad de actividad sospechosa o falto positivo decretada por el operador, validará y apoyará en la definición de líneas de acción para el tratamiento de actividades sospechosas e incidentes de seguridad, validará cada evento de información que le sea escalado por los operadores, conocerá los niveles de servicio comprometido para identificación y notificación de actividades sospechosas.
Operador	Encargado de ejecutar el monitoreo constante de la red e infraestructura tecnológica del Ingenio, interpretará si un evento presenta calidad sospechosa o podría ser un falso positivo, identificará y escalará posibles incidentes de seguridad, aplicará ciertas actividades de contención pre-autorizadas reactivas o proactivas hacia el tratamiento de actividades sospechosas e incidentes de seguridad, realizará análisis para determinar el nivel de calidad sospechosa, registrará los eventos que puedan ser calificados como actividad sospechosa dentro del SUM Server, notificará oportunamente acciones presentadas, entregará a los analistas de seguridad los informes debidamente detallados y redactados sobre las bitácoras de eventos suscitados. Todo esto con la finalidad de investigaciones sobre eventos que hayan podido haberse dado.

Fuente: MORALES GONZÁLEZ, Carlos Andrés. *Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana*. http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y. Consulta: 15 de abril de 2021.

Las responsabilidades están distribuidas por cargo y nivel de participación dentro de estas nuevas acciones que mejoraran la supervisión, monitoreo y respaldo informático hacia el Ingenio.

4. IMPLEMENTACIÓN DEL SISTEMA DE GESTION

4.1. Cronograma de actividades

Durante el proceso de evaluación situacional y la creación de la propuesta, se tomarán en cuenta desde que fue aprobado el tema hasta la culminación y presentación del actual trabajo de investigación.

Tabla XXIX. **Cronograma de actividades**

No.	Actividades	Mayo 2021				Junio 2021				Julio 2021				Agosto 2021				Septiembre 2021			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Culminación y entrega de investigación																				
2	Evaluación y validación de tesis																				
3	Culminación y visto bueno																				
4	Prueba piloto																				
5	Obtención de resultados																				
6	Tratamiento de información																				
7	Análisis e interpretación sobre los procesos piloto																				
8	Análisis e interpretación sobre los procesos implementados																				

Fuente: elaboración propia.

El cronograma podría sufrir variaciones en el transcurso de la incorporación y adaptación dentro de la empresa.

4.2. Responsabilidad de las actividades

Para el Ingenio será trabaja multisectorial, la primera fase podría ser responsabilidad de alta gerencia quienes aceptarían y validarían la propuesta, luego se trasladaría la información y herramientas diseñadas hacia los departamentos que se verán involucrados, el primer departamento involucrado será Informática, este evaluara cada aspecto contenido que involucre la seguridad informática, accesos, control, monitoreo y supervisión de los usuarios.

Poder emigrar de la tecnología actual hacia el nuevo modelo es tarea compleja, para esa tarea sería necesario incorporar previamente hacía el departamento de seguridad el SOC propuesta. Con este complemento se podrá fortalecer y reforzar la seguridad con nuevas herramientas de monitoreo. Luego de esta acción ya podría trasladarse la responsabilidad hacia el departamento de recursos humanos, su tarea será capacitar al personal sobre el nuevo recursos tecnológico que será implementado, cuál será el manejo de la interfaz del usuario, cuáles serán los nuevos sistemas de monitoreo para que ellos estén por avisados y enterados que serán supervisados en todo momento, además de las nuevas herramientas que incorporará el departamento de informática, que si un usuario podría estar sin interacción dentro de su computador automáticamente será bloqueado.

Todas estas acciones serán evaluadas dentro del programa de actividades, específicamente se esperaría realizarlo en la segunda fase del cronograma, los altos mandos en trabajo conjunto con los jefes de área y algunos supervisores elegidos podrán debatir, optimizar o reducir el impacto de la propuesta, luego de

ser implementada la propuesta, la responsabilidad estará dividida por el recurso humano y los operadores del SOC.

4.3. Implementación de estandarización de procesos

La ruta crítica estará definida con el desarrollo del trabajo de Informática y el departamento de recursos humanos quienes deberán contener la descripción detallada del rol de cada usuario con el perfil necesario sobre las tareas específicas que deberán ser asignadas dentro del nuevo servidor y el nuevos Software.

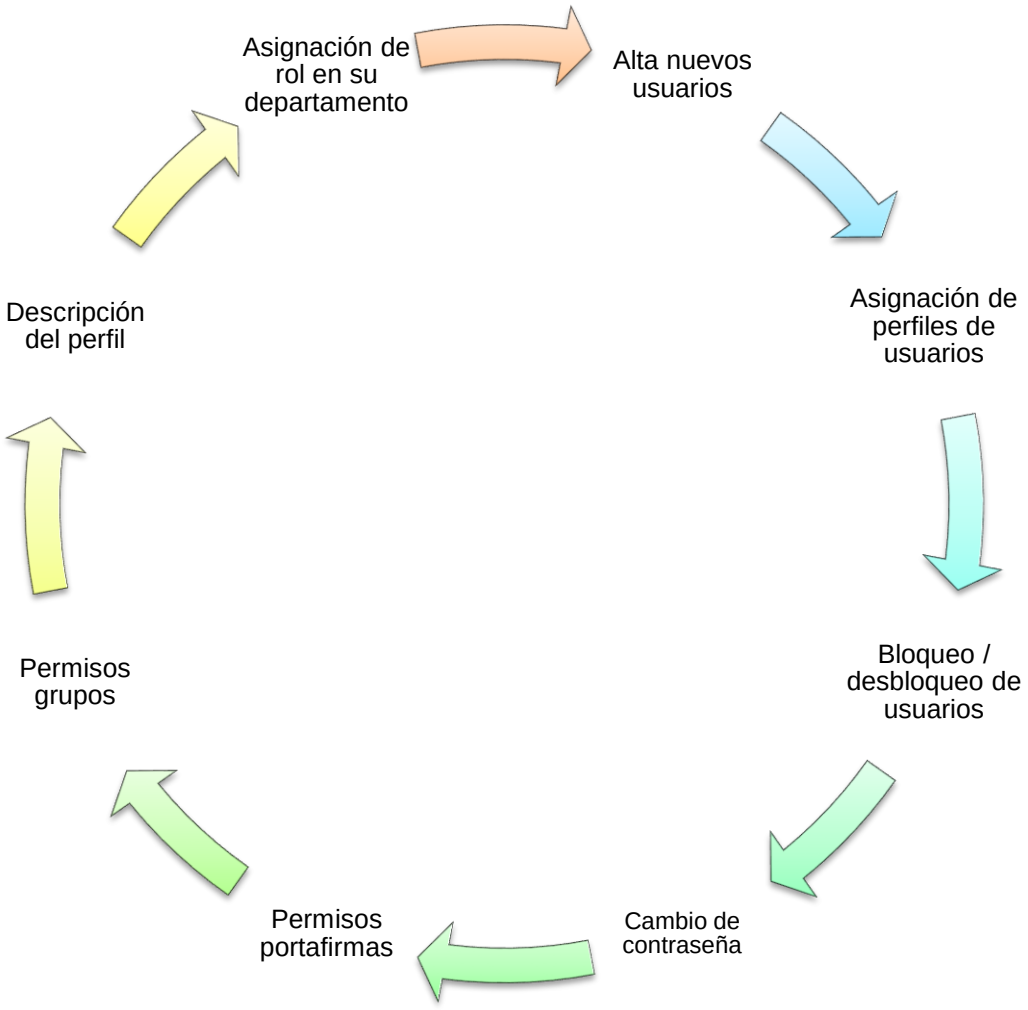
Para obtener la estandarización será necesario que se ejecuten los comandos descritos en la tabla XX (Descripción de las actividades del manual de accesos). Con la incorporación y desarrollo de ese manual se prevé que los usuarios serán acondicionados según las especificaciones por puesto y área de trabajo. No se podrán duplicar funciones o usuarios.

El diseño propone que inicialmente se deberá aprobar la compra y configuración del servidor, luego de eso se deberá contemplar la creación de la estación SOC, se podrá proceder a seleccionar al personal apto para iniciar a diseñar la configuración y desarrollo dentro del servidor por medio del Software SUM Server. Se procederá a solicitar la información por área de interés que será incorporada al sistema raíz del servidor, se pedirá información cruzada con la debida autorización de alta gerencia.

Por cada departamento se solicitará el listado detallado con los roles y perfiles de cada colaborador, esta información será cruzada con el departamento de recursos humanos para garantizar que se posee información actualizada y que se están respetando los niveles jerárquicos establecidos. Al poseer la base

de datos se podrá crear usuario por usuario con los permisos y credenciales aprobados por cada oficina responsable. Al concluir estas etapas se procederá a realizar pruebas y medir resultados previos.

Figura 41. **Accesos necesarios para la implementación de los procesos**



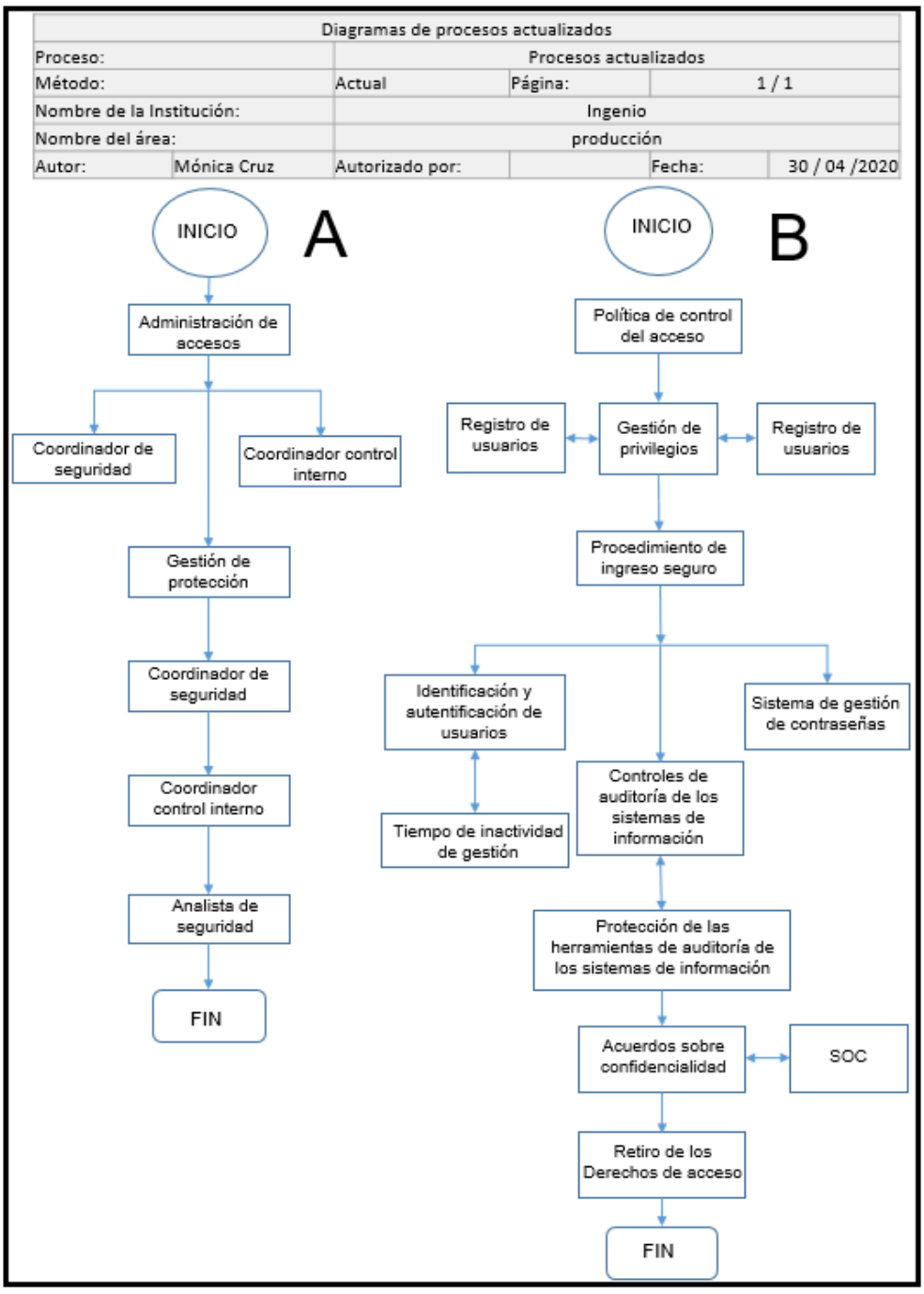
Fuente: elaboración propia.

Otro aspecto relevante dentro de la implementación, será asignar al personal idóneo que desempeñe las funciones de analistas para el departamento de informática y la unidad SOC. Las capacitaciones serán realizadas por el departamento de recursos humanos paralelamente al haber aprobado la propuesta y cuando se esté ejecutando el desarrollo tecnológico con la creación de usuarios, roles y perfiles con sus debidas credenciales.

4.3.1. Diagramas de bloque de procesos actualizado

Se presenta al diagrama en la columna A, ese diagrama es el que emplea actualmente el Ingenio, el diagrama B es la propuesta.

Figura 42. **Diagramas de procesos actualizados**

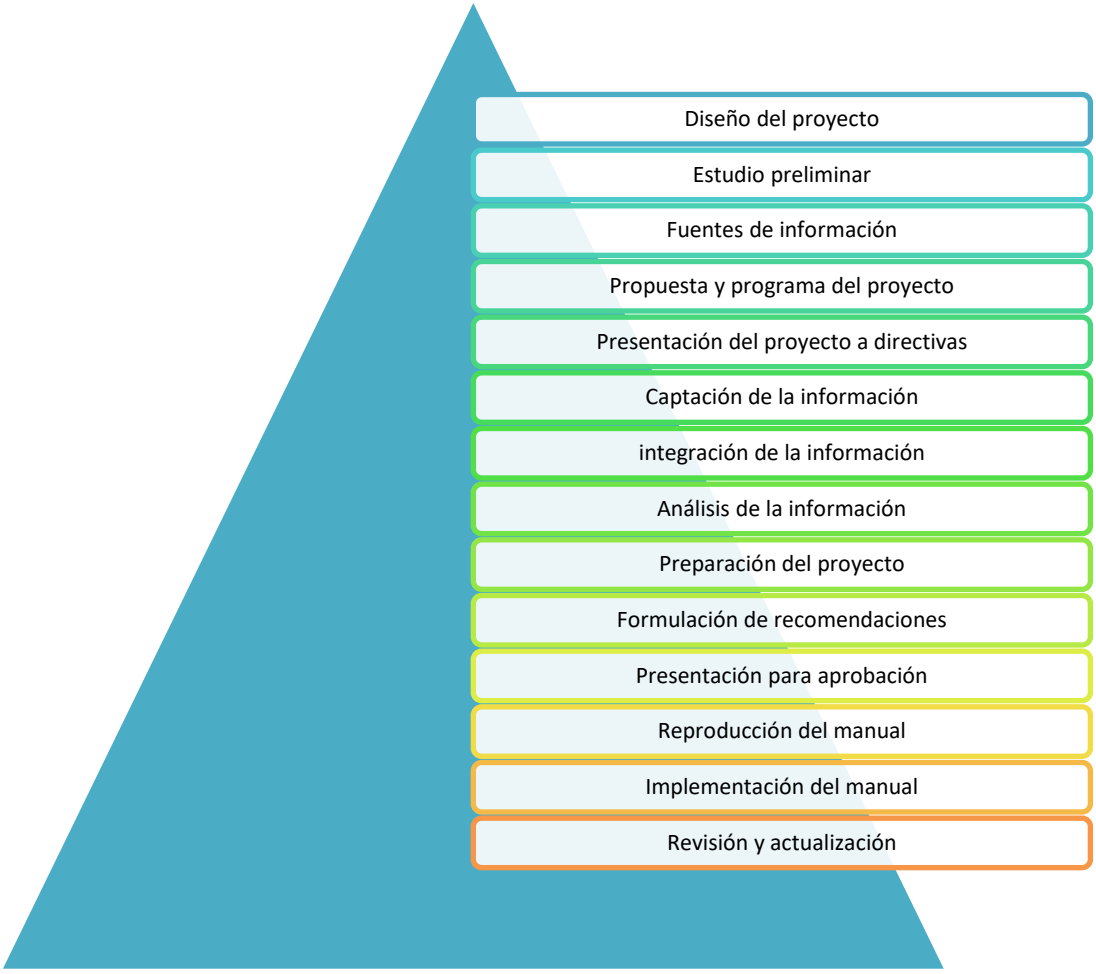


Fuente: elaboración propia, empleando Visio 2016.

