Análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira

Dayana Emilia Ojeda Pereira & Melba María Muñoz

Octubre de 2018

Universidad Nacional Abierta y a Distancia – UNAD

Ciencias Administrativas Contables, Económicas y de Negocios

Especialización en Gestión de Proyectos

Abstract

A vulnerability or security failure is everything that causes our computer systems to work in a different way, affecting the security of them, being able to cause, among other things, risks, threats, loss and theft of information.

It is essential to know which resources of the entity need protection in order to control access to the system and the rights of the users of the information system. Also, to have greater security in the information since it is one of the most important assets an organization can have, and therefore we must protect it to avoid risk, threat or loss of it. Information Security can be defined as a set of technical, organizational and legal measures that allow the organization to ensure the confidentiality, integrity and availability of information.

It should be noted that this research is under ISO / IEC 27001: 2013, which provides a methodology for the implementation of information security and thus improve the processes in the handling of data. It also allows an organization to be certified, which means that it has confirmed that the security of the information has been implemented in that organization in the best possible way.

Una vulnerabilidad o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas riesgos, amenazas, pérdida y robo de información.

Es fundamental saber qué recursos de la entidad necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Asimismo, tener mayor seguridad en la información ya que es uno de los activos más importante que puede tener una organización, y por consiguiente debemos protegerla para no correr riesgo, amenaza o pérdida de la misma. La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

Cabe señalar que esta investigación está bajo la norma ISO/IEC 27001:2013, la cual proporciona una metodología para la implementación de la seguridad de la información y así mejorar los procesos en el manejo de los datos. También permite que una organización sea certificada, lo cual significa que ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

Descriptores Clave

Riesgo, seguridad, vulnerabilidad, información.

Introducción

Una vulnerabilidad o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas riesgos, amenazas, pérdida y robo de información.

Por lo tanto, es fundamental saber qué recursos de la entidad necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Asimismo tener mayor seguridad en la información, debido a que es uno de los activos más importantes que puede tener una organización, y por consiguiente debemos protegerla para no correr riesgos, amenazas o pérdida de la misma. La seguridad de la información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

Cabe señalar que esta investigación está bajo la norma ISO/IEC 27001:2013, la cual nos ha servido de apoyo; como su objetivo es proporcionar una metodología para la implementación de la seguridad de la información y así mejorar los procesos en el manejo de los datos. También permite que una organización sea certificada, lo cual significa que ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

Problema de investigación

Planteamiento del Problema

Los avances tecnológicos en el mundo han creado grandes barreras para proteger la información; por lo tanto las compañías deben aprender cómo aceptar el cambio de manera segura para controlar y minimizar las vulnerabilidades en el manejo de la información. Así mismo en Latinoamérica existen estrategias que utilizan las compañías para mantener a salvo sus activos más valiosos; cabe resaltar que muchas empresas en Colombia emplean modelos de seguridad que se enfocan en mantener alejados a los atacantes externos.

De acuerdo a lo anterior la empresa Gestión & Negocios Administrativos SAS dedicada a la consultoría, interventoría y suministros, dispuesta a brindar soluciones apropiadas a sus clientes del sector público y privado, actualmente presenta problemas en la seguridad de la información. Su infraestructura física y los procesos no están acorde a la norma ISO/IEC 27001:2013. Estos problemas están sujetos a que no existe una red informática, esta es una dificultad que está presente por el sólo hecho de subestimarse las fallas que a nivel interno se producen, ya que los computadores no están conectados entre sí por medio de dispositivos físicos que envían y reciben documentos; con la finalidad de compartir información, recursos y ofrecer servicios. Por consiguiente los funcionarios se mantienen conectados a través de los correos electrónicos para enviarse información por medio del internet. Por lo tanto, cuando no hay internet se genera un tráfico de memoria USB a través de las dependencias para obtener un documento.

Además cabe señalar que actualmente no poseen un servidor diseñado para brindar alto rendimiento, almacenamiento y flexibilidad en el manejo de la información, que le permita proveer servicios a otras computadoras denominadas clientes dentro de la empresa.

Del mismo modo se presentan problemas en los procesos por lo que han tenido pérdida de información, porque no realizan frecuentemente copias de seguridad (backups) y monitoreo a los equipos de cómputo, los cuales son útiles para recuperarse de una catástrofe informática y recuperar archivos que pueden haberse eliminado accidentalmente. Respecto a las políticas de seguridad observamos que no están documentadas para que el personal de la entidad cumpla a cabalidad cada una de ellas, contribuyendo a que se agilicen los procesos de forma eficaz y eficiente.

De lo anterior cabe señalar que dentro de la observación que se realizó a la empresa Gestión & Negocios Administrativos SAS existen amenazas y vulnerabilidades que atentan contra la seguridad informática, en particular, las del ámbito de la interventoría y consultoría, que manejan grandes volúmenes de información que por su variedad e importancia la hacen blanco de posibles ataques; de allí la importancia de analizar las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira.

Formulación del Problema

Al realizar el análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS resulta oportuno formular la siguiente incógnita:

¿Cuáles son las vulnerabilidades en el manejo de la información, bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira?

Objetivos

Objetivo general

Analizar las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira.

Objetivos específicos

- Analizar las políticas de seguridad de la información en los procesos que maneja la empresa Gestión & Negocios Administrativos SAS acordes a la norma ISO/IEC 27001:2013.
- Evaluar la seguridad física y ambiental bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS
- Estudiar la gestión de incidentes y mejoras en la seguridad de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS

Justificación

En la empresa Gestión & Negocios Administrativos SAS se analizan las vulnerabilidades en el manejo de la información teniendo en cuenta las políticas de seguridad o directrices que rijan los procesos en la red informática que permite acceder a la información de manera eficaz y eficiente, salvaguardando la información de ataques por partes de intrusos, así mismo se garantiza la autenticidad, confidencialidad, integridad, disponibilidad de los datos.

Desde el punto de vista teórico, se enmarca en los planteamientos de la informática y las tecnologías de la información y comunicación, donde se analizaron las vulnerabilidades en el manejo de la información, bajo la norma ISO/IEC 27001:2013, siendo los sistemas de información y los datos almacenados uno de los recursos más valiosos con los que puede contar cualquier organización. Asimismo está generando una aplicación de un nuevo método de investigación para obtener conocimiento valido y confiable para el área de sistemas dentro de la entidad.

A nivel práctico, se centra en brindar información gerencial a través de controles o políticas de seguridad, que permitan minimizar las amenazas a las que están expuestos los activos dentro de la empresa Gestión & Negocios Administrativos SAS.

Bajo una perspectiva social, tiene su relevancia, porque ayudará a mejorar la calidad del servicio que actualmente presta a sus clientes, además, de regular el Sistema de Gestión de Seguridad de la Información para evitar pérdidas de datos causados por infiltrados que buscan

hacer daño a la organización. Del mismo modo, aporta información necesaria para el desarrollo de futuras investigaciones respecto a la seguridad de la información.

Sin embargo, si la empresa no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminarlos. La ISO/IEC 27001:2013, recomienda llevar a cabo una gestión de riesgo, que se defina primero el alcance del estándar en la empresa, y con base en ello, identificar todos los activos de información; estos deben ser evaluados para determinar su impacto en la organización; luego, se debe realizar un análisis para establecer qué activos están bajo riesgo, es en ese momento se debe tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigar el riesgo.

Tabla de contenido

Lista de tablas

Lista de gráficos

Delimitación

El análisis de vulnerabilidades se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro de cualquier Sistema de Gestión de la Seguridad de la Información; es por eso, que la presente investigación denominada: Análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira, está relacionada con la Gestión de las Organizaciones.

Delimitación Histórica o Temporal

En la presente investigación, la información requerida para el estudio estará enmarcada en el año 2018, con el propósito de fundamentarse en teorías y conceptos recientes pertenecientes al campo de las vulnerabilidades de la información y la norma ISO/IEC 27001:2013.

Delimitación Geográfica o Espacial

La presente investigación se desarrollará en la República de Colombia, en el Departamento de La Guajira, en el Distrito Especial Turístico y Cultural de Riohacha, más concretamente en la Empresa Gestión & Negocios Administrativos SAS ubicada en la Calle 10 # 7-39 de esta ciudad.

Marco teórico

¿Qué es vulnerabilidad?

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la organización, se puede agrupar las vulnerabilidades en grupos característicos: ambiental, física, económica, social, educativo, institucional y política (Erb, 2018).

¿Cuáles son los tipos de vulnerabilidades en la información?

Existen diferentes vulnerabilidades que, dependiendo de sus características, las podemos clasificar e identificar en los siguientes tipos (Montañez León, 2018):

De configuración: Si la gestión administrable por el usuario es tal que hace que el sistema sea vulnerable, la vulnerabilidad no es debida al diseño del mismo si no a cómo el usuario final configura el sistema. También se considera error de este tipo cuando la configuración por defecto del sistema es insegura, por ejemplo una aplicación recién instalada que cuenta de base con usuarios por defecto.

Validación de entrada: Este tipo de vulnerabilidad se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente de forma que una vulnerabilidad puede ser aprovechada por una cierta secuencia de entrada.

Salto de directorio: Ésta aprovecha la falta de seguridad de un servicio de red para desplazarse por el árbol de directorios hasta la raíz del volumen del sistema. El atacante podrá entonces desplazarse a través de las carpetas de archivos del sistema operativo para ejecutar una utilidad de forma remota.

Seguimiento de enlaces: Se producen cuando no existe una protección lo suficientemente robusta que evite el acceso a un directorio o archivo desde un enlace simbólico o acceso directo.

Inyección de comandos en el sistema operativo: Hablamos de este tipo de vulnerabilidad para referirnos a la capacidad de un usuario, que controla la entrada de comandos (bien a través de un terminal de Unix/Linux o del interfaz de comando de Windows), para ejecutar instrucciones que puedan comprometer la integridad del sistema.

Secuencias de comandos en sitios cruzados (XSS): Este tipo de vulnerabilidad abarca cualquier ataque que permita ejecutar código de "scripting", como VBScript o java script, en el contexto de otro dominio. Estos errores se pueden encontrar en cualquier aplicación HTML, no se limita a sitios web, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí. El problema está en que normalmente no se validan correctamente los datos de entrada que son usados en cierta aplicación. Hay dos tipos:

- ✓ Indirecta: consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas, sin usar sesiones.
- ✓ Directa: consiste en localizar puntos débiles en la programación de los filtros.

Inyección SQL: Inyección SQL es una vulnerabilidad informática en el nivel de base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.

Una inyección de código SQL sucede cuando se inserta un trozo de código SQL dentro de otro código SQL con el fin de modificar su comportamiento, haciendo que ejecute el código malicioso en la base de datos. Un ejemplo es cuando un programa realiza una sentencia SQL sin querer con parámetros dados por el usuario para luego hacer una consulta de base de datos. En dichos parámetros que da el usuario estaría el código malicioso. Con estas inyecciones de código se pueden obtener múltiples resultados tales como datos escondidos, eliminar o sobrescribir datos en la base de datos y hasta lograr ejecutar comandos peligrosos en la máquina donde está la base de datos.

El hecho de que un servidor pueda verse afectado por las inyecciones SQL se debe a la falta de medidas de seguridad por parte de sus diseñadores/programadores, especialmente por una mala filtración de las entradas (por formularios, cookies o parámetros).