4.3.2. Manual de procedimientos estandarizados

Se plantea el esquema que deberá desarrollar la empresa para el desarrollo del manual de procedimientos estandarizados en función de la propuesta en procesos y protocolos de supervisión.

Figura 43. **Estructura del manual de procedimientos estandarizados**



Fuente: PALMA, José. *Cómo hacer un manual de procedimientos.* https://www.gestiopolis.com/creacion-de-un-manual-de-procedimientos/. Consulta: 6 de diciembre de 2020.

4.4. Aplicación del método apto para mejora continua

El método propuesto se fusionará con la incorporación de un nuevo servidor, nueva plataforma digital, incorporar un nuevo Software con la descripción de sus procesos para creación, asignación de rol y autorización de contraseñas desde el sistema raíz, con asignación de permisos y accesos restringidos. Este nuevo método no podrá ser eficiente sin el acompañamiento y creación del departamento SOC. Toda la gestión administrativa será monitoreada 24 x 7 x 365, se podrán emplear los aspectos básicos de la Norma ISO 27001.

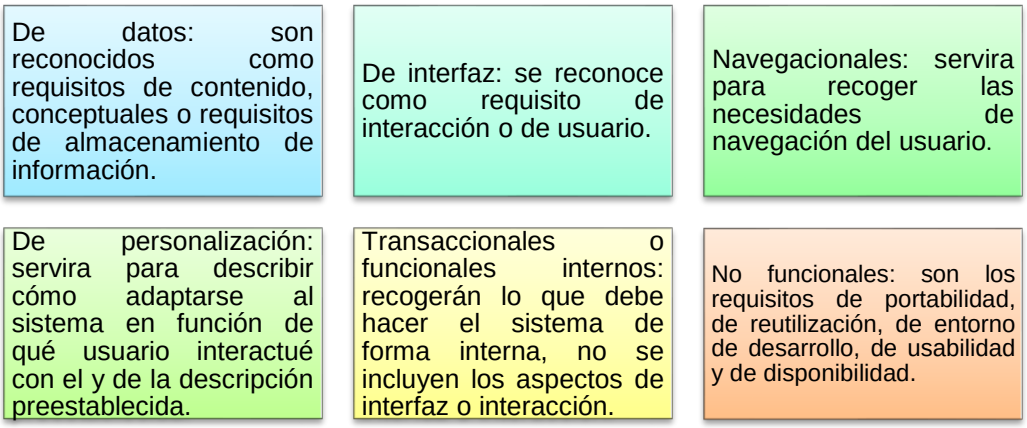
Este método no será exclusivamente para monitoreo en tiempo real, la gestión incorporará resultados y alertas tempranas en las deficiencias de los colaboradores que no permanezcan en su puesto de trabajo, que empleen el tiempo de oficina para el ocio o simplemente para llegar a ocupar un lugar sin promover resultados viables hacia la inversión de su estadía.

La valoración del método propuesta estará marcada con el punto de inflexión comparativo con la inversión versus los resultados esperados, si los resultados esperados pueden mejorar los datos actuales sobre la recolección de información en horas-hombre-producción. Esta valoración quedará sujeta hacia alta gerencia, ellos delimitarán porque sería viable y porque podría promover rotación de personal. No está por demás indicar que el departamento de recursos humanos deberá prepararse para diseñar las capacitaciones necesarias, medir cual será el posible el índice de rotación de personal y cuales podrán ser las plazas disponibles luego de 3 meses de medición y evaluación de resultados.

4.4.1. Estudio de requisitos

La sistematización con la incorporación de herramientas adecuadas de nivel informático es requerimiento importante para el Ingenio. Para lograr desarrollar la gestión administrativa con implementación de ese nuevo protocolo de control será necesario que el servidor posea comunicación, aceptación he intercambio dentro de la propia interfaz empleando herramientas internas muy propias de la informática. Para eso se necesitarán incluir ciertos requisitos en la propuesta para la Web interna.

Figura 44. **Requisitos relevantes en sistemas web**



Fuente: elaboración propia.

Estas técnicas se fundamentan en las fases del proceso de desarrollo de la Web. Se evalúan las técnicas que incluyen los procesos de definición de cada requisito dentro del ciclo de vida del proyecto. Las propuestas podrían incorporar la captura y definición de requisitos puntuales desde sus primeros objetivos.

Tabla XXX. **Presentación de propuestas por tipo de requisitos para la web**

Propuesta	Tipo de requisitos a ser incorporados en la arquitectura digital
WSDM: Web site design method	Su estructura es basada para el desarrollo de sitios Web, acá el sistema se puede definir en base a los grupos de usuarios. Su proceso de desarrollo está dividido en cuatro fases: diseño conceptual, diseño de la implementación, modelo de usuario y su implementación. La fase crítica dentro de esta plataforma es poder detectar los perfiles de usuarios para los cuales se está construyendo la aplicación.
SOHDM: Scenario-based object-oriented hipermedia design methodology	Por medio de esta aplicación se presenta hacia el servidor la necesidad de poder diseñar y disponer el proceso que permita capturar todas las diferentes necesidades del propio sistema. Se pueden utilizar escenarios como modelos o patrones.
RNA: Relantionship-navegational analysis	Se deberá plantear la secuencia de etapas para poder desarrollar las aplicaciones Web, se fundamentará el diseño en el flujo de trabajo de análisis de las necesidades. Sus cinco etapas o necesidades serán las siguientes: análisis del entorno, elementos de interés, análisis del conocimiento, análisis de la navegación y su implementación del análisis.
HFPM: hipermedia flexible process modeling	Por medio de esta propuesta se puede describir un proceso en forma detallada que pueda abarcar la totalidad del ciclo de vida del proyecto de un Software. Trabaja con la programación y ejecución de tareas, siendo las principales: Descripción breve del problema, descripción de los requisitos funcionales mediante casos de uso, realización del modelo de datos para cada caso de uso proponiendo el uso del modelo de clases, modelación de la interfaz del usuario y la modelación de los requisitos no funcionales.
OOHDM: object oriented hipermedia design model	Esta propuesta es de desarrollo metodológico, parte de los casos de uso. Resalta la necesidad de iniciar el diseño del sistema, especialmente en su entorno Web con el claro y amplio conocimiento de las necesidades de interacción en la que cada usuario se comunicará con el sistema.
UWE: uml-bases web Engineering	Será necesario desarrollar el proceso unificado, con la captura de requisitos. Para el resultado final de la captura de requisitos será el obtener un modelo de casos de tipo acompañamiento de la documentación que puede describir los usuarios del sistema, las reglas de adaptación, la interfaz y los casos de uso.

Continuación de la tabla XXX.

W200	Puede ser empleado para modelar los elementos multimedia. Sus tres etapas de análisis son: diseño funcional, diseño de hipermedia y el análisis de requisitos. Sus pilares serán el análisis de requisitos de navegación y el análisis de requisitos funcionales.
UWA: ubiquituos web applications	Para estos procesos es necesario iniciar la definición de los diferentes roles de usuario que sean permitidos interactuar con el sistema, la autorización en la relación entre ellos y los objetivos globales de este tipo de proceso. Se basará en la búsqueda de conflictos entre los usuarios.
NDT: navigator development techniques	Es una técnica para analizar, especificar y diseñar el aspecto de la navegación en aplicaciones Web. Será relevante la propuesta que ofrezca la definición y captura de requisitos.

Fuente: elaboración propia.

Estos requisitos serán necesarios para diseñar la red informática en la Web interna, estas tareas serán asignadas al departamento de informática para que pueda ser validadas, se podrá otorgar participación de los jefes de área para interpretar el lenguaje de programación y propongan sobre los aspectos requeridos. El SOC podrá otorgar aspectos relevantes al iniciar con estos análisis internos, con la definición de roles se espera otorgar las credenciales necesarias para el desarrollo técnico de lo que se desea buscar en la gestión administrativa.

4.4.2. Resultado de estudios

Según la clasificación de requisitos se realiza la tabla comparativa sobre las propuestas, esto se realiza para poder determinar cuáles son los tipos de requisitos que puede incorporar y proponer cada propuesta.

Tabla XXXI. **Resultado sobre el estudio de requisitos**

Propuesta	REQUISITO					
	Datos	Interfaz	Navegación	Personalización	Transacionales	Funcionales
WSDM	x			x		X
SOHDM	x	x			X	
RNA	x	X	x		X	
HFPM	x	X	x			x
OOHDM	x	X	x			
UWE	x	X	x	X		x
W2000			x	x	X	
UWA	x	X	x	x	x	
NDT	x	x	x	x	x	x
DDDP	x	x	x	x	x	x

Fuente: elaboración propia.

Se emplean los datos de ese tipo de estudio para obtener la matriz base que permita seleccionar la mejor propuesta, no se puede plantear la respuesta concluyente, quedará sujeta al análisis de junta directiva en colaboración de los jefes de área y el departamento de informática. Para el entendimiento, valoración y comprensión de la matriz de resultados de los requisitos es clave incorporar el personal debidamente calificado sobre las necesidades del Ingenio, por una mala decisión podrían obtenerse infinitos resultados negativos en el diseño final. También podrían considerarse los criterios de evaluación de los proveedores del servidor y quienes configuraran el nuevo Software.

4.4.3. Redacción de documentos

Los documentos serán de tipo oficial, incluirán el membrete del Ingenio en la esquina superior derecha. Se redactará de forma clara y precisa exponiendo el tipo de mensaje que se desea trasladar. Si es necesario se podrá incorporar imágenes o tablas para agrupar información concreta. Se deberán colocar las

credenciales del responsable que realiza el documento. No se recibirán informes o documentos sin el número de usuario con el nombre completo.

4.4.4. Alineación de los procesos

Con la relación en que se pueda ir desarrollando el análisis sobre la propuesta se podrán ir dando niveles estándares en la implementación de los procesos, para esta acción se podrán apoyar en el cronograma de actividades esperados. Cabe resaltar que los procesos serán considerados independientes sin precedencia uno de otro. El desarrollo de la interfaz será un proyecto externo asignado a la empresa que provea el servidor, a nivel interno se deberán habilitar los usuarios según el planteamiento de la administración de roles y perfiles.

Incorporar la interfaz al servidor será la siguiente fase en el proceso, previo a esto junta directiva habrá tenido que decidir si se instalara la unidad SOC y así dar brecha a su participación activa desde que se implantado el sistema raíz. Cada derecho y credenciales de participación ya deberán ser incorporadas a la interfaz, la complejidad en el desarrollo de la programación permitirá emitir alertas tempranas ante cualquier mal proceso establecido, la gestión administrativa podrá ser ejecutada al iniciar el sistema por completo con todos los usuarios, perfiles y roles cargados. Las pruebas piloto determinarán el alcance operacional, el efectivo monitoreo y la gestión de seguridad eficiente.

4.4.5. Capacitación

La capacitación deberá contar con la participación mínima de tres departamentos; el departamento de Informática, el departamento de recursos humanos y el departamento administrativo. El compromiso de estos tres

departamentos podrá robustecer las capacidades técnicas y operativas de su personal asignado que iniciará a trabajar con la nueva interfaz.

Tabla XXXII. **Proyección de la capacitación**

TEMA	DURACIÓN	MODALIDAD	FACILITADOR
Introducción	1 hora	Presencial	Recursos humanos
Descripción de módulos	1 hora	Presencial	Informática
Inicio de sesión	1 hora	Presencial	Proveedor de servicios
Gestión de cuentas	30 minutos	Presencial	Proveedor de servicios
Gestión de usuarios	30 minutos	Presencial	Proveedor de servicios
Operaciones del sistema	1 hora y 30 minutos	Presencial	Proveedor de servicios
Consultas del sistema	1 hora y 30 minutos	Presencial	Informática
Gestor administración	1 hora y 30 minutos	Presencial	Informática

Fuente: elaboración propia.

4.4.6. Comunicación de cambios

Previo a realizar algún cambio deberá ser trasladada la propuesta a los jefes de área involucrados, se deberá describir el tipo de cambio propuesta con la justificación exacta con los detalles del porque el cambio y para qué. No se autorizarán los cambios sin autorización de por lo menos tres departamentos con la firma física del jefe de área. Se espera que estas áreas mínimas de aprobación y control de la información sea el departamento administrativo, el departamento de recursos humanos y el departamento de informática.

4.5. Ciclo de vida de eventos de seguridad informática

Con el programa de monitoreo y alerta temprana se podrá detectar alguna brecha en la seguridad informática de forma inmediata, en la figura 37 se obtiene el ciclo de vida de algún evento de seguridad, la respuesta y reacción dependerá del nivel de experiencia del técnico asignado a estas tareas, se espera que el propio software con la incorporación del malware actué en fracción de segundos, seguido de eso es posible la contención y separación del sector que está siendo afectado con otra posible fracción de segundos.

Se procederá a analizar el evento, paralelamente se incorpora el plan de incidencias, para cada etapa dentro del plan dependerá de la velocidad con que se desarrolle el servidor y los programas auxiliares, para el recurso humano será breve accionar este tipo de protocolo, pero no se podrá descifrar la complejidad y magnitud del evento hasta que se presente, se consideran fracciones de segundo de respuesta, pero dependerá de la malicia del programa o de la persona que presente este tipo de peligro.

4.5.1. Detección del evento

Para la detección del evento será primordial que dentro del sistema se presente una alerta de ruptura de seguridad, sin ese tipo de alerta será difícil validar el evento con rapidez, podría ser observado hasta transcurrir algún tiempo indeterminado donde el técnico analista pueda percibir la brecha de seguridad en el sistema.

4.5.2. Registro e identificación del evento

Para esta acción se procederá a registrarlo dentro del propio sistema informático, se emitirá alerta temprana a los supervisores y altos mandos de lo sucedido. Se consignará el día del evento, la hora de inicio, la hora en que se logró contener y cuáles fueron los posibles sectores afectados o información extraída. Si el evento registrado es por adición o incorporación de algún virus dentro del sistema, se deberán detener todas las labores de forma preventiva hasta que se pueda controlar la situación.

4.5.3. Evaluación

Se medirán los alcances y penetración de la brecha de seguridad, así como su agresión hacia el servidor o los programas de interés que fueron afectados. La evaluación permitirá medir el tiempo de respuesta ante algún evento inesperado, cuales fueran las acciones preventivas adquiridas, si el técnico o supervisor del SOC actuó con apego a las tareas diseñadas. Si los resultados son deficientes sobre la conducta del personal asignado a estas tareas se deberán tomar posturas inmediatas para fortalecer el desplegué de sus funciones, medir la necesidad de capacitaciones y de último recurso evaluar la necesidad de sustituir ese personal con bajo nivel de calificación.

4.5.4. Resolución y recuperación

No se garantiza la recuperación de los sectores afectados o de la información comprometida, todo este tipo de acciones son subjetivas. La resolución será trasladada con un informe especial explicando cuales fueran las posibles causas que permitieron que se diera este evento, cual fue el panorama

que se vivía en ese determinado momento, si existe la participación y ocurrencia de personal interno o si la violación fue remota hacia algún dispositivo periférico dentro de las oficinas administrativas.