Inyección de código: Aquí encontramos distintos sub-tipos dentro de esta clase de vulnerabilidad:

- Inyección directa de código estático: el software permite que las entradas sean introducidas directamente en un archivo de salida que se procese más adelante como código, un archivo de la biblioteca o una plantilla. En una inyección de código de tipo estático o también llamada permanente, una vez inyectado el código en una determinada parte de la aplicación web, este código queda almacenado en una base de datos. Una de las soluciones más apropiadas es asumir que toda la entrada es malévola. También es posible utilizar una combinación apropiada de listas negras y listas blancas para asegurar que solamente las entradas válidas y previstas son procesadas por el sistema.

- Evaluación directa de código dinámico: el software permite que las entradas sean introducidas directamente en una función que evalúa y ejecuta dinámicamente la entrada como código, generalmente en la misma lengua que usa el producto. En una inyección de código de tipo dinámico o no permanente la inyección tiene un tiempo de vida limitado y no se almacena, al menos permanentemente, en ningún sitio. Las soluciones más apropiadas son las mismas que para la inyección directa de código estático.

- Inclusión remota de archivo PHP: vulnerabilidad existente únicamente en páginas dinámicas escritas en PHP está debida a la inclusión de la función include () la cual permite el enlace de archivos situados en otros servidores, mediante los cuales se puede ejecutar código PHP en el servidor. Se utilizan las funciones include, include_once, require, require_once las cuales son utilizadas para incluir en una página web otras páginas por tanto el atacante podrá obtener una Shell (es una interfaz con el sistema operativo, gracias a él podremos dar las órdenes y mandatos para que el sistema realice

las tareas que necesitamos) en el servidor de la víctima y ejecutar un archivo. Para que se pueda ejecutar dicho archivo debe tener una extensión diferente a ".php" ya que con esta extensión el archivo se ejecutaría en el servidor del atacante y no en el de la víctima, así un archivo ".txt", ".gif" serian algunos de los más adecuados.

Error de búfer: Un búfer es una ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada (Wikipedia, 2018).

El desbordamiento del búfer (Buffer overflow u overrun): un búfer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben, ese exceso se vierte en zonas del sistema causando daños. Son defectos de programación y existen algunos lenguajes que impiden que los desbordamientos puedan ocurrir.

El agotamiento del búfer (buffer underflow o underrun): es un estado que ocurre cuando un búfer usado para comunicarse entre dos dispositivos o procesos se alimenta con datos a una velocidad más baja que los datos se están leyendo en ellos. Esto requiere que la lectura del programa o del dispositivo del búfer detenga brevemente su proceso (dit.upm, 2018).

Formato de cadena: Nos referimos a este tipo de vulnerabilidad cuando se produce a través de cadenas de formato controladas externamente, como el tipo de funciones "printf" en el lenguaje "C" que pueden conducir a provocar desbordamientos de búfer o problemas en la representación de los datos.

Errores numéricos: El desbordamiento de entero (integer overflow): un desbordamiento del número entero ocurre cuando una operación aritmética procura crear un valor numérico que sea más grande del que se puede representar dentro del espacio de almacenaje disponible. Por ejemplo, la adición de 1 al valor más grande que puede ser representado constituye un desbordamiento del número entero.

El agotamiento de entero (integer underflow): consiste en que un valor se resta de otro, que es menor que el valor mínimo del número entero, y que produce un valor que no es igual que el resultado correcto.

Revelación/Filtrado de información: Un filtrado o escape de información puede ser intencionado o no intencionado. En este aspecto los atacantes pueden aprovechar esta vulnerabilidad para descubrir el directorio de instalación de una aplicación, la visualización de mensajes privados, etc. La severidad de esta vulnerabilidad depende del tipo de información que se puede filtrar.

Gestión de credenciales: Este tipo de vulnerabilidad tiene que ver con la gestión de usuarios, contraseñas y los ficheros que almacenan este tipo de información. Cualquier debilidad en estos elementos es considerado como una vulnerabilidad que puede ser explotada por un atacante.

Permisos, privilegios y/o control de acceso: Se produce cuando el mecanismo de control de acceso o asignación de permisos es defectuoso. Hay que tener en cuenta que se trata del sistema en sí y no se debe confundir con una mala gestión por parte del administrador.

Fallo de autenticación: Esta vulnerabilidad se produce cuando la aplicación o el sistema no es capaz de autenticar al usuario, proceso, etc. correctamente.

Carácter criptográfico: La generación de números aleatorios para generar secuencias criptográficas, la debilidad o distintos fallos en los algoritmos de encriptación así como defectos en su implementación estarían ubicados dentro de este tipo de vulnerabilidad.

Falsificación de petición en sitios cruzados (CSRF): Este tipo de vulnerabilidad afecta a las aplicaciones web con una estructura de invocación predecible. El agresor puede colocar en la página cualquier código, el cual posteriormente puede servir para la ejecución de operaciones no planificadas por el creador del sitio web, por ejemplo, capturar archivos cookies sin que el usuario se percate.

El tipo de ataque CSRF más popular se basa en el uso del marcador HTML <img>, el cual sirve para la visualización de gráficos. En vez del marcador con la URL del archivo gráfico, el agresor pone un tag que lleva a un código JavaScript que es ejecutado en el navegador de la víctima.

Condición de carrera: Una condición de carrera se produce cuando varios procesos tratan de acceder y manipular los mismos datos simultáneamente. Los resultados de la ejecución dependerán del orden particular en que el acceso se lleva a cabo. Una condición de carrera puede ser interesante para un atacante cuando ésta puede ser utilizada para obtener acceso al sistema.

Error en la gestión de recursos: El sistema o software que adolece de este tipo de vulnerabilidad permite al atacante provocar un consumo excesivo en los recursos del sistema (disco, memoria y CPU). Esto puede causar que el sistema deje de responder y provocar denegaciones de servicio.

Error de diseño: En ocasiones los programadores bien por culpa de los entornos de trabajo o bien por su metodología de programación, cometen errores en el diseño de las aplicaciones. Esto provoca que puedan aparecer fallos de seguridad y la consiguiente vulnerabilidad. También se puede aplicar el "error de diseño" si no hay fallos en la implementación ni en la configuración de un sistema, si no que el diseño inicial es erróneo (Elipe, 2018).

Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO7/IEC 27001:2013.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización (ISO 27000.es, 2012).

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO7/IEC 27001:2013, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En las siguientes secciones (a las que puede acceder directamente a través del submenú de la izquierda o siguiendo los marcadores de final de página) se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO7/IEC 27001:2013 (ISO 27000.es, 2018).

¿Qué es la seguridad de la información? (Wikipedia, 2018)

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

¿Por qué es importante la seguridad de la información?

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. Esta se clasifica como :

- **Crítica:** Es indispensable para la operación de la empresa.
- **Valiosa:** Es un activo de la empresa y muy valioso.
- **Sensible:** Debe de ser conocida por las personas autorizadas

Cabe resaltar que existen dos palabras importantes en la seguridad de la información:

- **Riesgo:** Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones.
- **Seguridad:** Es una forma de protección contra los riesgos.

Protocolos de Seguridad de la Información

Son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

- **Criptografía** (Cifrado de datos), se ocupa del cifrado de mensajes un mensaje es enviado por el emisor lo que hace es transposicionar u ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.
- **Lógica** (Estructura y secuencia). Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va enviar el mensaje.

- **Autenticación** Es una validación de identificación es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

El manejo de riesgo

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos en una empresa. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, después de haberlo identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

- **Evitar:** el riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades. Ejemplo: No instalar empresas en zonas sísmicas.

- **Reducir**: Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla; se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante. Ejemplo: No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

- **Retener, Asumir o Aceptar el riesgo:** Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente. Ejemplo de asumir el riesgo: Con recursos propios se financian las pérdidas.

- **Transferir:** Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades. Ejemplo: Transferir los costos a la compañía aseguradora.

Copias de seguridad

Realizar copias de seguridad a la información es necesario porque queda almacenada en más de un lugar, por ejemplo, en un disquete además del disco duro. Si se destruye el archivo original, la información puede recuperarse a partir de la copia de seguridad. Deben hacerse copias se seguridad con la suficiente frecuencia: cada vez que se modifique la información. De esta forma, tendremos en un lugar seguro la versión más actual del archivo y si pasa algo, perderemos una cantidad mínima de información.

¿Por qué deben hacerse copias de seguridad?

Es importante hacer backups a los archivos por que pueden destruirse por una serie de razones: puede borrarlos accidentalmente mientras está utilizando el ordenador; puede que el disco duro, el disquete u otro sistema de almacenamiento utilizado se estropee o se produzca una avería y los archivos guardados queden inutilizados. No es un hecho aislado que los ordenadores sufran tales daños físicos que no puedan recuperarse los archivos que contienen. Los archivos o los equipos pueden echarse a perder o ser objeto de un robo.

Asimismo, también los virus informáticos y otro tipo de software malicioso pueden causar la desaparición de archivos. La realización de copias de seguridad es una parte esencial de la seguridad de la información. Una de las funciones más habituales del software malicioso es la destrucción de información, ya que esto es especialmente perjudicial para las empresas y relativamente fácil de conseguir para los programadores.

Las copias de seguridad también pueden destruirse guardando información nueva sobre información antigua. Puede proteger los disquetes contra la escritura desplazando la pestaña que incorporan hacia la posición pertinente. De igual manera, se puede proteger las copias de seguridad del disco duro haciendo que sea imposible modificar o destruir el archivo.

¿Con qué frecuencia deben hacerse copias de seguridad?

Se debe recordar hacer copias de seguridad regularmente y con la suficiente frecuencia a fin de disponer siempre de la última versión de los archivos. También puede automatizar el proceso de realización de copias de seguridad a partir de las herramientas de su sistema

operativo. Los archivos más importantes, se recomienda realizar varias copias de seguridad y guardarla en diferentes lugares físicos.

Almacenamiento de las copias

Las copias de seguridad no pueden guardarse en el mismo lugar donde está el ordenador. El sitio donde se almacenen las copias debe ser un sitio en el que no entre la luz del sol, no haya campos magnéticos fuertes ni se derramen sustancias como café. Las copias de suma importancia pueden guardarse en un lugar a prueba de fuego. También es buena idea hacer más de una copia de seguridad y guardarlas en distintas copias en lugares seguros; no es aconsejable utilizar la impresión como único método de copia de seguridad.

También puede guardar la copia de seguridad en un servidor, si tiene acceso a uno, puede tratarse de un servidor de red de área local o bien de un servidor de Internet. Si la información se encuentra en un servidor, también los desconocidos pueden acceder a ella. Sólo es aconsejable guardar información en los servidores de Internet si quiere que ésta sea de alcance público.

Actores Que Amenazan La Seguridad

- **Hacker:** es cualquier persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura". Su formación y las habilidades que poseen les da una experticia mayor que les permite acceder a sistemas de

información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

- **Cracker:** es aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.
- **Lamer:** es una persona que alardea de pirata informático, cracker o hacker y solo intenta utilizar programas de FÁCIL manejo realizados por auténticos hackers.
- **Copyhacker:** es una persona dedicada a falsificar y crackear hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros. Los copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.
- **Bucanero:** es un comerciante que depende exclusivamente de de la red para su actividad. Los "bucaneros" no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.
- **Phreaker:** se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los teléfonos móviles, han tenido que entrar también en el mundo de la informática y del procesamiento de datos.

- **Newbie o "novato de red":** es un individuo que sin proponérselo tropieza con una página de hacking y descubre que en ella existen áreas de descarga de buenos programas de hackeo, baja todo lo que puede y empieza a trabajar con ellos.
- **script kiddie o skid kiddie:** es un simple usuario de Internet, sin conocimientos sobre hackeo o crackeo, aficionado a estos tema, no los conoce en profundidad limitándose a recopilar información de la red y a buscar programas que luego ejecuta, infectando en algunos casos de virus a sus propios equipos.
- **Tonto o descuidado:** es un simple usuarios de la información, con o sin conocimientos sobre hackeo o crackeo que accidentalmente borra daña o modifica la información, ya sea en un mantenimiento de rutina o supervisión.

Generalidades de la serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. Las normas que incluye se enumeran a continuación:

- *"ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Introducción y base para el resto. Tercera versión: enero de 2014.*
- *ISO/IEC 27001 - es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2013 y fue desarrollada en base a la norma británica BS 7799-2.*

- *ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001 (27001academy, 2018).*
- *ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2013 como ISO 17799:2013 y recibió su nombre oficial ISO/IEC 27002:2013 el 1 de julio de 2007. Última versión: 27002:2013, de setiembre de 2013.*
- *ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero de 2010. No es certificable.*
- *ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre de 2009, no se encuentra traducida al español actualmente.*
- *ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de*

la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011.

- *ISO/IEC 27006 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. Publicada en 2007 y revisada en diciembre de 2011 y septiembre de 2015.*
- *ISO/IEC 27007 - es una guía para auditar al SGSI. Publicada en noviembre de 2011.*
- *ISO/IEC 27016 - es una norma que se concentra en un análisis financiero y económico de equipos y procedimientos de la seguridad de la información. Publicada en febrero de 2014.*
- *ISO/IEC 27017 - es una guía de seguridad para Cloud Computing. Publicada en diciembre de 2015.*
- *ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Publicada en agosto de 2011. (BITCompany, 2011)*
- *ISO/IEC 27799:2008 - es una guía para implementar ISO/IEC 27002 en la industria de la salud"* (Wikipedia, 2018)

Beneficios de la serie 27000 (ISO 27000.es, 2012)

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.

- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

Marco conceptual

Dentro de los términos que se utilizaran durante el desarrollo de esta investigación se encuentran (ICONTEC, 2013):

Activo: cualquier cosa que tiene valor para la organización.

Análisis de Riesgo: uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Confidencialidad: propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Evaluación del riesgo: proceso de comparar el riesgo estimado con el criterio de riesgos dado para determinar la importancia del riesgo.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Seguridad de información: preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

Sistema de gestión de seguridad de la información (SGSI): es la parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.

Tratamiento del riesgo: proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

Amenaza: Causa que origina situaciones de riesgo; peligros potenciales a los que están expuestos los recursos o componentes de un sistema.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

Aplicación cliente/servidor: Una aplicación de LAN que utiliza los recursos o servicios de servidores en la misma o diferente LAN. El cliente es la aplicación o hardware que utiliza los servicios centralizados. El servidor es la aplicación o hardware que provee el servicio centralizado.

Autenticidad: Propiedad que garantiza que la identidad de un sujeto o recurso es la que se declara. La autenticidad se aplica a entidades tales como usuario, procesos, sistemas e información.

Comunicación Electrónica: Una comunicación electrónica se debe entender como un mensaje de datos, según la definición de este término establecida por la Ley 527 del 18 de agosto de 1999:

a) Mensaje de datos. “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

Confiabilidad: Propiedad de tener comportamiento y resultados previstos consistentes.

Correo electrónico: Es la facilidad de comunicación vía electrónica que permite enviar y recibir mensajes, archivos, confirmar citas y actualizar la agenda (comunicación correo -agenda electrónica); facilita el flujo de información dentro de la organización.

Hacking: Es una técnica que consiste en construir y solucionar problemas que atenten contra la vulnerabilidad de un sistema o aplicación; Además permite encontrar los límites de los productos, aparatos y servicios digitales de informática o comunicaciones y compartirlo con otros y/o los fabricantes mismos de ésos productos.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Intranet: Es una herramienta informática que permite obtener información y gestionar procesos útiles para la organización y sus funcionarios, mediante un ambiente de navegación similar al de Internet. ECORED es el nombre dado a la Intranet corporativa.

Internet: Es una red global de información cuyos servicios básicos son: Acceso a servidores www para búsqueda de información, correo electrónico y, por su medio, acceso a grupos de discusión o foros electrónicos basados en correo electrónico y servicios básicos Telnet y FTP.

Intruso: Individuo que trata o logra ingresar a un sistema sin ser usuario autorizado.

Riesgo: Es el efecto o consecuencia de la ocurrencia de un evento no deseado; es el producto de dos factores:

Probabilidad de que se presente una situación de riesgo por el Impacto o costo en el que se incurre. Es el potencial que una amenaza libere y aproveche las vulnerabilidades de un activo o grupo de activos para causar pérdida o daño del mismo.

Los riesgos del negocio son aquellos que pueden impactar los activos o procesos de una empresa. Pueden originarse como resultado de la interacción con el ambiente o como resultado de estrategias, sistemas, procesos, procedimientos e información usada por la organización. La naturaleza de estos riesgos puede ser financiera, regulatoria u operacional.

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Salvaguardar: Práctica, procedimiento o mecanismo para tratar los riesgos.

Servidor: Equipo computacional destinado al alojamiento de páginas de Internet y a la prestación de servicios web para aquellos usuarios que cuenten con acceso permitido a la máquina.

Software: El software son las instrucciones electrónicas que van a indicar al ordenador que es lo que tiene que hacer. También se puede decir que son los programas usados para dirigir las funciones de un sistema de computación o un hardware.

Spam: mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Usuario / login: Palabra que identifica a un usuario dentro de un sistema específico (Instituto de Tecnología de Massachusetts, 2018).

Virus (Lobocom, 2005)**:** Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

a. Solamente advertir al usuario de su presencia, sin causar daño aparente.
b. Tratar de pasar desapercibidos para causar el mayor daño posible.
c. Adueñarse de las funciones principales (infectar los archivos de sistema).

Archivo: Un archivo o fichero informático es un conjunto de bits almacenado en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene (Wikipedia, 2018).

Cracker: El término cracker (del inglés crack, romper) se utiliza para referirse a las personas que rompen algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío (Wikipedia, 2018).

ISO (Dispetrocom Ltda, 2017)**:** La Organización Internacional para la Estandarización, ISO por sus siglas en inglés (International Organization for Standardization), es una federación mundial que agrupa a representantes de cada uno de los organismos nacionales de estandarización (como lo es el IRAM en la Argentina), y que tiene como objeto desarrollar estándares internacionales que faciliten el comercio internacional.

Informática: es la ciencia que estudia el tratamiento automático y racional de la información.

Intrusión: conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.

Recursos: Son los necesarios para desarrollar sus actividades al llevar a cabo su fin.

Marco de referencia

Antecedentes investigativos

De acuerdo a las investigaciones realizadas, se evidenció que en la Universidad de La Guajira se ha realizado varios proyectos de este tipo, como son:

Titulado: Análisis del estado actual sobre el nivel de conocimiento y aplicación Del Sistema de Gestión de Seguridad de la Información en la Ipsi Anashiwaya en base a la Norma ISO 27001:2005 en el municipio de Riohacha, realizado por las estudiantes del programa de ingeniería de sistemas: Dayana Yiseth Estrada Mendoza y Yisset Andrea Pimienta Zapata, en el segundo periodo académico del año 2012.

Titulado: Diseño de un modelo de gestión de la seguridad de la información en la universidad de la Guajira basado en ISO 27001, realizado por las estudiantes del programa de ingeniería de sistemas: María Josefa Larrada Delgado y María Victoria Pérez Mejía, en el año 2010. En este proyecto se propuso crear un modelo para la Gestión de la Seguridad de la Información en Uniguajira, debido a la necesidad de gestionar la seguridad la información ya que hasta el momento no existía ningún trabajo en ese sentido. Dentro de este panorama general se intenta responder a preguntas como ¿Cuál es el estado actual de la SI en la universidad de la Guajira? ¿Cómo mejorar la confidencialidad, integridad y disponibilidad de la información?.

Cabe resaltar que existen pocos proyectos realizados bajo esta Norma (Iso 27001), lo que demuestra que existe la necesidad en el entorno de esta investigación, teniendo en cuenta el análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO 27001 para

adquirir seguridad en la misma. Así mismo, según investigaciones realizadas en la Web, en Colombia son pocas las entidades que están certificadas bajo la norma Iso 27001, como por ejemplo Ricoh Colombia, S.A., SETECSA S.A, UNE EPM Telecomunicaciones. S.A E.S.P, UNISYS Global Outsourcing & Infrastructure Services (GOIS)/Maintenance Support Services (MSS) (Hoyos, Ortiz, & Monsalve, 2010), SICTE S.A.S (epulpo, 2017), entre otros; en el Departamento de la Guajira son pocas las entidades tanto en el sector público como privado que han creado un modelo de gestión para la seguridad de la información y que así mismo pretendan certificarse; entidades como: Carbones del Cerrejón, Sena, Universidad de la Guajira, Gobernación de la Guajira, Alcaldía de Riohacha, Coorpoguajira y Otras entidades han venido realizando esta labor para el uso e implementación del SGSI.

Por su parte, Carbones del Cerrejón, la empresa más grande ubicada en el departamento de La Guajira, se desarrolló un proyecto sobre **mejores prácticas de operación definidas en el estándar NTI-ISO/IEC 27001, ITIL y COBIT**, implementado en el año 2011, pese a las políticas de seguridad de la información que poseían no se ajustaban a la realidad de la compañía, debido a que habían sido heredadas por la multinacional ExxonMobil, antigua propietaria del complejo carbonífero.

A nivel internacional en Quito, Ecuador, en la Escuela Politécnica Nacional en la facultad de ingeniería eléctrica y electrónica realizaron la investigación titulada (Alvarez & García, 2007): **Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 2700**1, para la intranet de la corporación metropolitana de salud, por las estudiantes: Flor María Álvarez Zurita Y Pamela Anabel García Guzmán, en Octubre del año

2007, la cual tenía como fin lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos.

Situación actual

Actualmente la Empresa Gestión & Negocios Administrativos SAS cuenta con 6 computadores de escritorio y 10 computadores portátiles manipulados por 6 personas que cumplen con labores administrativas y 10 empleados indirectos que se encuentran en la ejecución de obras que se realizan en el momento, de igual forma no posee una red informática, que permita llevar sus procesos de manera eficaz y eficiente, por ende comparte información vía correo electrónico por medio de la internet y memoria USB. Cuenta con un software independiente para el área de contabilidad denominado SIIGO y las demás áreas trabajan con herramientas ofimáticas de Microsoft Office.

Cabe resaltar que está en proceso un sistema integral de gestión de calidad para mejorar los servicios, el acceso de la información y se está proyectando implementar una nube que le permita acceder a la información de la empresa desde cualquier lugar del mundo por medio del internet.

Resultado de entrevistas y recorridos por las instalaciones y oficinas de la empresa Gestión & Negocios Administrativos SAS se encontró que existe conciencia en los empleados de la importancia del manejo de la información y la seguridad de la misma, como también de las mínimas políticas de seguridad para hacerle frente a los peligros más evidentes que corre la información en las áreas más importantes.

Una de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas

tecnológicos, asimismo para los funcionarios de la empresa Gestión & Negocios Administrativos SAS que tienen la responsabilidad de escoger cual de su información es más importante para protegerla con los escasos medios que poseen.

Los recursos con los que cuentan para la protección de la información resultan insuficientes, lo cual hace evidente la falta de una planeación de la seguridad informática que permite abrir un espacio para la consecución de los recursos necesarios para salvaguardar la información.