4.6. Proceso de inspección

La inspección se podrá realizar desde la estación SOC esa tarea está programada y asignada hacia los operadores, acción similar, pero con mayor penetración será realizada por los analistas. Con la ausencia del SOC se podrá realizar esa tarea con los supervisores de cada departamento, el departamento de informática gestionará para que la mayoría de su recurso humano participe de estas actividades, la temporalidad de inspección será 24 x 7 x 365 con presencia o ausencia de los colaboradores. No se podrá dar pautas de descanso para esta tarea, la función de esta acción es impedir que ocurra algún evento en la brecha de seguridad y que permita comprometer el activo más valioso del Ingenio, parte de la inspección es validar que los equipos periféricos y dispositivos remotos permanezcan activos con los protocolos de seguridad.

La inspección requiere emisión de reportes diarios, se podrán emplear diseños homogéneos para su redacción y envío, se deberá informar a los jefes inmediatos por cada área participante en la inspección, esta se podrá ejecutar desde las computadoras oficiales y destinadas explícitamente para estas acciones con capacidad de monitorear más de 5 procesos y 10 colaboradores.

4.6.1. Gestión de servicios corporativos

Se basa en la necesidad de desarrollar plataformas o productos digitales que permitan simplificar las tareas dentro de un área específica, esta gestión deberá ser solicitada de forma escrita con la incorporación de los aspectos

detallados para lo que se desea solucionar. Será realizada por un supervisor hacia el jefe de área o por el jefe de área hacia la junta directiva.

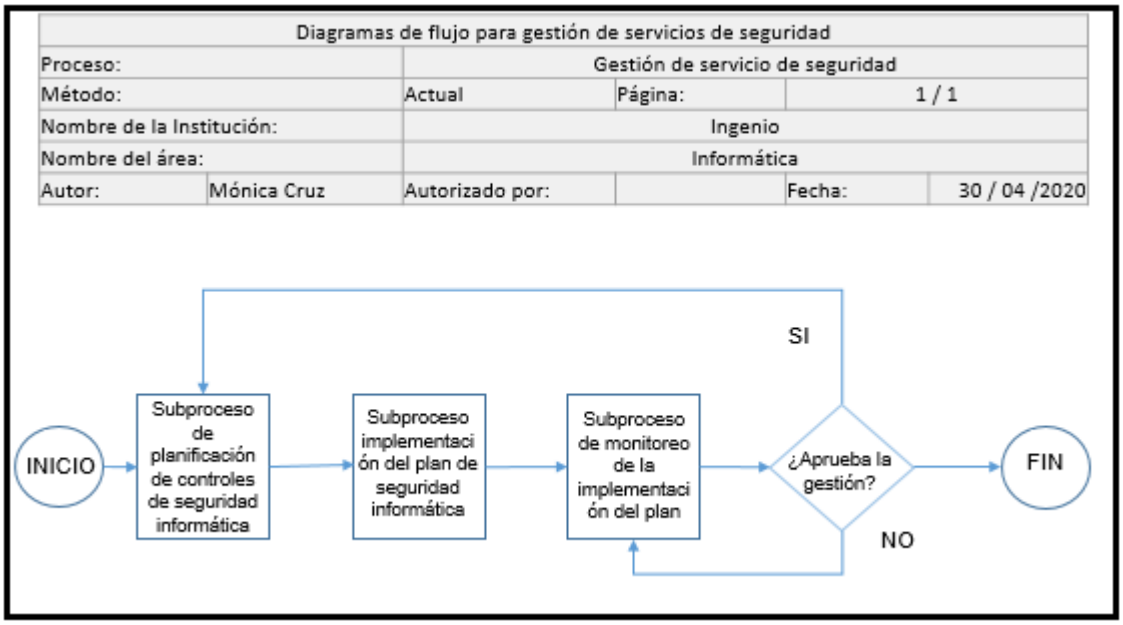
La intención es poder gestionar un conjunto de servicios que beneficien principalmente al Ingenio, dicho de otra forma, los solicitantes deberán poder priorizar si es de beneficio mutuo para agilizar procesos de trabajo o es una solicitud para confortar los deseos personales de su grupo de trabajo.

4.6.2. Gestión de servicios de seguridad

La gestión será redactada por el jefe de cada área o por el jefe de seguridad informática, se indicará la planificación necesaria que contenga los objetivos y alcances esperados, se puede emplear la base ya conocida del plan de seguridad informática como parte de la estructura en la gestión. Se deberá redactar de forma detallada el subproceso de implementación del plan de seguridad informática, dentro de la misma gestión se tiene que desarrollar la configuración con desarrollo textual del subproceso de monitoreo de la implementación, indicando por qué se está incorporando, hacia quienes va dirigida la acción y cuáles son las debilidades encontradas que puedan ser valoradas para dar el visto bueno.

Luego de estas etapas deberá ser trasladado a junta directiva, ellos deberán evaluar la propuesta y requerimiento para justificar si es viable o no, se redactar el debido informe anotando cada detalle en la discusión.

Figura 45. **Diagrama para la gestión de servicios de seguridad**



Fuente: elaboración propia, empleando Visio 2016.

4.6.3. Ingeniería de servicios de seguridad

Se complementa por la asesoría externa del proveedor de servicios, la formulación y gestión del proyecto de adquisición e incorporación del servidor, con la ejecución de su correcta instalación incorporando el Software que eficiente los procesos, se deberá valorar la legalización y adquisición de licencias de uso de los sistemas digitales para evitar demandas legales y alcances de los recursos sobre el aprovechamiento de la interfaz del usuario, por último pero muy importante dentro de la ingeniería de servicios es programar el correcto mantenimiento al servidor a los programas necesarios que serán instalados, a cada equipo de cómputo, a cada equipo remoto o equipo periférico que forma parte de la red de intercambio de paquete de datos. Todos estos aspectos formarán parte de la ingeniería de servicios de seguridad.

4.6.4. Operación de los servicios de seguridad

El monitoreo será su principal recurso dentro de la operación de estos servicios, se apoyará con las alertas de amenazas que reconozca el programa en su automatización, el personal a cargo de esta operación deberá ser responsable de las tareas asignadas, no se permitirán lapsos extensos para ausentarse de su puesto de trabajo y de su equipo de monitoreo. La operación en los servicios será efectuada 24 x 7 x 365 asignada a los técnicos, el grupo de supervisores podrán monitorear las mismas actividades que los técnicos, pero su penetración será de mayor alcance.

4.6.5. Monitoreo de seguridad

Para el monitoreo de seguridad se les asignara equipo de cómputo de alta capacidad, dos monitores por cada operador, no podrán utilizar ningún tipo de programa o software que no se haya autorizado previamente, podrán utilizar alguna herramienta dentro del sistema para escribir sus informes o realizar anotaciones sobre incidencias que marquen alerta temprana. Este monitoreo debería poder llevarse a cabo desde la estación SOC, de lo contrario se deberá adecuar la oficina explicita para acondicionar al personal y equipos especiales, por el tipo de actividad, deberá acondicionarse con equipo de refrigeración para evitar sobrecalentamientos de los equipos y su colapso.

Los analistas monitorearán colaboradores aleatorios desde su plataforma digital, podrán acceder a los equipos remotos dentro de las instalaciones, estos equipos remotos pueden ser cámaras de video vigilancia, micrófonos, entre otros. Se deben medir los patrones de participación he inactividad de toda la red, con esta acción se rendirán informes inmediatos hacia los jefes de área, el monitoreo es constante, continuo y sin descanso.

4.6.6. Inteligencia de seguridad

La programación adecuada dentro del servidor permitirá asignar señales de alerta, se propuso en el capítulo anterior incorporar alertas por inactividad de los usuarios transcurrido 4 tiempos o más, se podrá bloquear el usuario y su equipo de cómputo si el malware relaciona alguna actividad como acción negativa, notificando a los operadores de seguridad de esta ocurrencia de evento.

La inteligencia de seguridad será la plataforma basada en supuestos, estos supuestos deberán ser configurados por los proveedores de productos informáticos, o por los integrantes del departamento de seguridad en trabajo compartido con el departamento de informática. Cada supuesto se basará en la acción que pueda iniciar sin considerar los protocolos de trabajo ya suscritos, la inteligencia de seguridad reconocerá que este supuesto no actúa en conformidad con el usuario, el rol establecido y las credenciales limitadas cargadas en el sistema.

Por estas acciones se bloqueará la ruta de acceso, el equipo o estación de trabajo, los equipos periféricos y los sectores informáticos dentro del servidor que presuntamente están siendo atacados, se ejecutarán comandos que permita identificar con prontitud cuales han sido las acciones invasivas, si fue incorporado un virus al sistema o si es extracción de información. El desarrollo tecnológico podría ser un infinito de probabilidades sobre cada acción establecer una reacción, pero se necesitará desarrollar el panorama completo que establezca la acción-reacción-consecuencia, dicho así los desarrolladores informáticos trabajarán acorde a las consideraciones del Ingenio que permita establecer los protocolos de reacción al presentarse la amenaza, evaluar cuáles serán las consecuencias por la reacción ante el bloqueo o paro total.

4.7. Control estadístico por control de variables

Implementar el método de control estadístico para evaluar los procesos es parte de la gestión administrativa, será útil para medir la calidad actual en sus servicios y así detectar si algún proceso cambio de alguna forma que pueda afectar la calidad. Esta acción se desarrollará siempre con intención de prevención y no de reacción.

Ejecutar el control de variables fortalecerá las acciones destinadas hacia el monitoreo de los colaboradores y sus tareas programadas, no se pueden obtener resultados inmediatos de cada usuario sin poseer su trabajo concluido, pero si es posible medir el desarrollo del mismo diariamente al interpolar la información recabada por tiempo de inactividad sobre el tiempo idealmente programado para concluir ciertas tareas ya asignadas.

4.7.1. Objetivo de control estadístico

Medir constantemente que los procesos asignados sean ejecutados en los tiempos estimados de trabajo, reducir el tiempo de ocio de los colaboradores y medir la velocidad en que el servidor puede operar la información y paquetes de datos que está siendo traslada constantemente.

El objetivo es obtener datos, estos datos podrán ser evaluados con herramientas estadísticas, se proporcionarán diagramas o graficas donde se pueda observar si estos ritmos de trabajo poseen sesgos, actuaron bajo control o sobre los márgenes establecidos, o si fueron un total desperdicios de recurso monetario, con sesgos hacia las zonas negativas de las gráficas acumulando la mayoría de datos que representan innoperaciones, abandonos de puestos de trabajo, empleo de la red para otras actividades o por alertas de bloqueo.

4.7.2. Técnicas empleadas en el control estadístico

El Ingenio podrán emplear un grupo de técnicas de control para la detección temprana, análisis, propuesta de solución y minimización de problemas sobre las áreas de trabajo de interés. Se podrán diseñar con estructura limitada sobre alguna muestra representativa o sobre el conjunto de actividades que se realizan constantemente. La detección de las causas probables de los problemas permitirá comprobar si los factores seleccionados representan las verdaderas causas de los problemas. Se fortalecerá acciones en la toma de decisiones al evitar lazos de amistad o compadrazgos. Se permitirá detectar anomalías en los procesos. Se podrá incorporar el análisis lógico, ordenado y sistemático en la búsqueda de mejoras. El control de operaciones será un mecanismo continuo, donde las herramientas auxiliares del control estadístico permitirán evaluar diariamente los ritmos de producción.

Tabla XXXIII. **Técnicas propuestas**

Técnica	Descripción
Tormenta de ideas	Servirá para identificar las posibles soluciones a cada problema y el conjunto de oportunidades potenciales para alcanzar la mejora esperada.
Diagrama de flujo	Con esta técnica se podrá facilitar la obtención de soluciones al problema desde sus síntomas hasta la posible solución de las causas.
Diagrama de causa y efecto	Se podrá emplear ese método para lograr expresar de forma sencilla la estructura de los problemas complejos con la proyección de la relación causa-efecto de los factores originales.
Diagrama de Pareto	Se puede emplear para disminuir los costos de operación. Se asocia a la mayoría de costos de operación a los defectos en los procesos con atribución a un número pequeño causas, se podrá ajustar al Ingenio, aunque sus procesos de producción no sean tangibles en la oficina administrativa siempre se esperan resultados concretos al concluir el proyecto de ejecución.

Continuación de la tabla XXXIII.

Histograma	Servirá para lograr visualizar de manera rápida las causas de cualquier variación en los procesos asignados, así mismo se deberá reaccionar inmediatamente y tomar acciones correctivas.
Diagrama de dispersión	Se podrá evaluar cuantitativamente los tipos de relaciones de correspondencia entre las variables asignadas o de interés, podría ser el tiempo de inactividad por un usuario.

Fuente: elaboración propia.

4.7.3. Definir la característica de calidad

El modelo de la gestión administrativa velara por incorporar estrategias relacionadas al adecuado modelo de perfilación de los usuarios, monitorear en la red en tiempo real las acciones cotidianas permitirán mitigar los retrasos en proyectos asignados individualmente o colectivamente por área de operaciones, dicho esta la característica de calidad será la reducción de eventos que comprometan las acciones y la vulnerabilidad hacia el sistema interno informático.

Su pilar será la prevención, evaluar la probabilidad del riesgo, proyectar los posibles eventos dañinos hacia los servicios diarios, disminuir la intención que comprometa la honestidad de los colaboradores, supervisores y jefes de área con el trato humano hacia sus semejantes permitirá reforzar la ideología de calidad en el Ingenio.

4.7.4. Selección del grupo racional

El grupo se conformará por las personas que prestan los servicios constantemente al Ingenio, dentro de la selección se conglomeran los cargos y rangos dentro de la empresa para diseñar un solo esquema. Para la ejecución asertiva se deberán incorporar los aspectos de la planificación, control, dirección y organización.

Figura 46. **Mapa para la selección del grupo racional**

Fuente: elaboración propia.

Con el mapa mental se establece para la gestión administrativa suponer que los colaboradores de la empresa incorporarán a su ciclo de trabajo la tendencia en maximizar las utilidades de trabajo presentes con el beneficio de lograr reducir costos de operación y los riesgos hacia su entorno diariamente.

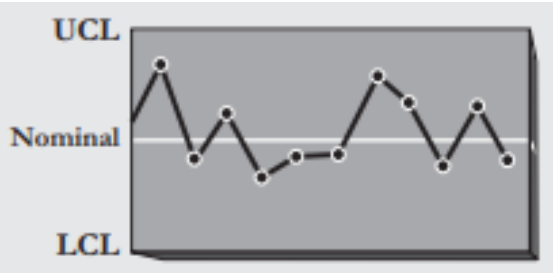
4.8. Elaboración de gráfico de medias y rangos

Cada departamento deberá gestionar por separado el control, monitoreo y manejo de datos estadísticos sobre sus procesos asignados, la elaboración de gráficos permitirá evaluar sobre un periodo de tiempo definido los alcances o debilidades de esos procesos monitoreados. Complementar las gráficas con las nuevas herramientas podría ser complejo o laborioso, la idea central es lograr contener la mayor cantidad de información de los procesos cotidianos, obtener índices de participación de los usuarios conectados a la red y establecer si las metas proyectadas lograron completarse por incidencia de eventos externos a la mala programación o por incompetencia del recurso humano.

4.8.1. Proceso bajo control

Los procesos asignados por departamento deberán ser individualizados y monitoreados por separado. Se podrá considerar que ese proceso en análisis estará bajo control cuando su localización, expansión o forma de distribución no presenta variaciones en el transcurso del tiempo. Si dentro de este proceso surgen causas asignables, deberán ser eliminadas y analizadas.