La voluntad por crear un ambiente "seguro" es notable, pero no es suficiente con suponer que se está haciendo todo lo posiblemente necesario, ya que de la misma manera cómo evolucionan los controles evolucionan las trampas para saltar dichos controles; por eso es de igual importancia la actualización y la mejora continua de dicho controles.

Los funcionarios de la empresa demostraron en la entrevista que consideran que es importante que se controle el acceso a la información para que se garantice en el manejo de la información la integridad, confidencialidad, disponibilidad y autenticidad. Al respecto es conviene decir que existe conocimiento por parte de los empleados entrevistados sobre los procesos que maneja su dependencia y la información involucrada, así como la importancia de dichos procesos en la consecución de los objetivos de la empresa Gestión & Negocios Administrativos SAS lo cual es necesario para la protección de la información.

Marco legal

Para el desarrollo de la presente investigación se tuvo en cuenta las leyes que rigen en Colombia por medio de la cual se busca proteger el uso de las tecnologías, la información que es el objeto de mayor valor que tienen las organizaciones, dado que en Colombia cada día surgen nuevas formas de delitos informáticos que pueden afectar la seguridad de la información en las empresas.

Ley 1266 de 2008 Habeas data. Protección datos personales y financieros

Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009 Delitos informáticos

- ✓ Propiedad Intelectual
- ✓ Derechos De Autor
- ✓ Software Libre
- ✓ Software Propietario

Así mismo el marco normativo de los diferentes estándares que están vinculados a un Sistema de Gestión de la Seguridad de la Información. En él se ven representados estándares internacionales de diferente naturaleza y con diferente alcance. Algunos de ellos, como por

ejemplo la serie ISO/IEC 27.000 e ISM3, son específicos de la gestión de seguridad de la información, generales y aplicables a cualquier sector de actividad.

Marco metodológico

Al respecto conviene decir que la metodología es el conjunto de acciones destinadas a describir y analizar el fondo del problema planteado, a través de procedimientos específicos que incluye las técnicas de observación y recolección de datos, determinando el "cómo" se realizará el estudio (estudiantesunesur, 2016). La presente investigación está enmarcada en un estudio de campo, la cual nos permite dar un análisis sobre las vulnerabilidades en el manejo de la información de la entidad y que además nos permite recoger de forma ordenada datos relativos al tema escogido objeto de estudio.

Los datos de interés recogidos durante esta investigación fueron dados de una forma directa de la realidad por los propios investigadores, a través de entrevistas, y aplicaciones de encuestas, en este sentido se trata de investigaciones a través de datos originales, dado que la misma consiste en analizar las vulnerabilidades en el manejo de la información bajo la norma ISO7/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS de la ciudad de Riohacha, Departamento de la Guajira; la cual tiene como fin principal la búsqueda de posibles soluciones a la situación planteada.

Asimismo, este proceso responde a una descripción de hechos tal y como suceden en la realidad y a la referencia de textos trabajos realizados anteriormente; teniendo en cuenta que la investigación monográfica documental "es el conjunto de problemas con de propósito ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos" (Perez Leal, 2017).

Dicha situación se determinó, por cuanto se hizo una descripción sistemática de los hechos con el objetivo de analizar el problema para entender su naturaleza y factores que lo contribuyen.

Por lo anteriormente expuesto, el propósito de la investigación, atreves del mismo se busca indagar una realidad para descubrir cómo es actualmente manejada la seguridad de la información en la empresa Gestión & Negocios Administrativos SAS.

Tipo De Investigación

De acuerdo al estudio realizado, se determinó que el tipo de investigación es descriptiva (Tatayo y Tamayo, 2003), describe que comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre como una persona, grupo o cosa, se conduce o funciona en el presente. La investigación descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentarnos una interpretación correcta. Desde otro punto vista, manifestar o mostrar un análisis de vulnerabilidades en el manejo de la información actual, bajo la norma ISO7/IEC 27001:2013 en la empresa Gestión & Negocios Administrativos SAS.

Método De Investigación

El método consiste en obtener conclusiones particulares a partir de una ley universal (Rodriguez Moguel, 2005).

El método que se implementa en la investigación es el **deductivo;** por lo que se llega a un análisis coherente y adecuado del problema partiendo de lo general a lo particular y aplicado en la práctica, los conocimientos y criterios teóricos sobre el tema; logrando una explicación de los hechos que se van a tener en cuenta para el análisis de las vulnerabilidades en el manejo de la

información bajo la norma ISO7/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS de la ciudad de Riohacha.

Población

En todo proceso de investigación es importante establecer la población objeto de estudio, puesto que de este punto depende el resultado de esta investigación. Según (Moreno, 1987), define la población: como la idea asociada a aquel conjunto de individuos, grupos, instituciones etc.; que por tener determinadas características, han sido seleccionados por el investigador como unidades en relación con las cuales se estudiara la acción y los efectos de variables de interés. De igual manera a la población al que se le aplico las entrevistas y encuestas fue a la Gerente y el área Administrativa el cual, estuvo conformado por 13 empleados de la empresa Gestión & Negocios Administrativos SAS.

Muestra

La muestra es la parte de la población con la que se realiza la investigación o el estudio. Según (Vivanco, 2013), "*la muestra corresponde a una colección de unidades seleccionadas de una población con el fin de estimar los valores que caracterizan a la población*"

Debido al tamaño de la Población se determina por los investigadores que se debe realizar la encuesta, escogida como instrumento de investigación, dicho cuestionario agrupa una serie de preguntas relativas a un evento, sobre el cual los investigadores desean obtener información aplicada a todo el personal involucrado con el manejo y uso del sistema; se asumió este instrumento porque permite abordar los objetivos que plantea el estudio, asimismo brinda a los investigadores la posibilidad de ser aplicado colectivamente y da fidelidad para el momento de codificar los datos.

Es por ello, que la encuesta realizada a los funcionarios de la empresa Gestión & Negocios Administrativos SAS estuvo definida por 13 preguntas formuladas de manera cerrada.

Sistemas de variables

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial).

En la presente investigación se hará un análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO7/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS de la ciudad de Riohacha, donde se conocerá cual es el estado real de la seguridad de la información.

Definición de variables

SI: Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (Wikipedia, 2018).

Operacionalización de variables

En el siguiente cuadro se definen las variables de esta investigación, asimismo los indicadores y las dimensiones, teniendo en cuenta los objetivos dado a que son la base fundamental para llevar a cabo esta investigación.

Según (Tatayo y Tamayo, 2003), "*la Operacionalización de variables es la relación causa-efecto que se da entre uno o más fenómenos estudiados. En toda variable el factor que asume esta condición debe ser determinada mediante observaciones y estar en condiciones de medirse para enunciar que, de una entidad de observación a otra el factor varia y por tanto, cumple con su característica*"

Mapa de Variable

Objetivo: Análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira			
VARIABLE	**OBJETIVOS ESPECÍFICOS**	**DIMENSIÓN**	**INDICADORES**
SEGURIDAD DE LA INFORMACIÓN	**1.** Determinar las políticas de seguridad de la información en los procesos que maneja la empresa Gestión & Negocios Administrativos SAS acordes a la norma ISO/IEC 27001:2013.	**1.1.** Seguridad de la información	✓ Redes ✓ Porcentaje de ataques ✓ Controles ✓ Copias de seguridad ✓ Acceso a internet ✓ Acceso a software.
	2. Analizar la seguridad física y ambiental bajo la norma ISO/IEC 27001:2013, en la empresa	**2.1.** Seguridad	✓ Controles de acceso

Objetivo: Análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira			
VARIABLE	**OBJETIVOS ESPECÍFICOS**	**DIMENSIÓN**	**INDICADORES**
	Gestión & Negocios Administrativos SAS		✓ Políticas de Seguridad ✓ Evaluación riesgo físico y ambiental.
	3. Estudiar la gestión de incidentes y mejoras en la seguridad de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS	**3.1.** Incidentes y mejoras	✓ Reporte de eventos. ✓ Mantenimiento ✓ Responsabilidades ✓ Recolección de evidencia. ✓ Riesgos ocasionales.

Fuentes de investigación

Fuentes Primarias

Encuestas: Se formularon una serie de preguntas escritas, a las personas con el fin de obtener determinada información necesaria para la investigación.

Fuentes secundarias

Se adquirieron a través de libros, enciclopedias, revistas, páginas web y trabajos realizados con relación a este tipo de investigación.

Recursos utilizados

Para la investigación se utilizaron los siguientes recursos:

- 2 computadores portátiles con acceso a internet
- 1 impresora (tinta)
- Papelería
- Memorias USB

Técnicas e instrumentos

Técnicas

Las técnicas utilizadas en el proceso para llevar a cabo esta investigación son las siguientes:

Entrevistas personales: en esta técnica se dio la relación directa establecida entre el investigador y su objeto de estudio a través de los funcionarios de la empresa Gestión & Negocios Administrativos SAS con el fin de obtener testimonios orales.

Observación directa: como investigadores esta técnica la utilizamos para observar y recoger datos mediante la observación, para poder analizar las vulnerabilidades que se puedan presentar en el manejo de la información en el desarrollo de las actividades que llevan a cabo los funcionarios en la empresa Gestión & Negocios Administrativos SAS

Observación indirecta: se presentó esta técnica porque como investigadores corroboramos los datos que se tomaron de los funcionarios de forma oral y escrita que de una u otra manera tienen contactos de primera mano con la fuente que proporciona la información en la entidad

.

Instrumentos

Formulación de encuestas: esta técnica se utilizó porque está destinada a obtener datos de los funcionarios, cuyas opiniones nos interesan como investigadores, para obtener la información necesaria ya que nos permite llevar a cabo esta investigación en la entidad.

Técnicas de análisis de los datos

La técnica de análisis de datos representa la forma de cómo será procesada la información recolectada, esta se puede procesar de dos maneras cualitativa o cuantitativa, en esta ocasión se utilizó la forma cuantitativa para las encuestas que se realizaron a los 6 funcionarios del área administrativa de la empresa Gestión & Negocios Administrativos SAS, el análisis cuantitativo se define como: "*una operación que se efectúa, con toda la información numérica resultante de la investigación. Esta, luego del procesamiento que ya se le habrá hecho, se nos presentará como un conjunto de cuadros y medidas, con porcentajes ya calculados*" (Sabino, 1992). Esto permitirá obtener los porcentajes y representar gráficamente los resultados de los datos adquiridos para tener la información ordenada con representaciones visuales que nos permitan su posterior estudio.

Análisis e interpretación de resultados

El propósito de hacer el análisis e interpretación de los resultados obtenidos en la aplicación de la encuesta realizada a los funcionarios de la Empresa Gestión & Negocios Administrativos SAS en la ciudad de Riohacha, el cual está encaminado al análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO 27001, estableciendo políticas de seguridad que permitan mejorar cada uno de los procesos en la información y minimizar los riesgos para darle solución a problemas que se presentan con el manejo de la seguridad de la Información en la entidad.

Interpretación de los resultados

La encuesta arrojó resultados en los que se evidencia que la empresa Gestión & Negocios Administrativos SAS, carece de las políticas para garantizar la seguridad de la información que es generada o manipulada al interior de los procesos empresariales y que se constituyen como factor de vital importancia en la ejecución de las actividades propias de cada área o departamento.

Es así como al cuantificar los resultados, obtuvimos que tan solo el 23% de los encuestados afirman de la existencia de políticas de seguridad de la información al interior de la empresa, sin embargo, estos mismos las desconocen. Causa de esto, podría ser la falta de una persona que haga el debido seguimiento, monitoreo y control a la información que es utilizada en la empresa y que garantice la aplicación de tales políticas de seguridad, como lo afirman el 85% de los encuestados y que adicionalmente puede traer como consecuencia la pérdida irremediable de

información de gran valor, considerando que el 46% de los encuestados afirma que en algún momento se les ha presentado pérdida de información.

Sumado a lo anterior, no cuentan con un protocolo de acciones preventivas o correctivas para su aplicación cuando se presenta la pérdida de información o con la gestión de los equipos de cómputo, motivo por el cual se han visto en la necesidad de reiniciar con el proceso de elaboración de los documentos, generando de esta manera pérdida de tiempo, dinero y esfuerzo.

En general, el resultado de la encuesta evidencia la necesidad de establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta, tal y como lo expresa la norma para el sistema de gestión integral de la información (ICONTEC, 2013).

Conclusiones y recomendaciones

Partiendo del análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS de la ciudad de Riohacha, los resultados obtenidos de las encuestas y entrevista, se pudo identificar deficiencias o fallas que se presentan en el manejo de la información, las cuales pueden afectar los datos, generar perdida de información, robo, fraudes, ataques, riesgos, entre otros. Por lo tanto durante la elaboración de esta investigación se concluyó que existen algunas vulnerabilidades en el manejo de la información tales como:

- Existen algunas políticas de seguridad de la información las cuales no están documentadas, por lo tanto los funcionarios de la entidad no tienen conocimiento de las mismas.

- Observamos que no hay seguridad física dentro de la entidad debido a que los documentos impresos se encuentran al alcance de cualquier persona, ya que no se encuentra en un área segura.

- No se encuentra un funcionario encargado de la seguridad de la información, mantenimiento y monitoreo de las computadoras.

- No existe una gestión de incidentes y mejoras en la seguridad de la información dentro de la entidad para asegurar una respuesta rápida, efectiva y ordenada a los incidentes respecto a la seguridad de la información.

- No se realiza periódicamente copias de seguridad (Backus), lo cual ha generado perdida de información ya sea por descuido de los funcionarios o por daños físicos.

- No existe una red informática en la entidad que permita compartir información, recursos y otros servicios.

Por lo anterior se recomienda a la entidad:

- Documentar las políticas de seguridad existentes y se implementen otras de acuerdo a la norma ISO/IEC 27001:2013, para controlar y minimizar los riesgos.

- Crear en la entidad un área segura que almacene los documentos en físicos para asegurar que solo se permita el acceso al personal autorizado y evitar posibles pérdidas.

- Establecer una persona que se encargue de vigilar, mantener y monitorear los equipos de cómputo para mejorar la seguridad de la información.

- Determinar acciones preventivas que eliminen las causas de las no conformidades para el mejoramiento continuo.

- Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicación.

- Implementar una red informática que brinde beneficios como: mayor facilidad en la comunicación de los funcionarios, mejorar la integridad y disponibilidad de los datos y mayor seguridad para acceder a la información.

Bibliografía

Alvarez, F. M., & García, P. (10 de 2007). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD*. Obtenido de https://www.buenastareas.com/ensayos/Implementaci%C3%B3n-De-Un-Sistema-De-Gesti%C3%B3n/4996287.html

Dispetrocom Ltda. (9 de 10 de 2017). *¿QUÉ ES EL ISO Y PARA QUÉ SIRVE?* Obtenido de https://dispetrocom.com/2017/10/09/que-es-el-iso-y-para-que-sirve/

dit.upm. (23 de 07 de 2018). *DESBORDAMIENTO DE MEMORIA*. Obtenido de DESBORDAMIENTO DE BUFFER: http://www.dit.upm.es/~pepe/401/3706.htm#!-alone

Elipe, E. (23 de 07 de 2018). *Seguridad y Alta Disponibilidad.* Obtenido de https://esperanza7989.files.wordpress.com/2011/10/tema-1-de-sad.pdf

epulpo. (29 de 05 de 2017). *La empresa colombiana SICTE obtiene las certificaciones ISO 27001 e ISO 20000 apoyándose en la potente y flexible solución ePULPO*. Obtenido de https://www.e-pulpo.com/content/la-empresa-colombiana-sicte-obtiene-las-certificaciones-iso-27001-e-iso-20000-apoy%C3%A1ndose-en-

Erb, M. (23 de 07 de 2018). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de 6. Amenazas y Vulnerabilidades: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

estudiantesunesur. (22 de 08 de 2016). *METODOLOGIA DE LA INVESTIGACION*. Obtenido de CAPÍTULO III “MARCO METODOLÓGICO”: https://estudiantesunesur.wordpress.com/2016/08/24/capitulo-iii-marco-metodologico-2/

Hoyos, A., Ortiz, Y., & Monsalve, A. F. (2010). *Proceso Certificacion 27001*. Obtenido de EMPRESAS CERTIFICADAS DE COLOMBIA: http://certificacion27001.blogspot.com/2010/09/empresas-certificadas-de-colombia.html

ICONTEC. (2006). *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001*. Bogotá: ICONTEC.

ICONTEC. (20 de 12 de 2013). *Norma Tecnica NTC-ISO-IEC COLOMBIANA 27001* . Obtenido de TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

Instituto de Tecnología de Massachusetts. (23 de 07 de 2018). *Red Hat Enterprise Linux 4: Introducción a la administración de sistemas*. Obtenido de Capítulo 6. Administración de cuentas de usuarios y acceso a recursos: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/ch-acctsgrps.html

ISO 27000.es. (2012). *¿Qué es un SGSI?* Obtenido de http://www.iso27000.es/sgsi.html

ISO 27000.es. (2012). *Serie 27000*. Obtenido de Beneficios: http://www.iso27000.es/iso27000.html#seccion2

ISO 27000.es. (23 de 07 de 2018). *Sistema de Gestión de la Seguridad de la Información.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Lobocom. (10 de 06 de 2005). *¿QUE SON LOS VIRUS?* Obtenido de https://www.lobocom.es/post/52/-que-son-los-virus-

Montañez León, G. (23 de 07 de 2018). *Análisis de las principales vulnerabilidades de un sistema informatico.* Obtenido de Principales vulnerabilidades:

https://gabrielsad.files.wordpress.com/2012/09/3-anc3a1lisis-de-las-principales-vulnerabilidades-de-un-sistema-informc3a1tico.pdf

Moreno, M. G. (1987). *Introducción a la metodologia de la investigación educativa.* Obtenido de http://gooogle-books.blogspot.com/2016/11/introduccion-la-metodologia-de-la.html

Perez Leal, J. (18 de 12 de 2017). *CÓMO DETERMINAR LA NATURALEZA DE SU TRABAJOS DE GRADO*. Obtenido de https://asesoriatesis1960.blogspot.com/2017/12/como-determinar-la-naturaleza-de-su.html

Rodriguez Moguel, E. (2005). *Metodología de la Investigación.* Obtenido de https://es.scribd.com/document/311168172/METODOLOGIA-DE-LA-INVESTIGACION-ERNESTO-A-RODRIGUEZ-MOGUEL-pdf

Sabino, C. (1992). *EL PROCESO DE INVESTIGACIÓN.* Obtenido de https://metodoinvestigacion.files.wordpress.com/2008/02/el-proceso-de-investigacion_carlos-sabino.pdf

Tatayo y Tamayo, M. (2003). *El Proceso de la Investigación Cientifica.* Obtenido de https://clea.edu.mx/biblioteca/Tamayo%20Mario%20-%20El%20Proceso%20De%20La%20Investigacion%20Cientifica.pdf

Vivanco, M. (06 de 05 de 2013). *Muestreo estadístico.* Obtenido de https://es.scribd.com/document/139625697/Manuel-Vivanco-Muestreo-estadistico-2

Wikipedia. (18 de 07 de 2018). *Archivo (informática)*. Obtenido de https://es.wikipedia.org/wiki/Archivo_(inform%C3%A1tica)

Wikipedia. (18 de 06 de 2018). *Buffer*. Obtenido de https://es.wikipedia.org/wiki/Buffer

Wikipedia. (21 de 07 de 2018). *Cracker*. Obtenido de https://es.wikipedia.org/wiki/Cracker

Wikipedia. (22 de 04 de 2018). *ISO/IEC 27000-series*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27000-series

Wikipedia. (18 de 06 de 2018). *Seguridad de la información*. Obtenido de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Anexo 1. Encuesta

ENCUESTA
Universidad Nacional Abierta y a Distancia - UNAD
Especialización en Gestión de Proyectos

Dirigido a todos los empleados de la Empresa Gestión & Negocios Administrativos SAS, involucrados con el manejo y uso de la información, manipulación de documentos electrónicos y físicos y la seguridad de la información.	
OBJETIVO: Analizar las vulnerabilidades en el manejo de la información, bajo la norma ISO 27001, para establecer estrategias de seguridad y minimizar los riesgos. La información de este documento será estrictamente confidencial, razón por la cual le pedimos el favor de contestar con exactitud y sinceridad los interrogantes que a continuación se enumeran. Escoja una sola opción:	
1. ¿Sabe usted si en la entidad existen políticas de seguridad de la información establecidas?	Si ☐ No ☐
2. ¿Está usted conforme con las políticas implantadas para proteger y salvaguardar la información?	Si ☐ No ☐
3. ¿Existe una persona encargada de realizar seguimiento, monitoreo y control a las políticas en el manejo de la información?	Si ☐ No ☐
4. ¿Ha tenido perdida de documento en la empresa?	Si ☐ No ☐
5. ¿Existen acciones correctivas cuando se presentan perdida de información?	Si ☐ No ☐
6. ¿Sabe usted si con frecuencia en la entidad realizan copias de seguridad de la información (Backus)?	Si ☐ No ☐
7. Los mayores riesgos ocasionados en la entidad con respecto al manejo de la información se presentan a través de:	**Descuido del Personal** ☐ **Ausencia de Controles** ☐ **Incumpliendo de Políticas** ☐ **Otros** ☐
8. ¿Qué medios utiliza para trasmitir la información dentro de la entidad?	**Internet** ☐ **Intranet** ☐ **Red Informática** ☐ **Otros** ☐
9. ¿En la entidad se encuentra disponible la información en el momento que sea necesario acceder a esta?	Si ☐ No ☐
10. ¿Considera usted que en la entidad la autenticidad y la confidencialidad que se tiene en el manejo de la información es adecuada?	Si ☐ No ☐
11. ¿Que le gustaría que se mejorara en la entidad con respecto al uso y manipulación de la información?	**Confidencialidad** ☐ **Integridad** ☐ **Disponibilidad** ☐ **Otros** ☐
12. ¿Se realiza periódicamente mantenimiento preventivo y correctivo a los equipos de computación utilizados en la empresa Gestión & Negocios Administrativos SAS?	Si ☐ No ☐
13. ¿El lugar donde se ubican los archivos están seguros de inundaciones, robos o cualquier otra situación que pueda poner en peligro la información?	Si ☐ No ☐

Anexo 2. Resultados de la encuesta

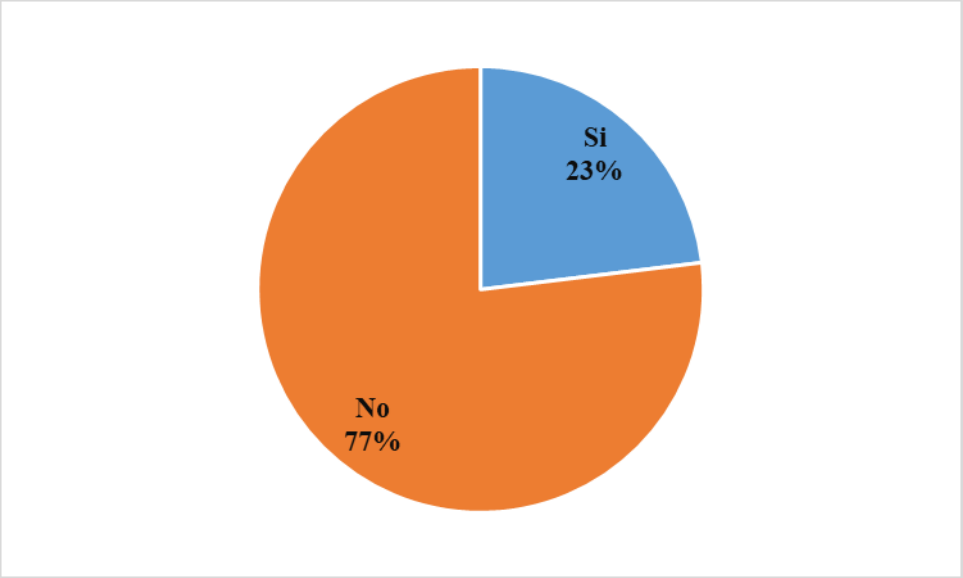
1. ¿Sabe usted si en la entidad existen políticas de seguridad de la información establecidas?