Figura 47. **Representación de un proceso bajo control**

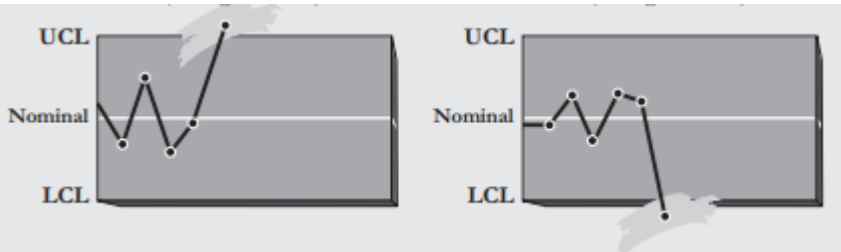


Fuente: CARRO PAZ, Roberto. *Control estadístico de procesos*. p. 10.

4.8.2. Proceso fuera de control

Se basará en los resultados de muestra ubicados fuera de los acotamientos de la gráfica, se visualizará al sobrepasar el límite inferior o el límite superior, el proceso puedo mostrar un sinfín de gráficas, pero será el analista asignado quien determinará el momento y las condiciones que dieron participación a que ocurriera uno o infinitos eventos determinísticos.

Figura 48. **Proceso fuera de control**



Fuente: CARRO PAZ, Roberto. *Control estadístico de procesos*. p. 10.

4.8.3. Análisis de una condición fuera de control

La condición se basará en un conjunto de acciones que dieron vía a que existiera la ocurrencia del evento que ocasiono que ese proceso de incidencia se saliera de control. Se puede estudiar la causa probable que determino se diera la viabilidad de esa condición, un condicionamiento podrá ser analizado se existe o no la probabilidad de ocurrencia. Para ese claro ejemplo se cita el incorporar la tecnología de monitoreo y control la automatización de poder bloquear cada usuario que se encuentre con cuatro minutos de inactividad, eso representaría una condición fuera de control, porque es algo que no se estaría esperando, pero tiene alto porcentaje de que pueda ocurrir el evento.

4.8.4. Estimación de capacidad del proceso

Los resultados estimados son proyectos en base a posibles alcances de producción o de eficiencia sobre los procesos establecidos, la estimación de la capacidad podrá estar limitada por diferentes variables directas o indirectas, las variables directas pueden ser monitoreadas y analizadas, las variables indirectas podrán ser estudiadas hasta que se presenten en los procesos.

La estimación quedará limitada por la capacidad de trabajo de la mano de obra, se podría incorporar a este análisis la capacidad de manejo de información del servidor y la capacidad de desarrollo tecnológico de los programadores que configurarán cada requerimiento ajustado a las exigencias del Ingenio. No solamente estos factores podrán ser parte del análisis, la capacidad de los procesos puede estar limitada por el ancho de banda, protocolos de comunicación entre la computadora y el servidor, así como el manejo de paquete de datos por los analistas y supervisores de área.

4.8.5. Elaboración del gráfico de medias y rangos

Esta técnica y herramienta se empleará para poder asegurarse que dentro de un proceso la variabilidad podrá ser representada bajo control. El analista a cargo de su desarrollo podrá optar con la posibilidad de ajustar la expansión de los límites inferiores o superiores de control modificando el valor Z.

Su enfoque podrá ser útil para establecer equilibrio entre los típicos errores conocidos como “tipo I” y “tipo II”. La elaboración se realzará obteniendo los datos y agrupándolos por columnas, cada columna podría representar el tiempo de observación o los días de interés, para cada fila está asignado un evento o numero representativo este determinará la valoración en ese tiempo *T.*

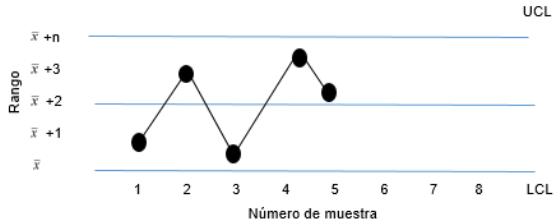
Tabla XXXIV. **Diseño de tabla para la captación y agrupación de datos**

Número de muestra	1	2	3	R	$\bar{x}$
1					
2					
3					
4					
5					
n					

Fuente: elaboración propia.

En las columnas 1,2,3… n+1, se colocarán los datos en sentido vertical descendente, para eso se podrán ir empelando las filas, iniciando en la fila 1 columna 1, cada columna puede representar un periodo de tiempo analizado. Para obtener el rango se calcula restando el valor más bajo del valor más alto. La grafica incorpora $\bar{x}$ diferentes variables que permiten al analista establecer rango apropiados, dentro de la gráfica se presenta el UCL, este valor se representa el mayor valor estimado dentro del procesos, para la parte inferior se incorpora LCL que representa el menor valor que también podría llegar a darse. Para calcular se deberán sumar los datos por cada fila y luego dividirse en el total de celdas presentes. Ese valor ya puede ser asignado a la gráfica y representado por un punto para cada número de muestra.

Figura 49. **Grafica de medias y rangos**



Fuente: elaboración propia, empleando Microsoft Excel 365.

4.9. Administración de controles

Se puede asignar personal calificado que esté a cargo del monitoreo y aplicación de los controles propuestos según el resumen de la figura 32, estos controles están sustentados en la Norma ISO 27001. La intención de la administración de controles es garantizar que sean implementados, ejecutados y validados, que sus fines sean siempre la prevención, automatización y fortalecer el modelo eficiente que desea llegar a poseer el Ingenio.

Tabla XXXV. **Asignación por supremacía de cargos en la administración de controles**

Cargo dentro del organigrama	Tipo de control
Operador	Recopilación y resguardo de la información
Jefe de área	Jerarquía del solicitante
Analista	Protección de las herramientas de auditoría
Analista	Controles de auditoría
Analista	Fuga de información
Operador	Restricción del acceso a la información
Operador	Gestión de contraseñas
Analista	Identificación y autentificación de usuarios

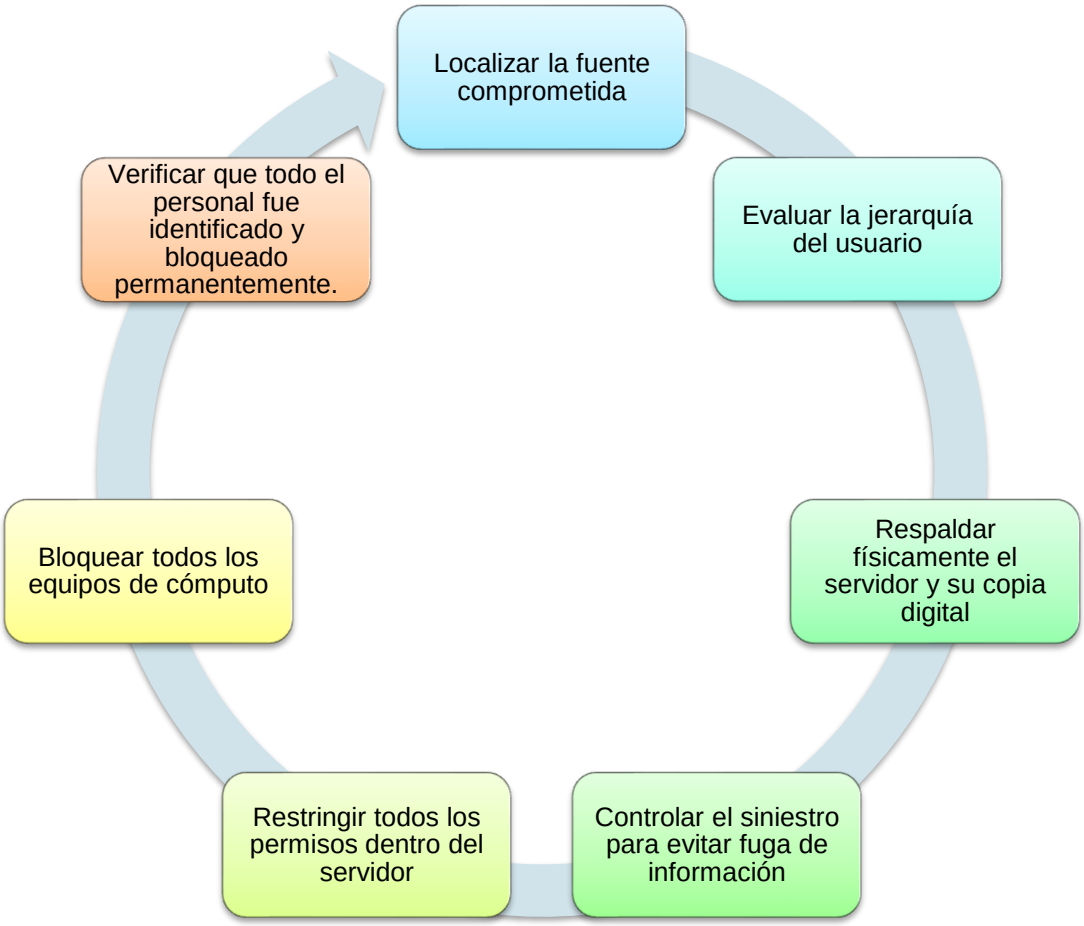
Fuente: elaboración propia.

Estas acciones serán incorporadas, ejecutadas y continuamente realizadas por el rol asignado dentro del organigrama, la idea de establecer este tipo de administración compartida es para delegar responsabilidades y no concentrar en un solo puesto o persona muchas más tareas de las que puede realizar. Se determina que con la asignación de un volumen elevado de tareas administrativas la persona cumple deficientemente con el 60 % de lo establecido, el otro 40 % queda inconcluso.

4.9.1. Procedimiento de contingencia

Si se presenta algún inconveniente con la asignación y ejecución de las tareas programadas en la administración de controles, se podría replicar el procedimiento de contingencia propuesto en la figura 14, pero se adaptaría hacia las acciones que puedan detenerse y comprometa la secuencia de las operaciones.

Figura 50. **Procedimiento de contingencia**



Fuente: elaboración propia.

4.9.2. Plan de comunicación

Incorporará aspectos relevantes sobre los eventos que se presentaron y las acciones implementadas. Se ejecutará el debido análisis interno y externo que permita delimitar responsables y vulnerabilidades. Se podrán definir de esa acción los objetivos del plan, a nivel interno ya se puede tener conocimiento de las personas o autoridades hacia quien será redactado. Se podrá redactar el mensaje con claridad, breve y conciso. Dentro del mismo plan se debe considerar el tiempo y los recursos necesarios, eso servirá de base para desarrollar la estrategia a implementarse. Por último, se deberá evaluar y medir los resultados obtenidos.

Tabla XXXVI. **Estructura del plan de comunicación**

Aspectos a comunicar	Cuándo	Destinatario	Responsable	Metodología
Política de calidad	Nuevas contrataciones	Nuevos empleados	Operador	
Administración de operaciones	Nuevas contrataciones	Nuevos empleados	Operador	
Reglamento interno	Nuevas contrataciones	Nuevos empleados	Operador	
Asignación de rol	Nuevas contrataciones	Nuevos empleados	Operador	
Asignación de usuarios	Nuevas contrataciones	Nuevos empleados	Operador	
Tiempos establecidos para bloqueos de equipos	Nuevas contrataciones	Nuevos empleados	Operador	
Supervisión, control y monitoreo de los equipos	Nuevas contrataciones	Nuevos empleados	Operador	

Fuente: elaboración propia.

La matriz para elaborar el plan de comunicación se presenta como parte de la propuesta, cada aspecto podrá ser sustituido o eliminado, se considera que incorporar esos aspectos relevantes al iniciar los cambios podrá aportar mejoras a todos los colaboradores que interactúen con el sistema de control y sus tareas diarias.

4.9.3. Registro de incidencias

Las incidencias deberán ser comunicadas con los protocolos previamente desarrollados, será enviado por correo hacia los responsables de cada área donde se presentó la falla. Este registro de incidencias deberá ser respaldado y guardado dentro del servidor, con una copia en formato digital en alguna red externa, que no comprometa el historial para ser consultado o evaluado cuando sea considerado necesario.

4.10. Análisis financiero

Se propone emplear un conjunto de cambios en el Ingenio, este conjunto de actos, acciones y cambios necesitarán ejecutar algún plan de inversión, para llegar a ese plan de inversión es necesario conocer el análisis financiero, se podrá representar con valores estimados en costos de contratación de empresas que puedan desarrollar este tipo de proyectos. Pueden considerarse también los costos de infraestructura, compra de equipos de cómputo, compra del servidor, instalación, mano de obra para su instalación, diseño y desarrollo del software raíz donde se configuren los sistemas auxiliares que permitan interconectar los departamentos entre si y los usuarios. Para este tipo de análisis se deberán evaluar propuestas, estimaciones de recursos humanos y sobre todo el tiempo-hombre necesario de los jefes de área para disponer de esa inversión en estudiar la propuesta.

4.10.1. Valor presente neto

Para el desembolso inicial en los cambios propuestos serán considerados los valores estimados de los recursos tecnológicos y su estimado en infraestructura, se podrán evaluar acciones por años de participación. Se empleará un valor de 9 % para el interés.

Tabla XXXVII. **Costos anuales de ejecución he implementación de la propuesta**

Año	Acción propuesta o implementación	Total
1	Compra de servidor, configuración de servidor, trabajo de obra gris, compra de licencias de software, desarrollo de software bajo especificaciones únicas por el Ingenio.	Q 180 000,00
2	Instalación y desarrollo de unidad SOC con el personal necesario.	Q 75 000,00
3	Mantenimiento del servidor.	Q 5 000,00
4	Mantenimiento del servidor.	Q 5 000,00
5	Mantenimiento del servidor.	Q 5 000,00

Fuente: elaboración propia.

Tabla XXXVIII. **Resumen por año de gastos y costos**

Año	1	2	3	4	5
Costo por implementación	180 000,00	75 000,00	5 000,00	5 000,00	5 000,00
Mano de obra	25,000	25,000	0	0	0
Total	Q 205 000,00	Q 100 000,00	Q 5 000,00	Q 5 000,00	Q 5 000,00

Fuente: elaboración propia.

Se estima contratar 8 personas para el año 1 y año 2 con salario base más un porcentaje de comisiones, eso representa los Q 25 000,00.

Formula I:

$$Costo\ total = \text{costo inicial} + \text{costos anuales} * \frac{1}{(1+\text{i})\wedge\text{n}}$$

$$Costo\ total = 205\,000 * \frac{1}{(1+0{,}09)\wedge 1} + 100\,000 * \frac{1}{(1+0{,}09)\wedge 2} + 5\,000 * \frac{1}{(1+0{,}09)\wedge 3} + 5\,000 * \frac{1}{(1+0{,}09)\wedge 4} + 5\,000 * \frac{1}{(1+0{,}09)\wedge 5}$$

Costo total de implementación de la propuesta= Q 282,912,96

Formula II:

Costo promedio anual $= \frac{282\,912{,}96}{5} = 56\,582{,}59$

El costo anual para incorporar la propuesta es Q 56 582,59.

4.10.2. Tasa interna de retorno

Puede ser considerada también como la tasa interna de rendimiento, se tratará de determinar la tasa de interés con la cual el VAN del flujo de ingresos y egresos podría ser cero. Se consideran siempre los 5 años propuestos en el cálculo del valor presente neto. La tasa de interés también será el 9 %.

Tabla XXXIX. **Cálculo de la TIR**

		Tasa de descuento	15 %
Periodo	Flujos netos de efectivo	Valor actual
Año 0	Q 205 000,00	Q 188 073,39
Año 1	Q 100 000,00	Q 84 167,99
Año 2	Q 5 000,00	Q 3 861,00
Año 3	Q 5 000,00	Q 3 543,58
Año 4	Q 5 000,00	Q 3 267,00

Fuente: elaboración propia.

Formula III

$$0 = 188\,073{,}99 * \frac{1}{(1+0{,}09)\wedge 1} + 84\,167{,}99 * \frac{1}{(1+0{,}09)\wedge 2} + 3{,}861 * \frac{1}{(1+0{,}09)\wedge 3} + 3{,}543 * \frac{1}{(1+0{,}09)\wedge 4} + 3{,}267 * \frac{1}{(1+0{,}09)\wedge 5}$$

$$0 = 188\,073{,}99 * (0{,}1481479437) + 84\,167{,}99 * (0{,}21700483568) + 3\,861 * (0{,}3179928658) + 3\,543 * (0{,}4658844887) + 3\,267 * (0{,}6825573153) - 320\,000$$

0 = 0

TIR = 46 % + 1 % $\frac{320{,}000}{282\,912{,}96}$

Para este porcentaje se puede dar como viable y factible el proyecto, esta tasa sobrepasa el 30 % que sería un mínimo aceptable.