Tabla 1 Pregunta 1 Existencia de políticas de seguridad de la información

Variable	F. Absoluta	F. Relativa
Si	3	23%
No	10	77%
Total	**13**	**130%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 1 Pregunta 1 Existencia de políticas de seguridad de la información



Interpretación: Con relación a los resultados reflejados en el gráfico 1 el 77% de los encuestados contestaron No saber de la existencia en la entidad políticas de seguridad de la información, mientras que el 23% restante expresaron conocer la existencia de estas políticas de seguridad de la información. De lo anterior se evidencia, que en la empresa Gestión & Negocios Administrativos SAS la gran mayoría de los funcionarios desconocen las Políticas de Seguridad de la información.

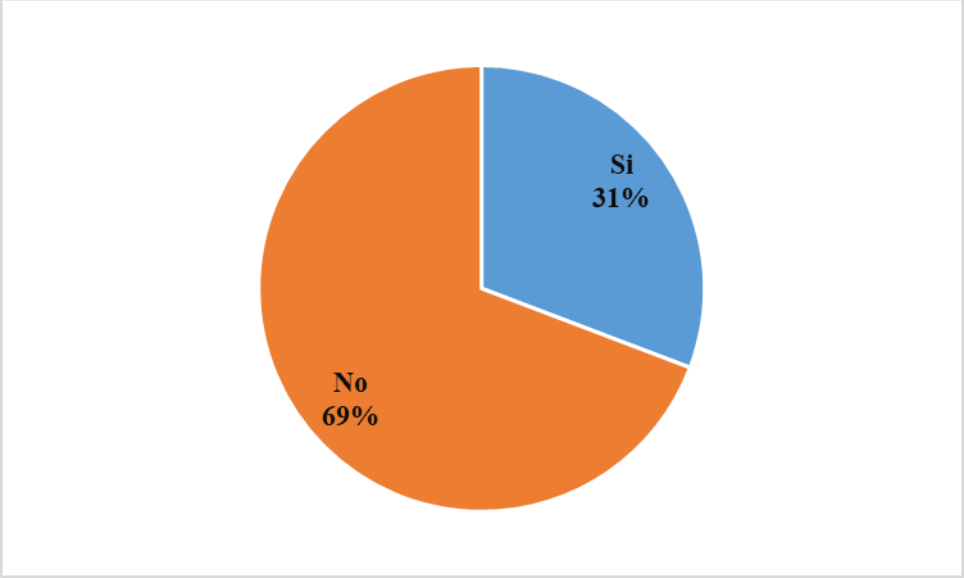
2. ¿Está usted conforme con las políticas implantadas para proteger y salvaguardar la información?

Tabla 2 Pregunta 2 Conformidad con la políticas de seguridad de la información actual

Variable	F. Absoluta	F. Relativa
Si	4	31%
No	9	69%
Total	**13**	**130%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 2 Pregunta 2 Conformidad con la políticas de seguridad de la información actual



Interpretación: Con relación a los resultados reflejados en el grafico 2 el 69% de los encuestados contestaron que NO están conformes con las políticas implantadas para proteger y salvaguardar la información, el 31% expresaron que SI. De lo anterior se observó que la mayoría de los empleados de la entidad no están conformes con las políticas de seguridad para proteger y salvaguardar la información.

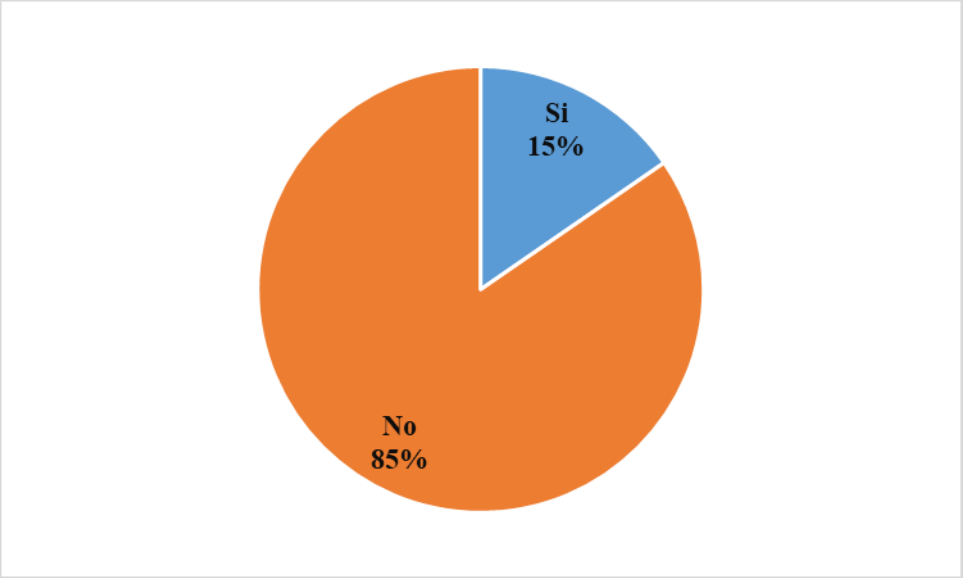
3. ¿Existe una persona encargada de realizar seguimiento, monitoreo y control a las políticas en el manejo de la información?

Tabla 3 Pregunta 3 Personal a cargo de las políticas de seguridad de la información

Variable	F. Absoluta	F. Relativa
Si	2	15%
No	11	85%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 3 Pregunta 3 Personal a cargo de las políticas de seguridad de la información



Interpretación: Con relación a los resultados reflejados en el grafico 3 el 85% de los encuestados contestaron que NO hay una persona encargada de realizar seguimiento, monitoreo y control a las políticas en el manejo de la información, el 15% respondieron que SI. De lo anterior se observó que en la empresa no realizan seguimiento, monitoreo y control a las políticas en el manejo de la información.

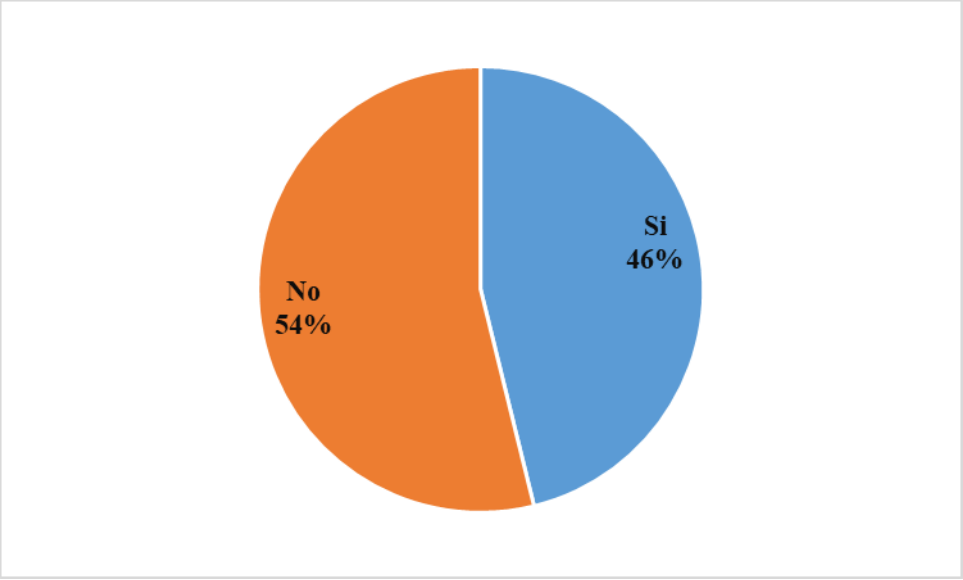
4. ¿Ha tenido perdida de documento en la empresa?

Tabla 4 Pregunta 4 Perdida de documentación

Variable	F. Absoluta	F. Relativa
Si	6	46%
No	7	54%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 4 Pregunta 4 Perdida de documentación



Interpretación: Con relación a los resultados reflejados en el grafico 4 el 46% de los encuestados contestaron que SI han tenido perdida de documento en la entidad, mientras que el 54% restante manifiestan NO haber registrado perdida de documentación. De lo anterior se observó que en la empresa se ha presentado perdida de documentos considerando que no dispone ni de un sistema de seguridad de información ni de políticas para tal fin.

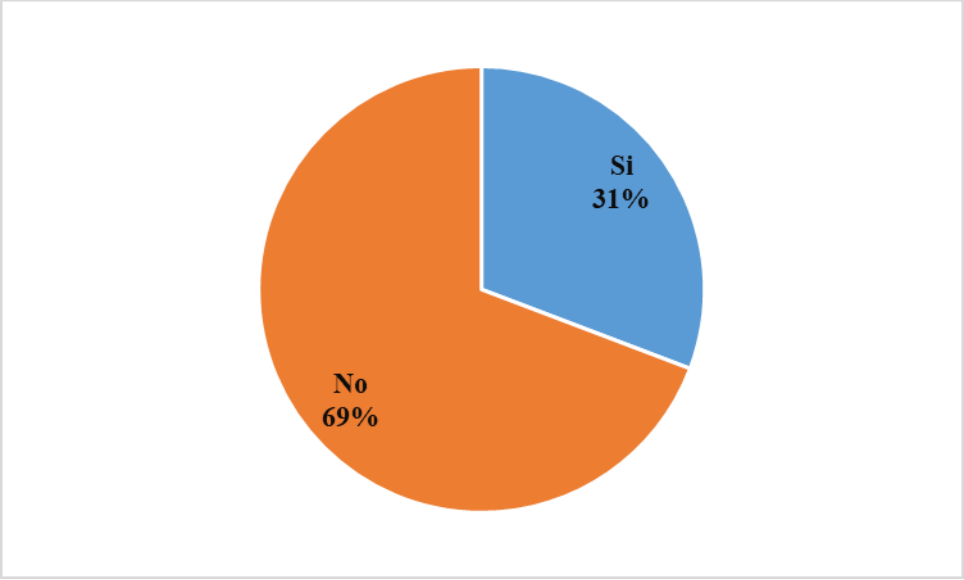
5. ¿Existen acciones correctivas cuando se presentan perdida de información?