4.10.3. Beneficio costo

Se define como la relación obtenida entre los beneficios y los costos del proyecto, generalmente se consideran los valores actuales. Se empleará la tasa de actualización para descontar los flujos de efectivo. Se podrá aceptar si el proyecto de inversión puede representar el B/C mayor que 1. Cuando se considera esta preposición es porque el VAN se presenta en mayor proporción que la inversión inicial por lo cual el VAN deberá ser positivo. Se presumen que por cada año transcurrido serán representados Q 100,000,00 de ganancias anuales, para un beneficio de Q 500,000,00 según datos internos del Ingenio.

Formula IV

$$R = \frac{500\,000}{205\,000} = 2{,}43$$

La relación beneficio/costo demuestra ser mayor a 1, esto indica que por cada Q 1,00 de inversión se podrá recuperar Q 2,43.

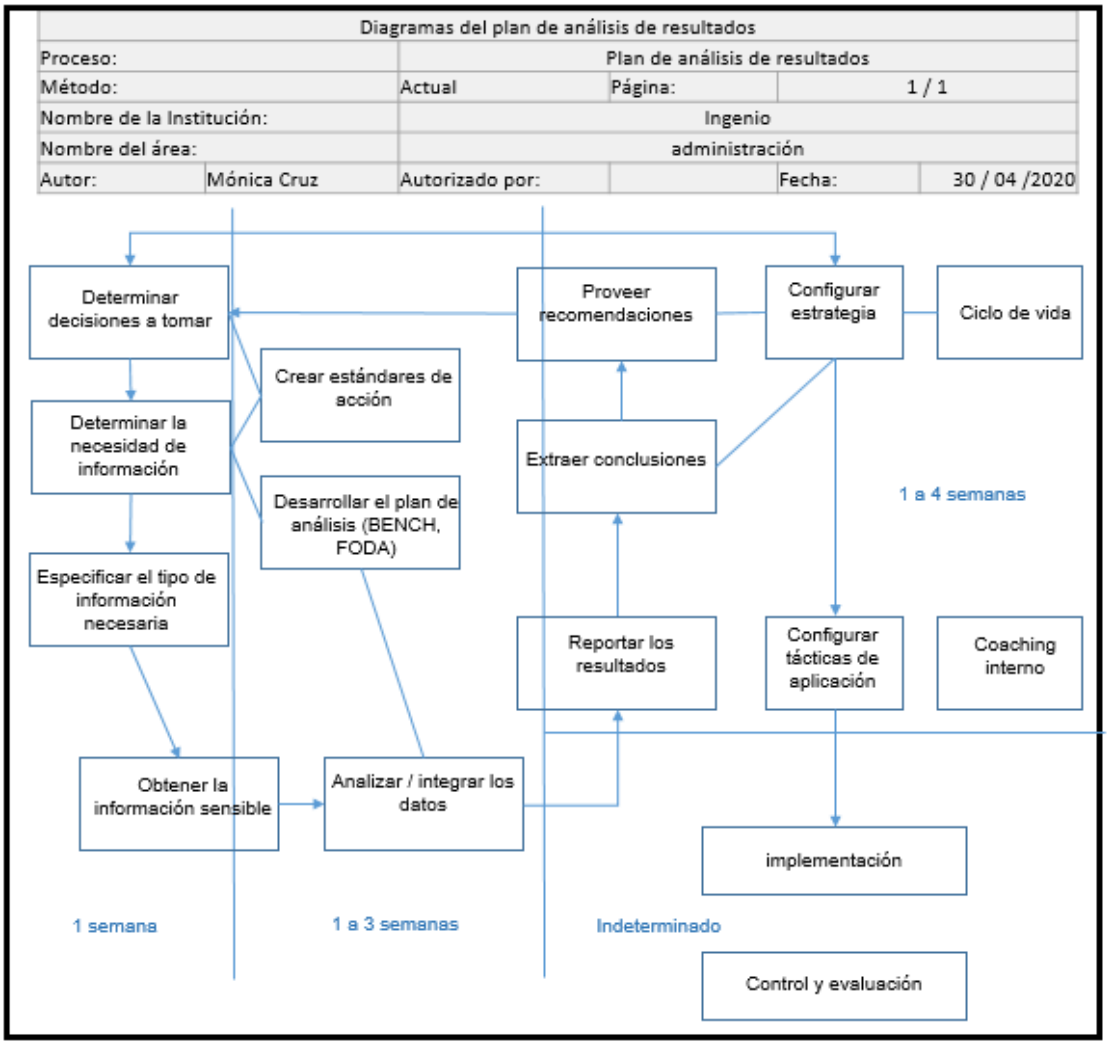
4.10.4. Análisis estadístico

Los resultados sobre cada proceso monitoreado serán representados por las herramientas propuestas en la tabla XXXII, este tipo de análisis demostrará en sus informes que tipo de actividades se desarrollan acorde a la programación y sobre los resultados programados, de existir inconformidades se deberán emitir los informes necesarios hacia las dependencias de interés.

4.10.5. Plan de análisis de resultados

Está acción servirá para que los jefes de área puedan presentar de forma sintetizada los resultados sobre cada acción programada en un determinado tiempo t. Se podrán diseñar para capturar el resumen de cuatro semanas de trabajo continuo, se deberán anotar todas las consideraciones importantes que no lograron cumplirse y por qué no se llegaron a las metas establecidas, de lo contrario se deberá incluir toda la información sobre ajustes y mejoras diseñadas en el transcurso de las operaciones.

Figura 51. **Propuesta del plan de análisis de resultados**



Fuente: RIESTRA, Canek. *El plan de análisis paso a paso.* https://es.slideshare.net/Canek_Riestra/el-plan-de-anlisis-paso-por-paso. Consulta: 25 de noviembre de 2020.

5. EVALUACIÓN Y MEJORA CONTINUA

5.1. Resultados obtenidos

Las debilidades inmediatas fueron expuestas por sus protocolos de seguridad y monitoreo dentro de sus instalaciones, la prevención será el pilar de la propuesta. Cada acción propuesta es de interés relevante y particular hacia el Ingenio. Se pudo determinar que el sistema de monitoreo actual permite que existan infinitas brechas a la seguridad de su información. Los usuarios que se conectan a la red no están sometidos a incorporarse a la red con protocolos estandarizados.

No se llevan registros de los usuarios por cada vez que se conectan, las computadoras de la administración se encuentran vulnerables, no están ancladas a un servidor local, toda la información es trasladada por internet hacia servidores externos. Cuando se presentan brechas de seguridad solo se anotan los resultados obtenidos, por utilizar servidores externos no pueden reaccionar y detener la acción, eso provoca retrasos en el manejo y traslado de información sensible. Esta información debe ser extraída en un dispositivo físico, luego deberá ser trasladada hacia el siguiente punto dentro de sus instalaciones para que se le pueda dar continuidad al trabajo ahí descrito.

Los equipos periféricos tampoco poseen protocolos de seguridad, el Ingenio ha invertido en infraestructura interna considerables sumas de dinero, pero no se han focalizado en concentrar esa inversión en establecer el sistema homogéneo de gestión administrativa, centralizando las operaciones y dividiendo las tareas por áreas y personas responsables.

5.1.1. Interpretación

La baja participación por parte de su alta gerencia en recorrer sus oficinas administrativas podría provocar estos acontecimientos. Cuando el personal traslada reportes sobre quejas o informes de violaciones de seguridad son redactado de forma sencilla en un correo, no tienen diseños o esquemas homogéneos de como redactar un informe relacionado a las malas condiciones en las que se encuentran trabajando.

La duplicidad de funciones es otro factor que destaca, algunos supervisores monitorean a colaboradores de otros departamentos hacia los cuales deberían prestar atención constantemente. Los jefes de cada área no se involucran con los colaboradores de bajo rango, otorgan toda la responsabilidad de solucionar los problemas a los supervisores.

No se posee un departamento de seguridad informática como tal, disponen de agentes de seguridad, pero su tarea es monitorear al personal dentro de las oficinas, no tienen la capacidad o el conocimiento para monitorear los sistemas informáticos sobre el desarrollo de sus tareas programadas o si cada persona que se encuentra frente a una computadora está trabajando o perdiendo el tiempo. Todas estas interpretaciones se pueden transformar en dinero y recursos desperdiciados.

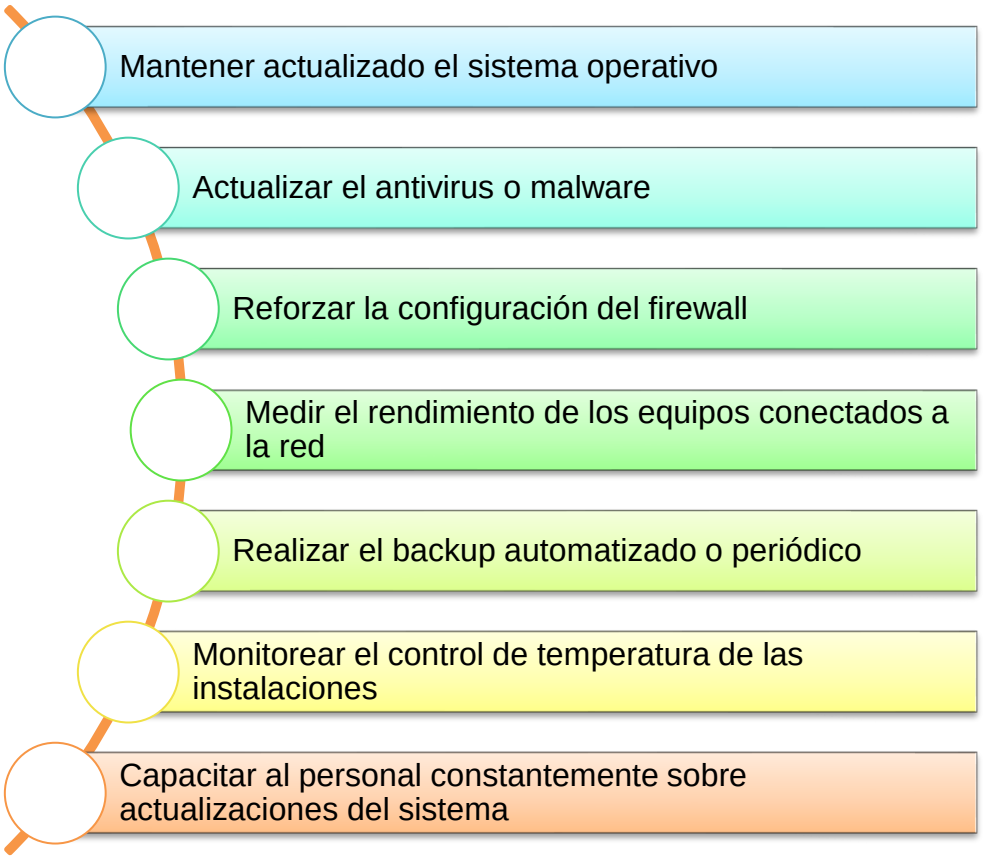
5.1.2. Aplicación

Se obtuvo la medición de la situación actual por realizar visitas continuas, la empresa autorizo por periodo indeterminado asistir a sus instalaciones, además otorgaron permisos especiales para recorrer áreas críticas y de interés hacia ellos para que formarán parte de la propuesta de las mejoras.

5.2. Control y mantenimiento preventivo

Diseñar las tareas de mantenimiento hacia el modelo informático y los equipos conectados a la Web es tarea compartida, se podrá contar con el diseño del proveedor del servidor, los diseñadores contratados para desarrollar la Web interna junto a su interfaz deberán mostrar el plan de seguimiento y mantenimiento preventivo al sistema.

Figura 52. **Tareas del mantenimiento preventivo según el control establecido**



Fuente: elaboración propia.

5.2.1. KPI´S

Las estrategias de medición no pueden ser aún establecidas, los índices medibles podrían ser los derivados del tiempo, empleo de recursos, manejo de personal, reducción de incidentes y optimización de tareas.

Figura 53. **KPI´S propuestos**

Fuente: elaboración propia.

5.2.2. Medidas y aseguramiento de controles

Su función es respaldar el aseguramiento de la eficacia sobre la gestión de los riesgos y el aprovechamiento de su entorno. Luego de centralizar y automatizar partes de la gestión administrativa podría simplificarse la administración de controles internos y promover la colaboración de su recurso humano completo.

Tabla XL. **Medidas y aseguramiento de controles**

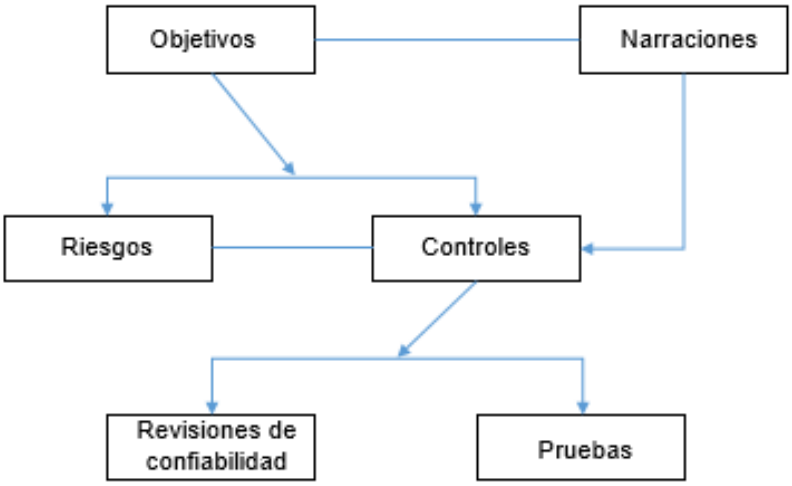
Medida	Controles	Descripción
Configurar su evaluación del riesgo	Configurar una evaluación del riesgo	Se puede elegir entre dos tipos de flujos de trabajo de evaluaciones del riesgo, podrían optarse por auditorías operativas o auditorías integrales.
	Documentar categorías de riesgos	Las categorías de riesgo forman la base de una evaluación del riesgo y también son los contenedores de la organización para el trabajo realizado en una evaluación del riesgo. Cada categoría de riesgo establece la cuestión objeto de examen y cómo se evaluará el rendimiento. Las categorías de riesgo se pueden definir para que el trabajo de monitoreo se pueda dividir en tareas manejables para que los miembros del equipo de auditoría las completen.
	Documentar narraciones	Las narraciones proporcionan una forma de comprender cómo se ajustan los controles internos del Ingenio en el proceso de seguridad y prevención.
	Documentar riesgos y controles	Documentar resultados de riesgos y controles da como resultado la producción de una matriz de control de riesgos (RCM). Una matriz de control de riesgos es una combinación de riesgos identificados y los controles correspondientes (las medidas o cursos de acción sobre cómo se mitigará el riesgo).

Continuación de la tabla XL.

Evaluar el diseño y la eficacia de los controles	Evaluar el diseño del control	Los operadores de primera línea de una organización pueden usar la aplicación control de la misión para administrar los controles a los que tienen acceso, fuera de la aplicación Área de trabajo del riesgo. Control de la misión es una aplicación que presenta información de control desde Evaluaciones del riesgo en una vista simplificada y centralizada.
	Definir el plan de pruebas	El plan de pruebas identificará como se probará el control de medidas de seguridad establecido. Se podrá definir el plan de prueba para especificar el método de prueba, el tamaño total de la muestra y los diferentes pasos de prueba que deberán realizarse para probar el control.
	Evaluar la eficacia del control	La evaluación de la efectividad del control implica documentar los resultados detallados de las pruebas y especificar si el control fue aprobado o no. Una vez que haya terminado de evaluar la efectividad del control, puede marcar porciones de texto y enlazarlas con la evidencia, como manuales de políticas o procedimientos, normas, acuerdos del nivel de servicio (SLA)/especificaciones del nivel de servicio (SLS) y contratos.
Demostrar aseguramiento	Las evaluaciones del riesgo brindarán la capacidad de agregar automáticamente evaluaciones del riesgo, los resultados de esas pruebas en toda la evaluación del riesgo en una sola medida porcentual se podrán utilizar para reportes. El aseguramiento podrá incrementar proporcionalmente con las revisiones de confiabilidad y las pruebas aprobadas.	

Fuente: elaboración propia.

Figura 54. **Diagrama de evaluaciones del riesgo**



Fuente: elaboración propia.

5.2.3. Control de los datos fuente

Las acciones destinadas al control son supervisadas por el departamento de mayor jerarquía establecido. Si el Ingenio decide incorporar el departamento SOC, ellos serán los responsables del resguardo y manejo de toda la información. Los datos fuente son obtenidos del procesamiento de la información constante, por eso el modelo de gestión administrativa propone captar la información total en formato 24 x 7 x 365. No se podrá acceder a la base de datos sin autorización con credenciales específicas.

5.2.4. Control de almacenamiento de información

El total control se llevará a cabo por los departamentos de informática o la unidad SOC. Se deberá priorizar según el rol establecido dentro del servidor, pero se tiene que delimitar que dependencia marca supremacía sobre esta acción. Se

entenderá como control sobre la información poder estandarizar ciertos procesos de almacenaje por tipicidad de ocurrencia.

Si los datos enviados son relevantes con resultados esperados o solamente son datos obtenidos por procesamiento de información, cada resultado obtenido tendrá que ser automáticamente guardado además de su proceso involucrado, la programación estandarizada promueve la cultura de monitoreo y resguardo de acciones parentales según las tareas asignadas por cada puesto dentro del organigrama de la empresa. Los accesos de control de almacenamiento también serán debidamente establecidos con los permisos y protocolos de ingresos previamente desarrollados por los jefes del departamento de informática o de la unidad SOC.

5.3. Auditorías

La auditoría es el tipo de acción destinada a recopilar datos, está integrada en un proceso estructurado. Cuando sea necesario, se podrán realizar estudios para verificar los datos, en particular cuando los datos son derivados de juicios y opiniones.

Las auditorías aseguran la precisión de los datos y la eficacia del sistema de gestión. Se realizan autoevaluaciones y los resultados se utilizan para determinar la madurez del Ingenio y mejorar su desempeño global.

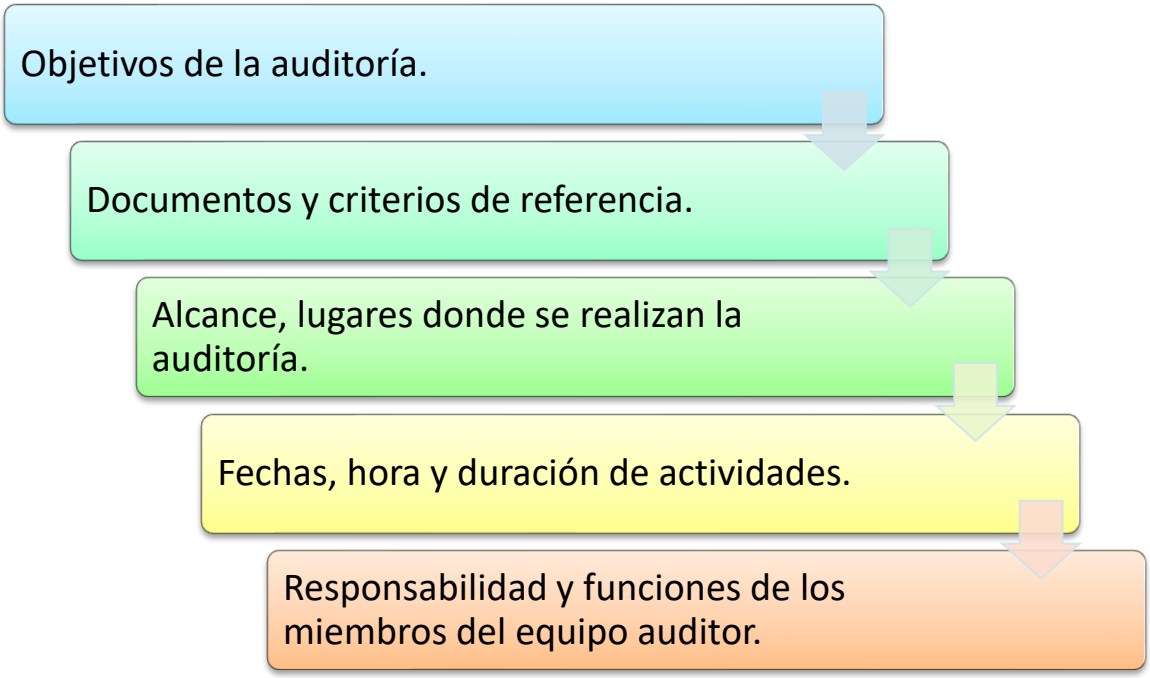
5.3.1. Plan de auditorías

El plan de auditoría será elaborado por el supervisor de ejecutar esas actividades. La elaboración deberá ser diseñada de acuerdo al departamento o área que será auditada y establecerá la guía de los horarios con las necesidades existentes de la coordinación entre todas las partes involucradas.

El plan de auditoría deberá contener el tipo de auditoría que se desarrollará, el alcance deseado y la complejidad involucrada. La naturaleza del plan de auditoría es dinámico, describiendo así que no será conformado por un solo documento estático. Se deberá evolucionar acorde a las necesidades y el contexto del departamento en análisis.

Todos los documentos que conforman el plan de auditoría deben tratarse de forma adecuada, se deberán resguardar de cualquier acción que comprometa su ejecución y la obtención de datos en ella consignados. El plan de auditoría garantiza beneficios y ventajas que afectan de forma positiva los departamentos de interés, destacando la identificación de fallas existentes en diferentes procesos, promoviendo acciones correctivas y preventivas o la incorporación de mejoras continuas en sus procesos organizativos.

Figura 55. **Elementos del plan de auditorías**



Fuente: elaboración propia.

Para desempeñar las mismas acciones, pero con diferentes objetivos en cada auditoría, se podrán incorporar plantillas pre diseñadas que permitan a los auditores o a los jefes de área entender con claridad que es lo que se busca por cada instrumento involucrado. La plantilla estará determinada por un conjunto de recuadros o áreas con datos repetitivos, la separación de filas y columnas necesarias para anotar cada hallazgo, si el auditor considera útil acompañar una fotografía se podría utilizar la parte trasera de la página para imprimir ese tipo de recurso.

5.3.1.1. Auditorías internas

Son procesos sistemáticos, independientes y documentados donde se evidencia y evalúa de manera objetiva con el fin de establecer la extensión o duración en que se cumplen los requisitos del sistema de gestión de calidad.

Se deberá asignar una persona ajena al departamento o área de interés, deberá conocer claramente cuáles son los procesos y tareas que se realizan en el área de incidencia, esta persona asignada deberá diseñar sus propias hojas de ruta o lista de chequeo, eso le servirá para comprobar y documentar que todo lo evaluado se realiza según los procesos establecidos.

Cualquier falla, desviación o proceso fuera de control será anotado como una no conformidad del sistema, para eso es necesario llenar la plantilla de formato previamente diseñado con eso se esperaría demostrar las evidencias del proceso.

Tabla XLI. **Procedimiento de las auditorías internas**

Secuencia	Descripción
Requisito	El motivo por el que los auditores no deben auditar su propio trabajo, se debe a que las personas que están realizando constantemente una actividad, la conocen tan bien que pueden pasar por alto cosas en las que nunca han pensado y que un tercero puede detectar mejor y, por otra parte, su implicación puede impedirles una ponderación objetiva.
Frecuencia	Las auditorías internas generalmente se realizan una vez por año, y son planificadas por el responsable de gestión de calidad de modo que el informe de los resultados obtenidos esté preparado con tiempo suficiente para su presentación en la revisión del sistema de gestión de calidad del Ingenio.
Criterios de auditoría	Son los especificados para cada departamento o proceso auditado.

Continuación de la tabla XLI.

Diseño	La auditoría interna anual se divide en varias auditorías. Una auditoría general que se realizará al sistema de gestión de calidad para verificar que cumple con cada uno de los requisitos dispuestos por la norma y otras dirigidas a cada uno de los procesos que forman parte del sistema. Esta labor debe ser revisada o auditada cada tres años durante la auditoría de tercera parte, de certificación o renovación, por parte de una entidad independiente.
Ejecución	Llegada la fecha de la auditoría, el auditor interno informa al responsable del área a auditar sobre la finalidad de la auditoría y sus etapas. Luego procede a ejecutar la auditoría en compañía del responsable del área. Se va analizando y valorando con ayuda del formato, cada uno de los requisitos indicados. Conforme se descubran evidencias de incumplimientos o posibles mejoras, estas serán anotadas por el auditor y comentadas con el responsable del área.
Conclusiones de la auditoría	El auditor elabora el Informe de la Auditoría Interna donde registra las deficiencias encontradas. El informe de la auditoría se realiza de común acuerdo con el responsable del área auditada y sus participantes de forma que se cause un reconocimiento colectivo de la situación como a la vez la aceptación de la necesidad de aplicar las medidas correctivas que sean acordes a la situación. El director del área, firma el informe, se queda con una copia que sirve para analizar las siguientes acciones correctivas.

Fuente: elaboración propia.

5.3.1.2. Auditorías externas

El entorno empresarial es complejo y la cantidad de operaciones con sus procesos que se desenvuelven son muchísimos, sobretodo en empresas que ya tienen una dimensión suficientemente grande y operan a nivel internacional. Es aquí cuando suma importancia el concepto de auditoría para poseer un mayor control sobre la empresa.

Las empresas deben tratar de tener todas las brechas atadas y cumplir con la normativa exigida en cada uno de sus procesos internos, para que en caso de que se realice una auditoría externa, el resultado sea favorable. De todos los tipos de auditoría que se puede encontrar, esta es una de las temidas por las empresas ya que las realiza una persona independiente de la empresa.

La auditoría externa o independiente consiste en que una empresa ajena supervise que los estados financieros de una organización cumplan la normativa específica. A través de la auditoría externa se realiza un análisis y control exhaustivos por parte de un auditor, que es totalmente ajeno a la actividad de la empresa, con el objetivo de emitir una opinión imparcial e independiente sobre el sistema de operación de la empresa y su control interno. Además, a través de la auditoría externa, se formulan sugerencias de mejora de la organización.

El dictamen que nace como resultado de la auditoría externa tiene plena validez y trascendencia frente a terceros, un documento que se da bajo la figura de la fe pública, teniendo total credibilidad y estando verificada toda la información en él reflejada.

La auditoría externa se ejecuta a requerimiento de organismos oficiales, clientes u organismos de certificación (organizaciones privadas que certifican el cumplimiento de una norma de referencia).

Esta auditoría externa puede subdividirse del siguiente modo:

- Auditorías de segunda parte. Solicitadas por un cliente de la empresa auditada, que le sirva de información previa a la realización de una compra o contratación para corroborar que realmente la empresa cumple con los requisitos legales.

- Auditorías de tercera parte. Ejecutadas por una tercera parte independiente de la empresa auditada.

5.3.1.2.1. Evaluación de controles de accesos

Esta tarea podrá ser desarrollada por un conjunto de actividades y acciones propuestas para apoyar el monitoreo y análisis del recurso humano que trabaja constantemente según su rol otorgado y privilegios asignados.

Tabla XLII. **Control de acceso**

Responsable	Controles	Riesgo	Actividad
Informática	Definir políticas de acceso a las instalaciones	Perdida de información originado por acceso no autorizado al centro de cómputo.	Gestión de acceso a equipos de cómputo.
	Registrar en la bitácora de seguridad todo ingreso al sistema.	Daño de equipos originado por ingreso no autorizado al sistema.	
	Registrar en video las áreas que cuentan con equipos de cómputo.	Fuga de información originada por acceso no autorizado a los equipos de cómputos.	

Continuación de la tabla XLII.

Analista de seguridad	Revisar permisos a usuarios sobre la configuración e instalación de software.	Sanciones legales originado por instalación de software no licenciado en los equipos.	Administración de permisos a perfiles para la instalación de software y manipulación de configuración
	Revisar procedimientos y permisos para la de instalación de software.	Daño en configuración de equipos originada por instalación de software no permitido, o manipulación de la configuración	
	Revisar políticas de caducidad de contraseñas.	Perdida de información originada por falta de configuración de profile	
	Configurar políticas de profile.	Fuga de información originada por contraseñas compartidas de red.	
Informática o unidad SOC	La creación de usuarios se inicia desde la dirección de Interventoría a través de solicitud por correo electrónico.	Fuga de información por ingreso a la aplicación por parte de personal no autorizado	Control de accesos
	Solicitar uso de credenciales una vez transcurridos 30 minutos	Robo de información por uso de sesión activa en el aplicativo	
	Ocultar la contraseña a medida que se digita	Robo de contraseña por observación al digitar	

Continuación de la tabla XLII.

	Retirar inmediatamente las identificaciones de los usuarios que han dejado la organización	Pérdida de información por ingreso al aplicativo de personal retirado de la organización	
	Deshabilitar o retirar inmediatamente los permisos de usuario que no corresponden con el cargo en la organización	Daño de información por acceso no autorizado a perfiles no definidos para el cargo	
	Revisar e incluir en los términos de la contratación cláusula de confidencialidad de la información que se maneja a través del sistema.	Fuga de información por ausencia o debilidad en la declaración de confidencialidad	
	Verificar la identidad del interventor antes de proporcionar una nueva contraseña o restablecer la existente	Pérdida de información por falta de verificación de la identidad al momento de restablecer contraseñas	

Fuente: elaboración propia.

5.3.1.2.2. Aseguramiento de manejo de aplicaciones por usuario

Se podrán cumplir las acciones luego de ser implementados sus protocolos y programas de prevención de riesgos, las aplicaciones autorizadas para los usuarios dependerán del diseño original con sus credenciales incorporadas al programar el servidor.

Este aseguramiento se verá afectado por diseños ineficientes, duplicidad de usuarios, asignación de tareas no estimadas para un determinado usuario, mala ejecución de auditorías y por errores humanos comúnmente comprometen las relaciones laborales cotidianas. Las aplicaciones asignadas para cada usuario serán directamente proporcionales al perfil asignado desde su contratación por el departamento de recursos humanos. El adecuado manejo permitirá disminuir problemas de navegación y uso de recursos destinados para desarrollar sus tareas programadas.

5.4. Aseguramiento del cumplimiento de auditorías

Para obtener el aseguramiento de las auditorías diseñadas, se deberá establecer un sub procero de monitoreo diseñado para garantizar que las políticas y procedimientos relacionados con el sistema de control de la calidad sea relevante, adecuado y esté operando efectivamente.

Ese proceso debe incluir evaluación progresiva dentro del propio sistema de control de calidad, incluyendo la revisión de la muestra de trabajos concluidos. Se requiere que el proceso de monitoreo sea asignado a una persona con experiencia y autoridad para asumir la responsabilidad necesaria. Se requerirá que los involucrados en la revisión sean independientes, que no hayan

participado en el trabajo ni en cualquier otra revisión de control de calidad del trabajo.

Se necesitará incluir la posibilidad de manejo de cambios en los sistemas de planificación y control, como la visión, misión y objetivos o estrategias, así como cambios del organigrama, de sus relaciones o de normas para el desempeño de las dependencias o directivos o el abordaje de los procesos medulares de un sistema de aseguramiento de la calidad.