Tabla 5 Pregunta 5 Acciones correctivas para perdida de documentación

Variable	F. Absoluta	F. Relativa
Si	4	31%
No	9	69%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 5 Pregunta 5 Acciones correctivas para perdida de documentación



Interpretación: Con relación a los resultados reflejados en el grafico 5 el 69% de los encuestados contestaron que NO existen acciones correctivas cuando se presentan perdida de información, el 31% manifestaron que SI. De lo anterior se concluyó que en la entidad no existen acciones correctivas cuando se presentan perdidas de información.

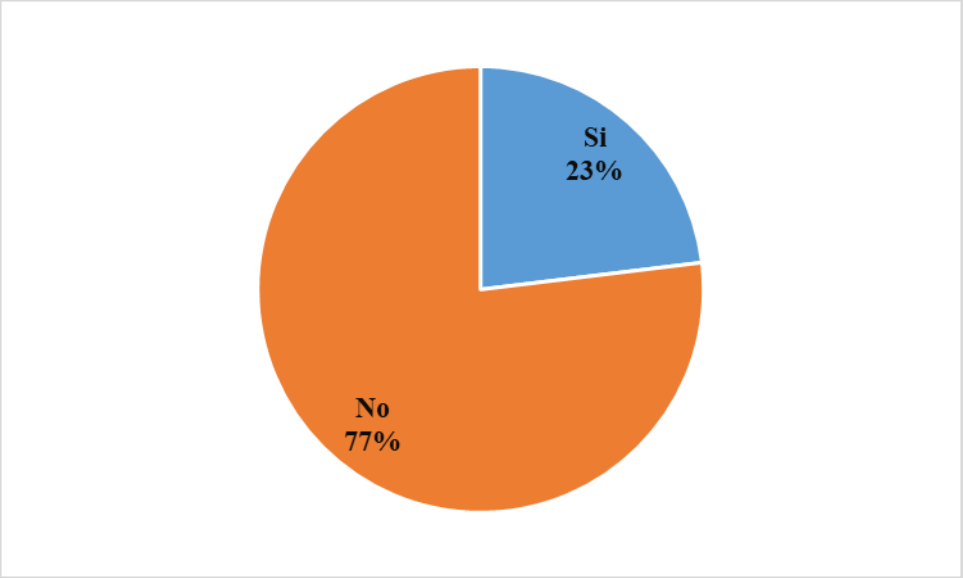
6. ¿Sabe usted si con frecuencia en la entidad realizan copias de seguridad de la información (Backus)?

Tabla 6 Pregunta 6 Frecuencia de la realización de copias de seguridad

Variable	F. Absoluta	F. Relativa
Si	3	23%
No	10	77%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 6 Pregunta 6 Frecuencia de la realización de copias de seguridad



Interpretación: Con relación a los resultados reflejados en el grafico 6 el 77% de los encuestados contestaron que NO conocían de la realizan o la periodicidad con la que en la empresa se realizan copias de seguridad de la información (Backus), el 23% expresaron que SI. De lo anterior se pudo observar que en la entidad existe desconocimiento al respecto de que si se realizan periódicamente copias de seguridad de la información.

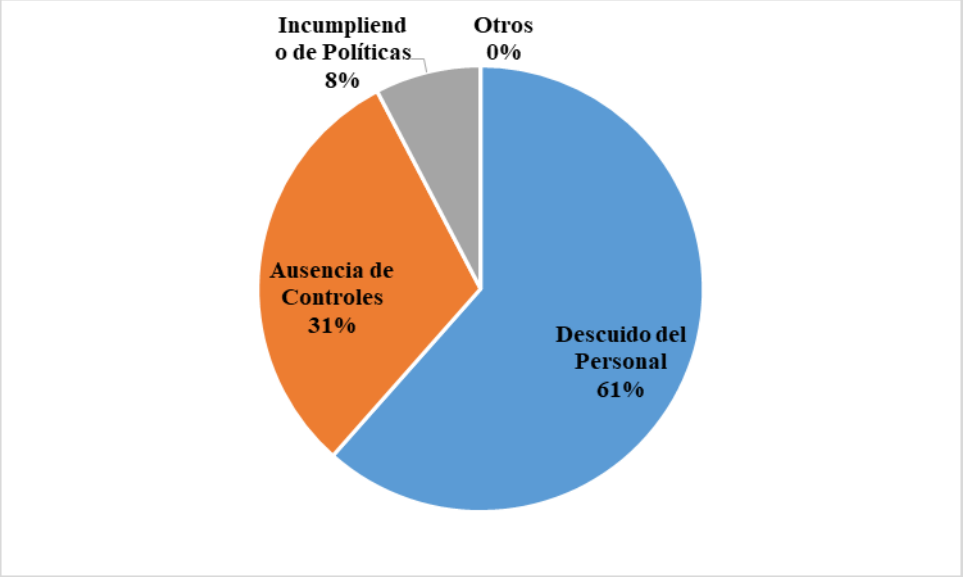
7. Los mayores riesgos ocasionados en la entidad con respecto al manejo de la información se presentan a través de:

Tabla 7 Pregunta 7 Riesgos de manejo de información

Variable	F. Absoluta	F. Relativa
Descuido del Personal	8	62%
Ausencia de Controles	4	31%
Incumpliendo de Políticas	1	8%
Otros	0	0%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 7 Pregunta 7 Riesgos de manejo de información



Interpretación: Con relación a los resultados reflejados en el grafico 7 el 61% de los encuestados contestaron que los mayores riesgos ocasionados en la entidad con respecto al manejo de la información se presentan por descuido del personal, el 31% ausencia de controles, mientras que el 8% restante respondieron que por Incumpliendo de políticas. De lo anterior se concluyó que en la entidad Los mayores riesgos ocasionados con respecto al manejo de la información se presentan por descuido del personal.

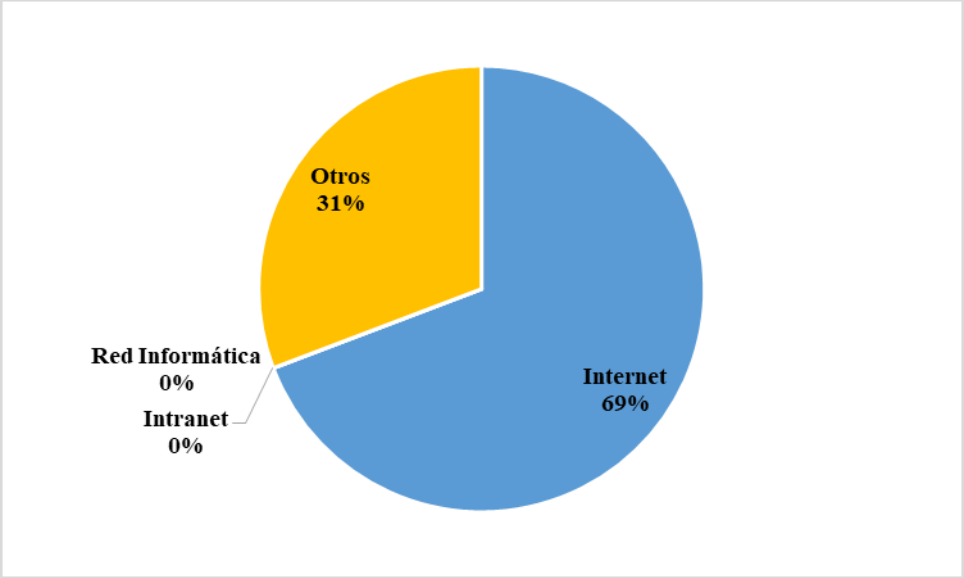
8. ¿Qué medios utiliza para trasmitir la información dentro de la entidad?

Tabla 8 Pregunta 8 Medios de trasmisión de información

Variable	F. Absoluta	F. Relativa
Internet	9	69%
Intranet	0	0%
Red Informática	0	0%
Otros	4	31%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 8 Pregunta 8 Medios de trasmisión de información



Interpretación: Con relación a los resultados reflejados en el grafico 8 el 69% de los encuestados contestaron que el medio más utilizado para trasmitir la información dentro de la entidad es el Internet, el 0% respondieron el Intranet, el 0% manifestaron Red Informáticas y el 31% restante respondieron otros. De lo anterior se observó que el medio que utilizan para trasmitir la información dentro de la entidad es el internet y otros medios electrónicos como memorias USB y medios impresos.

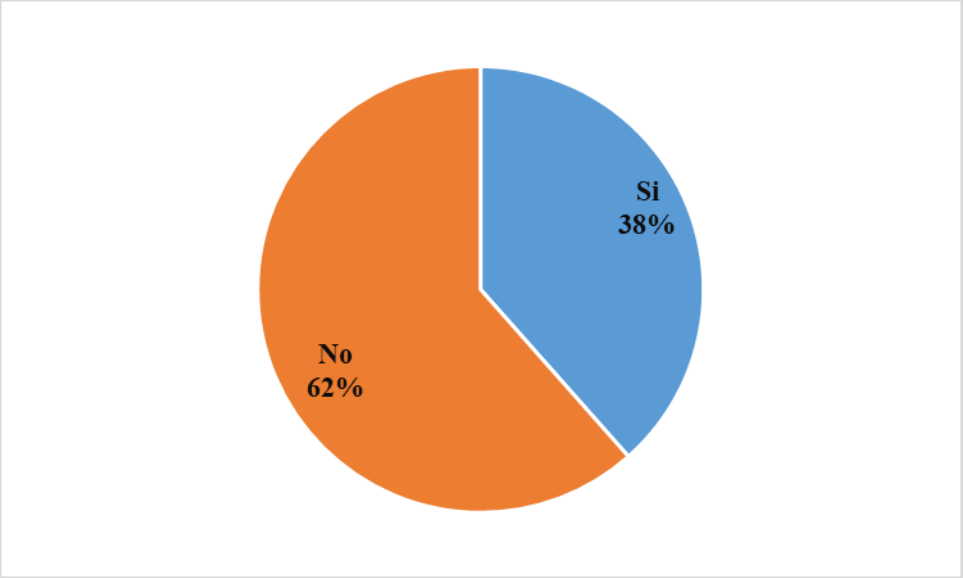
9. ¿En la entidad se encuentra disponible la información en el momento que sea necesario acceder a esta?

Tabla 9 Pregunta 9 Disponibilidad y acceso a la información

Variable	F. Absoluta	F. Relativa
Si	5	38%
No	8	62%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 9 Pregunta 9 Disponibilidad y acceso a la información



Interpretación: Con relación a los resultados reflejados en el grafico 9 el 620% de los encuestados contestaron que NO se encuentra disponible la información en el momento que sea necesario acceder a esta, el 38% manifestaron que SI. De lo anterior se concluyó que en la entidad no se encuentra disponible la información en el momento que sea necesario acceder a esta para llevar a cabo las actividades.