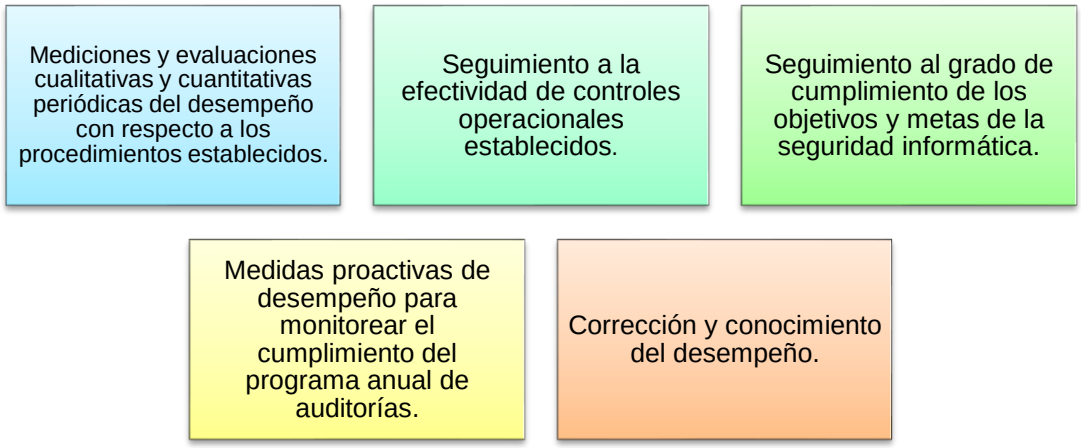
El establecimiento de un sistema de gestión de la calidad dentro de las acciones cotidianas, deberá ser compatible con cualquier tipo de estructura departamental, y puede tener impacto en la forma como están agrupadas las unidades que dan forma al organigrama de la organización, y que permiten concebir de manera precisa aquellos procesos claves para agregarle valor a las auditorías internas.

5.4.1. Evaluaciones periódicas de controles

Ejecutar este tipo de acción permitirá a la empresa obtener datos sobre las mediciones y seguimiento del desempeño de la gestión administrativa. Para evaluar los indicadores se deberá apoyar en documentos como registros de inspecciones, registros de auditorías, registro de reuniones de seguridad, estadísticas mensuales y estadísticas anuales como índices de seguridad y reportes de investigación de incidentes.

Se deberá evaluar periódicamente el avance de cumplimiento de los indicadores establecidos para luego diseñar planes de acción que promuevan la mejora continua.

Figura 56. **Alcances y beneficios esperados por las evaluaciones periódicas**



Fuente: elaboración propia.

5.4.2. Cumplimiento de observaciones y recomendaciones

Trabajar apegado al contexto del Ingenio garantizará el cumplimiento de cada etapa diseñada para incorporar el nuevo modelo de gestión administrativa. Se puede desarrollar cada recomendación por valoración de incidencia dentro del propio modelo de gestión, se podría priorizar la tabla que incorpora las propuestas de la Norma ISO 27001. Cada observación tiene que ser evaluada por los jefes de área, quienes decidirán si cumple con los prototipos diseñados en función de la asignación de perfiles, usuarios, roles y credenciales de accesos.

El cumplimiento no se verá afectada por ejecutar parcial o totalmente el proyecto completo, serán totalmente independientes, cada observación o recomendación está validada de múltiples factores evaluados, pero los contextos

completos de los niveles de seguridad informática proveerán una red completa que respaldará cada acción asignada al sistema raíz.

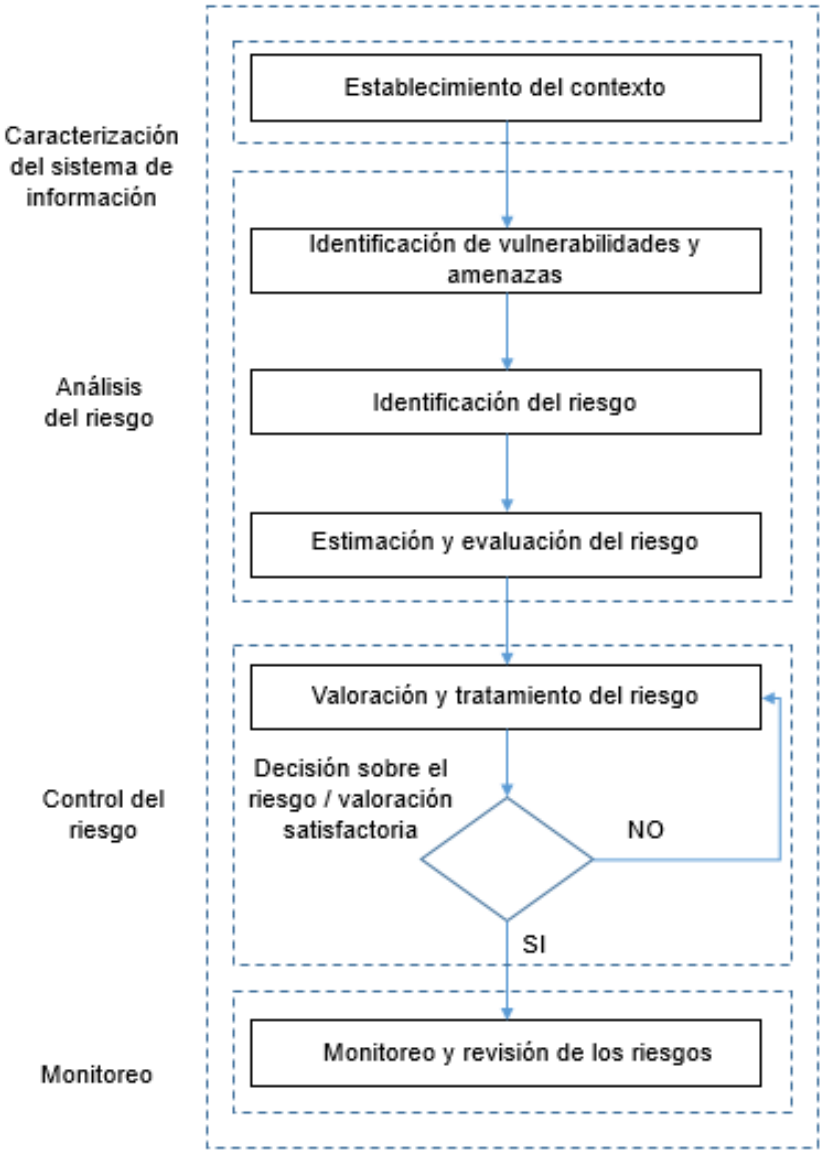
Se podría puntualizar que las recomendaciones y observaciones fueron expuestas por la recolección y recopilación de información interna, no se posee información sensible que aumente el nivel de criticidad hacia las acciones que podrían aventajar los recursos disponibles, para estas observaciones trazadas se puede destacar que el control, asignación y monitoreo de los usuarios es la pieza central. Medir las acciones continuas y cotidianas es otro factor relevante que muestra una señal de alerta, por medio de estas acciones se pueden cuantificar tiempos efectivos de trabajo, interrupción en los trabajos asignados.

No se podrán realizar tareas sesgadas sobre el diseño original, se exceptúa en la regla cuando los jefes de área otorguen permisos especiales luego de un proceso de análisis, deliberación y aceptación.

5.5. Plan de mejora de riesgos

Se puede emplear la mezcla de diagnósticos, seguimiento y evaluación de riesgos. Para este tipo de metodología será necesario incluir el diagnostico de seguridad mediante la aplicación de lista de chequeo, incorporar análisis de riesgos aplicando la Norma ISO 27001 y con el escaneo de vulnerabilidades constante.

Figura 57. **Diagrama para incorporar el plan de mejora de riesgos**



Fuente: ALFARO VIANA, Ivan Andrés. *Diseño del plan de seguridad informática del sistema de información misional*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2743/Trabajo%20de%20grado3023.pdf?sequence=1&isAllowed=y. Consulta: 19 de noviembre de 2020.

5.5.1. Acciones correctivas en riesgos administrativos

Estas acciones dependerán del tipo de falla ocurrida, se puede ponderar el nivel de riesgo dentro del organigrama de la empresa. Si la falla ocurre a niveles inferiores se podrán ejecutar los bloqueos ya propuestos, limitando los privilegios del usuario o del computador donde se ha detectado el problema. Pero si el problema se presenta en la parte superior de la organización la acción que pueda solucionar el problema deberá ser consultada con sus similares dentro de la empresa.

El nivel de riesgo estará dado en la proporción de que se comprometa la información y en el porcentaje de acceso de la brecha ocasionada, si estas acciones se presentan con alto nivel de agresividad, la mejor acción será detener por completo las labores y buscar la fuente del problema.

5.5.2. Diagnóstico de incidencias por departamento

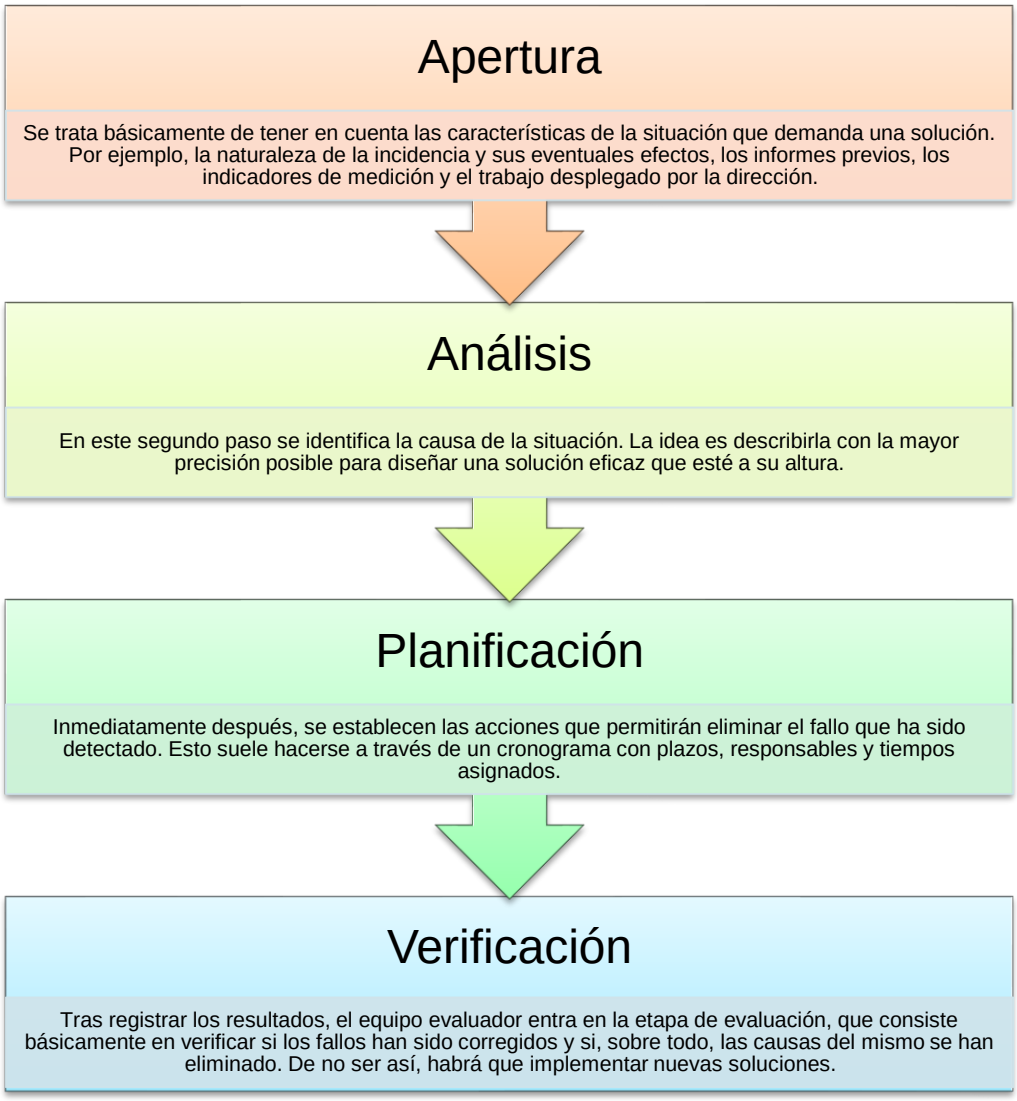
Los diagnósticos serán realizados al concluir una falla, o por un conjunto de alertas que el programa ha recolectado en algún determinado tiempo. Esta tarea permitirá obtener datos relevantes acerca de los incidentes que se presentaron, empleando los histogramas de frecuencia sería simple evaluar los eventos y los daños ocasionados.

Se espera que los diagnósticos de incidencias permitan mejorar la programación semi automatizada en la Web interna, todo tipo de incidencia deberá ser evaluada, aunque no representó amenaza critica en el tiempo de su ocurrencia, deberá ser analizada para considerar que fue lo que la ocasiono y porque llego a ocurrir. Parte esencial en el diagnóstico de incidencias es trabajar con supuestos, de lo que pudo provocarlo y lo que no pudo detenerlo.

5.5.3. Método de detección de problemas

El método se compondrá de cuatro aspectos o líneas de interés, con el trabajo conjunto se espera que la detección de problemas sea tarea fácil.

Figura 58. **Método de detección de problemas**



Fuente: elaboración propia.

5.6. Seguimiento de plan de mejora

El seguimiento se podrá ejecutar solamente sí Junta Directiva aprueba el conjunto de acciones propuestas, además de aprobar la restructuración en ciertas áreas donde se presentan la mayor concentración de debilidades y errores humanos.

No se fija como un modelo impositivo el aplicar las mejoras, solamente se plantean soluciones viables que pueden mejorar los procesos he incrementar los resultados que promuevan los beneficios a un colectivo de usuarios asignados a una misma Web o red interna.

Para el seguimiento podría incorporarse el uso y formulación de un cuadro de mando integral, el Ingenio podrá continuar construyendo sus indicadores en torno a las perspectivas claves, se podrán logar incorporar algunos aspectos que pueden ejecutar el seguimiento profesional y adecuado para el plan de mejora.

Tabla XLIII. **Cuadro de mando integral**

Acción	Descripción
Perspectivas	Áreas de interés que tiene una empresa, para desarrollar los objetivos estratégicos e indicadores.
Porcentaje de importancia estratégica de la perspectiva	Porcentaje establecido para cada una de las perspectivas, teniendo en cuenta su impacto.
Objetivos estratégicos	Resultados esperados por la empresa en a largo plazo, los cuales permiten que la operación se lleve a cabo.
Proceso	Áreas de la organización.
Indicador	Variables cuantitativas o cualitativas que permite observar el comportamiento de un proceso respecto de las metas esperadas.
Descripción	Detalle de cada indicador.

Continuación de la tabla XLIII.

Variables relacionadas	Término del indicador.
Sistema táctico	Porcentaje de importancia establecido por la empresa dentro de la perspectiva.
Meta	Valor que da la referencia al cumplimiento para cada indicador.
Valor obtenido	Resultado de la medición.
Relación de resultado	Valor obtenido en la medición, sobre la meta definida.

Fuente: elaboración propia.

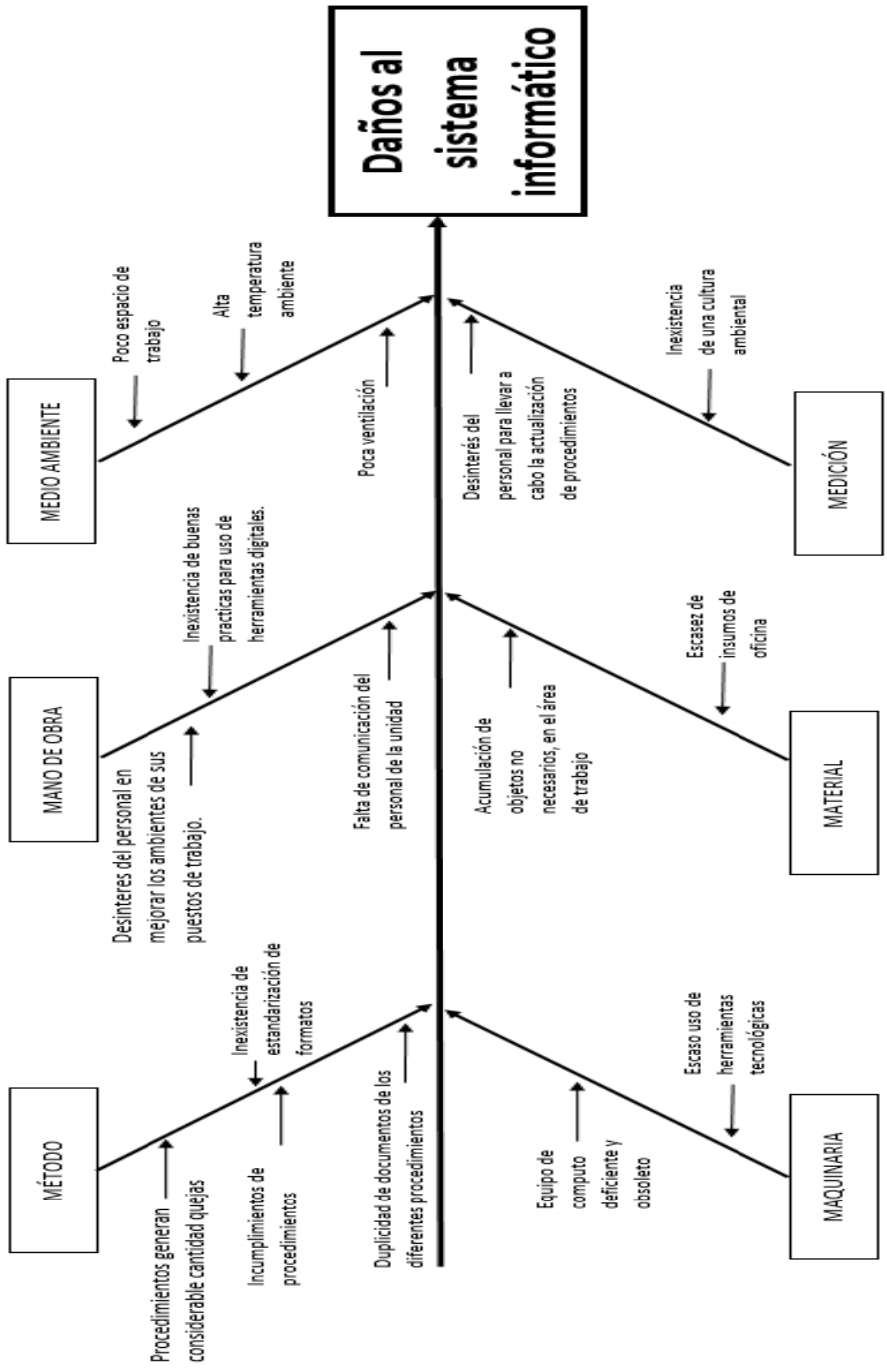
5.6.1. Identificar causas del problema

Los problemas son los resultados de diferentes debilidades dentro del sistema de gestión administrativa, existirán infinitas causas determinantes, algunas podrán ser causadas por errores humanos, otras por debilidades del propio de sistema administrativo y otras por fallas dentro del sistema operativo con el que se trabaja en el Ingenio.

La identificación temprana de las causas permitiría que los problemas no llegarían a ocasionar daños considerables en el trabajo cotidiano, para la identificación de las posibles causas de los problemas podría emplearse el diagrama Ishikawa identificando las posibles causas según el medio de donde será analizado.

Crear esta herramienta permitirá al analista ir separando causas viables o causas con menor oportunidad de incidencia, no se podrán descartar por ilógicas que parezcan las causas menos esperadas, cada diagrama podrá desarrollarse para cada problema que se presente.

Figura 59. **Ishikawa para identificar causas de un problema**

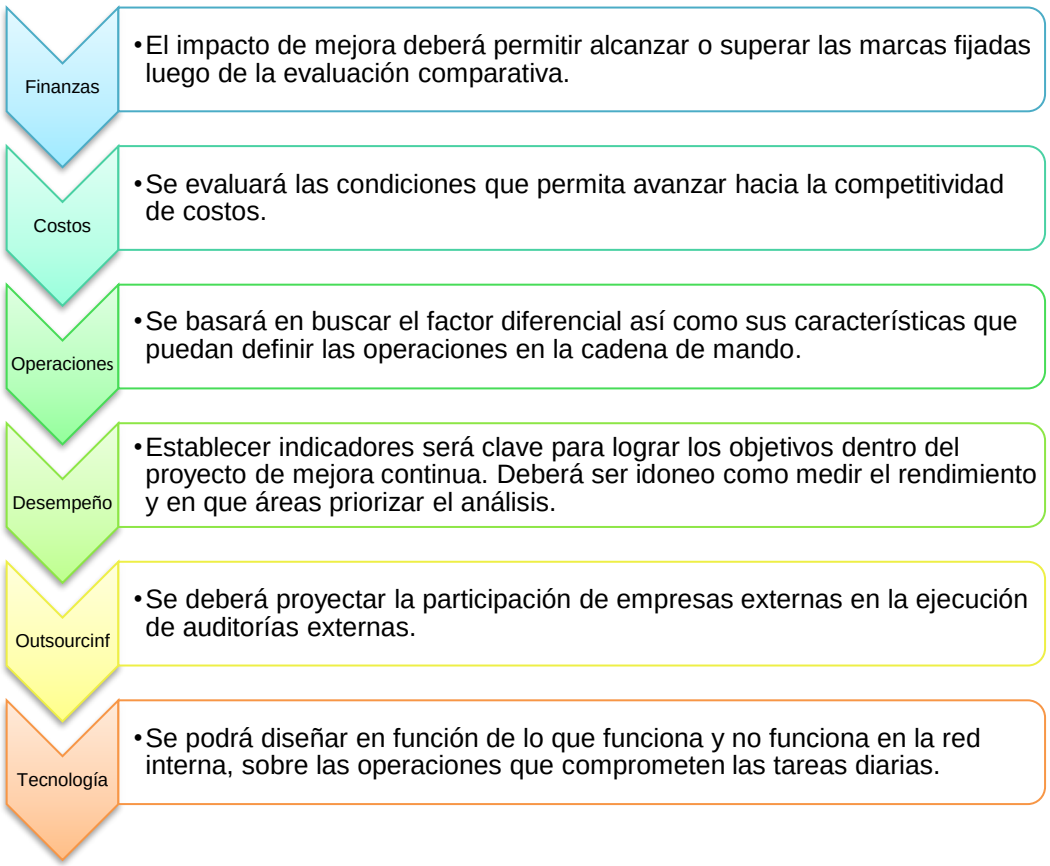


Fuente: elaboración propia, empleando Visio 2016.

5.6.2. Formulación de objetivos

Para la formulación de objetivos en el plan de mejora continua, se podrá fundamentar sobre la evaluación realizado en un determinado tiempo futuro, las condiciones actuales propician diseños de objetivos actuales, las variaciones y fluctuaciones en diferentes segmentos internos por separado permitirán que la empresa logre obtener resultados positivos o un total colapso por no ejecutar las modificaciones apegados al plan propuesto.

Figura 60. **Áreas de análisis para la formulación de objetivos**



Fuente: elaboración propia.

5.6.3. Realizar planificación y seguimiento

La planificación podrá ser diseñada a partir del visto bueno del Ingenio para incorporar las mejoras propuestas, el seguimiento de cada tarea aprobada será parte fundamental del cronograma de actividades que permita monitorear los avances y la lista de precedencia completa. Esta nueva planificación podrá ser diseñada por los supervisores de área y trasladada a junta directiva para que sea evaluada por los jefes de área, luego de ser aprobada la planificación deberá ser divulgada y compartida en las personas que formarán parte de esas actividades.

5.6.4. Seleccionar acciones a mejorar

Las acciones principales que podrían mejorar los procesos administrativos y poder incorporar paulatinamente la propuesta diseñada será por medio de algunas acciones tempranas, se sugiere aplicar diferentes herramientas.

Tabla XLIV. **Acciones que deben mejorar**

	ITEM
•	Planificación estratégica y operativa
•	Análisis y rediseño de procesos
•	Cuadro de mando integral
•	Aprendizaje de mejores prácticas de monitoreo

Fuente: elaboración propia.

CONCLUSIONES

1. Las fallas que destacaron con la recolección de datos son por el mal manejo de los programas informáticos, el factor que destaca es la falta de automatización en los procesos y la creación de usuarios con permisos establecidos según su rol y perfil asignado.

2. Los riesgos principales se presentan con la sustracción de información sensible del Ingenio, la falta de mecanismos que permitan alertar cuando ocurren brechas al sistema informático, la falta de mecanismos digitales que emitan alarmas tempranas cuando existe la vulneración y no esperar hasta que transcurra un tiempo prolongado para poder encontrar el problema.

3. Sus protocolos de asignación de usuarios son deficientes, no poseen servidor propio en el edificio, esto permite que se utilicen plataformas externas para manejar la información interna y por medio de esas plataformas se crean usuarios sin control alguno, los procesos productivos no son monitoreados sistemáticamente, solamente se obtienen datos al concluir el ciclo de trabajo programado.

4. Los controles que se presentaron podrán mejorar las acciones diseñadas para establecer los controles de seguridad informática, se presentó el modelo básico fundamentado en la Norma ISO 27001.

5. Las auditorías con que desempeñan los monitoreos en las oficinas son deficientes y esporádicas, no poseen programación, el personal que las realiza no tienen conocimientos específicos sobre los temas o actividades que están evaluando al ejecutar estas tareas.

RECOMENDACIONES

1. Incorporar el nuevo servidor a las oficinas administrativas podría reducir los índices de fallas, con esa acción se dará inicio a un nuevo concepto de automatización en asignación de tareas de los colaboradores, previo a eso de deberán crear los usuarios tal y como se propone en el capítulo tres, se asignarán los permisos conforme el perfil del usuario y su rol dentro de la organización.

2. Incorporar por la alta gerencia las modificaciones de la empresa incorporar la unidad SOC, con ese modelo de personal y tareas de monitoreo 24 x 7 x 365 se reducirán a su mínima expresión las brechas de seguridad, se garantiza que ante la eventualidad de una posible amenaza se reaccionara con alerta temprana emitiendo la señal de alarma el Software contenido en el SUM Server.

3. Asignar a los usuarios el trabajo en conjunto por los departamentos de recursos humanos quienes detallarán las especificaciones de cada puesto dentro de la organización, luego será trasladado al departamento de informática quienes deberán configurar desde el sistema raíz las credenciales y permisos necesarios por cada usuario según el perfil trasladado por recursos humanos y el rol que tendrá diariamente.

4. Controlar la asignación de monitoreo por atributos forma parte del organigrama de la unidad SOC, asignar tareas preventivas a un operador es tarea sencilla, pero asignar tareas reactivas a los analistas es donde erradica la complejidad del sistema, quedará a interpretación del analista

si se podría presentar un falso positivo o se estaría bajo asedio de una brecha de seguridad.

5. Programar las auditorías internas como mínimo una vez al mes, tienen que ser objetivas, sin sesgos por amistades internas y con la intención de poder recolectar información que demuestre si este apto continuar trabajando con el modelo ya adoptado, o será necesaria realizar ajustes a corto plazo.

BIBLIOGRAFÍA

1. ALARCÓN ÁVILA, Rodrigo. *Implementación de un modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos*. [en línea]. <http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2694/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y>. [Consulta: 22 de mayo de 2021].

2. ALFARO VIANA, Ivan Andrés. Diseño del plan de seguridad informática del sistema de información misional. [en línea]. <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2743/Trabajo%20de%20grado3023.pdf?sequence=1&isAllowed=y>. [Consulta: 19 de noviembre de 2020].

3. CARRO PAZ, Roberto. *Control estadístico de procesos*. Argentina: Universidad Nacional de Mar de Plata, 2011. 25 p.

4. CHIAVENATO, Idalberto. *Administración de recursos humanos.* Colombia: McGraw-Hill. 2001. 721 p.

5. CIFCO. *Plan de contingencia equipo informático*. [en línea]. <https://www.studocu.com/en-us/document/navarro-college/computer-organization/plan-de-contingencia-para-equipo-informatico-2014-r2/17908576>. [Consulta: 15 de junio de 2021].

6. elandroide. *9 claves para documentar correctamente una incidencia.* [en línea]. <https://elandroidefeliz.com/9-claves-para-documentar-correctamente-una-incidencia-informatica/>. [Consulta: 6 de julio de 2021].

7. Informatica. *Guía de seguridad*. [en línea]. <https://docs.informatica.com/es_es/data-integration/metadata-manager/10-0/guia-de-seguridad/permisos/permisos-del-objeto-de-dominio/permisos-por-usuario-o-grupo/visualizacion-de-detalles-de-permiso-para-un-usuario-o-grupo.html>. [Consulta: 14 de marzo de 2021].

8. Ingenio Pantaleón. *Nuestra historia*. [en línea]. <https://www.pantaleon.com/#nuestra-historia>. [Consulta: 10 de enero de 2021].

9. Ingenio Pantaleón. *Políticas*. [en línea]. <https://www.pantaleon.com/desarrollo-responsable/un-equipo-responsable/politica-integral-de-gestion/#:~:text=Satisfacer%20las%20necesidades%20de%20nuestros,el%20deterioro%20de%20la%20salud>. [Consulta: 10 de enero de 2021].

10. Ingenio Pantaleón. *Ubicación*. [en línea]. <https://www.google.com/maps/place/Pantale%C3%B3n/@14,6016917,-90,5093126,18z/data=!4m5!3m4!1s0x8589a3c856983847:0x40ceac2cbf38ce93!8m2!3d14,6024436!4d-90,5090599?hl=es>. [Consulta: 10 de enero de 2021].

11. MAGIO, Sasha. *Actividades de monitoreo de seguridad interna y externa*. [en línea]. <https://techlandia.com/actividades-monitoreo-seguridad-interna-externa-info_194844/>. [Consulta: 15 de junio de 2021].

12. MORALES GONZÁLEZ, Carlos Andrés. *Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana*. [en línea]. <http://repository.unipiloto.edu.co/bitstream/handle/20,500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y>. [Consulta: 15 de abril de 2021].

13. MORENO BOIZA, Vanesa. *Análisis y diseño de una plataforma web para un sistema de gestión de usuarios*. [en línea]. <https://e-archivo.uc3m.es/bitstream/handle/10016/16046/PFCVanesaMorenoBoiza.pdf?sequence=1&isAllowed=y>. [Consulta: 15 de mayo de 2021].

14. PALMA, José. *Cómo hacer un manual de procedimientos*. [en línea]. <https://www.gestiopolis.com/creacion-de-un-manual-de-procedimientos/>. [Consulta: 6 de diciembre de 2020].

15. RIESTRA, Canek. *El plan de análisis paso a paso*. [en línea]. <https://es.slideshare.net/Canek_Riestra/el-plan-de-anlisis-paso-por-paso>. [Consulta: 25 de noviembre de 2020].

16. TERUEL, Amneris. *El ciclo de vida de un evento de seguridad*. [en línea]. <https://www.helpsystems.com/es/blog/el-ciclo-de-vida-de-un-evento-de-seguridad>. [Consulta: 15 de abril de 2021].

ANEXO

Anexo 1. **Servidor instalado en oficina**

Fuente: Last Dragon. *Como hacer tu site de computo*. https://www.lastdragon.net/?p=426. Consulta: 23 de abril de 2021.

Anexo 2. **Estación SOC**

Fuente: Winsted. *Estación de control E-SOC*. https://www.winsted.com/es/e-soc-consoles/. Consulta: 23 de abril de 2021.