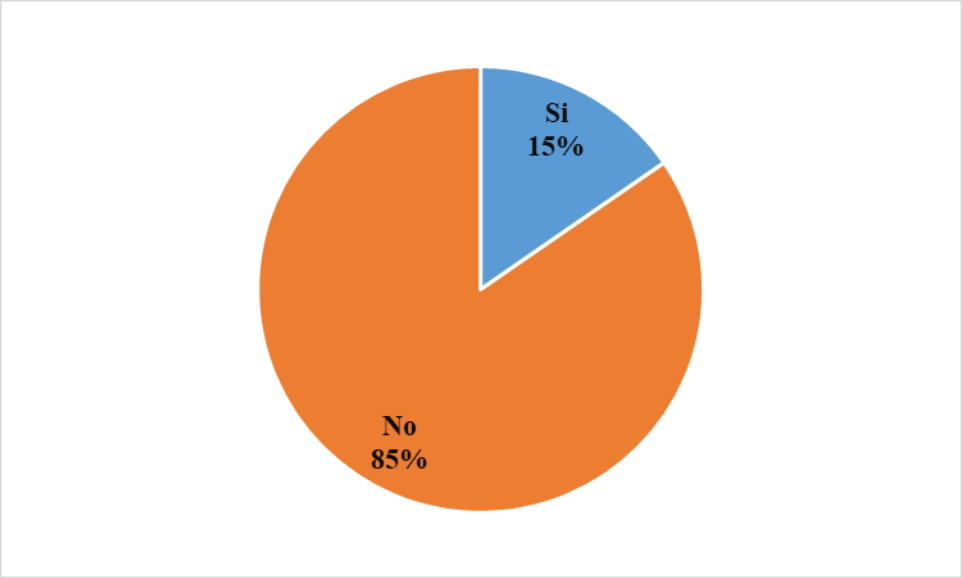
10. ¿Considera usted que en la entidad la autenticidad y la confidencialidad que se tiene en el manejo de la información es adecuada?

Tabla 10 Pregunta 10 Autenticidad y confidencialidad de la información

Variable	F. Absoluta	F. Relativa
Si	2	15%
No	11	85%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 10 Pregunta 10 Autenticidad y confidencialidad de la información



Interpretación: Con relación a los resultados reflejados en el grafico 10 el 85% de los encuestados manifestaron que NO considera que en la entidad la autenticidad y la confidencialidad que se tiene en el manejo de la información es adecuada, el 15% contestaron que SI. De lo anterior se evidencio que la mayoría de los empleados NO considera que la autenticidad y la confidencialidad que se tiene en el manejo de la información es adecuada en la entidad.

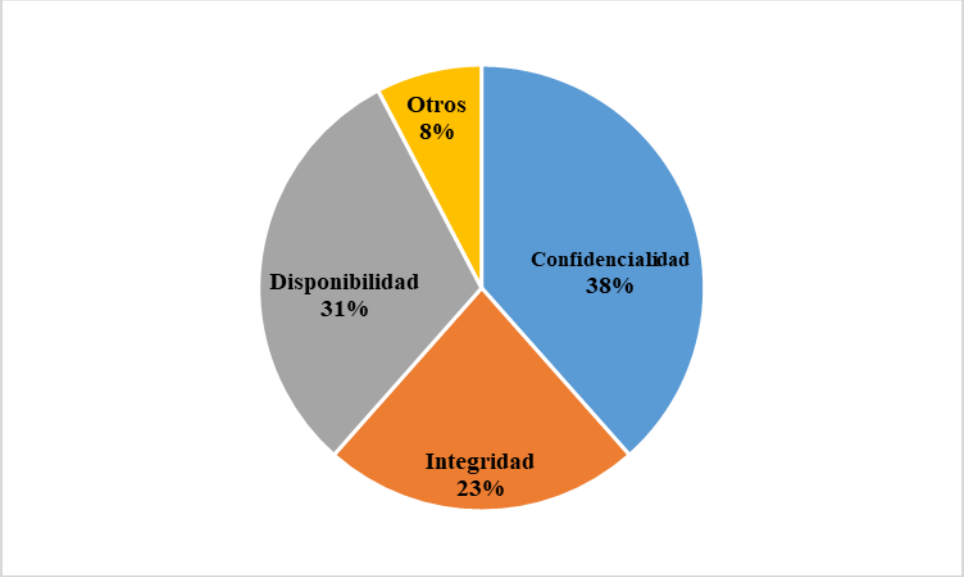
11. ¿Que le gustaría que se mejorara en la entidad con respecto al uso y manipulación de la información?

Tabla 11 Pregunta 11 Uso y manipulación de la información

Variable	F. Absoluta	F. Relativa
Confidencialidad	5	38%
Integridad	3	23%
Disponibilidad	4	31%
Otros	1	8%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 11 Pregunta 11 Uso y manipulación de la información



Interpretación: Con relación a los resultados reflejados en el grafico 11 el 38% de los encuestados contestaron que le gustaría que se mejorara en la entidad con respecto al uso y manipulación de la información es la confidencialidad, el 31% respondieron la disponibilidad, el 23% manifestaron la integridad, el 8% respondieron otros. De lo anterior se evidencio que a los empleados de la entidad les gustaría que se mejorara la confidencialidad con respecto al uso y manipulación de la información.

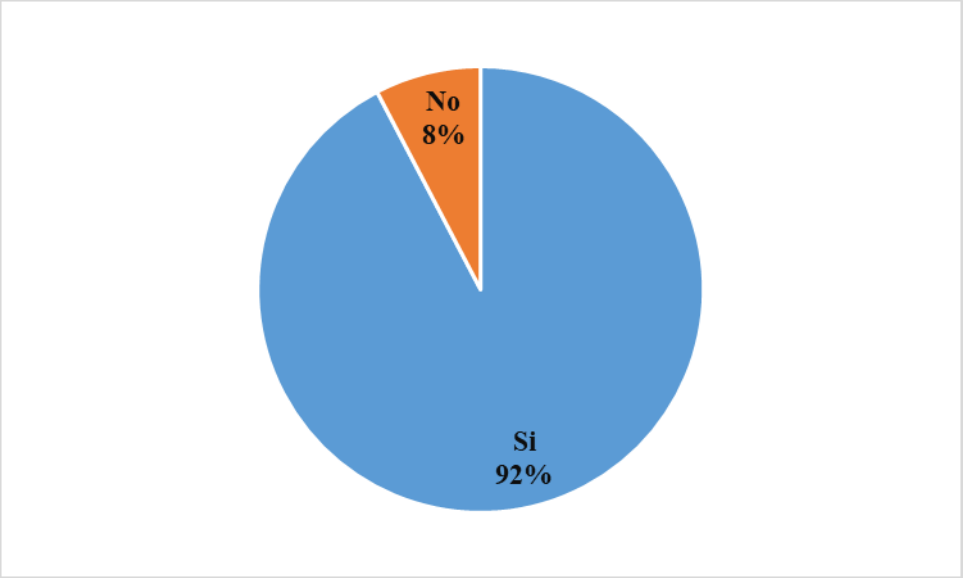
12. ¿Se realiza periódicamente mantenimiento preventivo y correctivo a los equipos de computación utilizados en la empresa Gestión & Negocios Administrativos SAS?

Tabla 12 Pregunta 12 Periodicidad del mantenimiento preventivo y correctivo

Variable	F. Absoluta	F. Relativa
Si	12	92%
No	1	8%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 12 Pregunta 12 Periodicidad del mantenimiento preventivo y correctivo



Interpretación: Con relación a los resultados reflejados en el grafico 12 el 92% de los encuestados manifestaron que NO realizan periódicamente mantenimiento preventivo y correctivo a los equipos de computación utilizados en la empresa, 8% expresaron que SI. De lo anterior se pudo observar que en la entidad no realizan periódicamente mantenimiento preventivo y correctivo a los equipos de computación utilizados en la empresa para minimizar los riesgos.

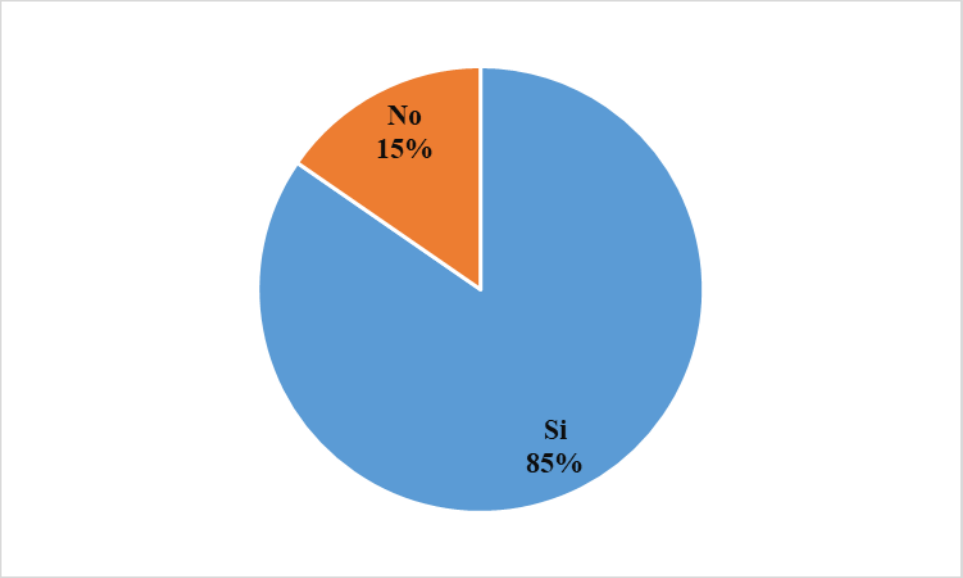
13. ¿El lugar donde se ubican los archivos están seguros de inundaciones, robos o cualquier otra situación que pueda poner en peligro la información?

Tabla 13 Pregunta 13 Seguridad del espacio donde se ubica el archivo

Variable	F. Absoluta	F. Relativa
Si	11	85%
No	2	15%
Total	**13**	**100%**

Fuente: Datos obtenidos a través de la encuesta.

Gráfico 13 Pregunta 13 Seguridad del espacio donde se ubica el archivo



Interpretación: Con relación a los resultados reflejados en el grafico 13 el 85% de los encuestados contestaron que SI que el lugar donde se ubican los archivos están seguros de inundaciones, robos o cualquier otra situación que pueda poner en peligro la información, 15% expresaron que NO. De lo anterior se pudo observar que el lugar donde se ubican los archivos están seguros de inundaciones, robos o cualquier otra situación que pueda poner en peligro la información.

Anexo 3. Descripción de la empresa

Gestión & Negocios Administrativos SAS es una compañía prestadora de servicios, de naturaleza privada, quienes desde el año de 2009 realizamos asesorías, interventorías, consultorías e investigación técnica y aplicada en procesos de reingeniería organizacional, tareas gerenciales de mejoramiento institucional, planeación, Control Interno, Auditorias técnica, administrativa, jurídica y Financiera a proyectos Sociales, diseño e implementación de programas y procesos de garantía de la calidad y planes de mejoramiento en las diferentes áreas que se manejan en la organización, en las áreas de Salud, Educación, económicas, agrícolas, de seguros, Asesorías en gestión Humana y Proyectos Sociales, de Obras, etc. Igualmente, el suministro de papelería y dotación para oficina y elementos de seguridad industrial y seguridad en el trabajo, sumado a actividades académicas, capacitación, investigación y proyección social. Fieles a nuestra vocación de servicio contribuimos a la formación continua del talento humano: profesionales, estudiantes y/o empleados de los sectores públicos y privados, a través de procesos de capacitación.

Tabla 14 Ficha técnica Gestión & Negocios Administrativos SAS

Nombre: Gestión & Negocios Administrativos S.A.S.
NIT: 900.278.213-0 **Sigla:** Gestión
Dirección: Calle 11B No. 16 – 04 Esquina **Tel:** 7280643
Correo electrónico: gestionltda1@gmail.com
Representante Legal: **LUZ ALEJANDRA FIGUEROA ROMERO**

Visión

Ser en el año 2025 una empresa líder a nivel regional y nacional en la implementación de soluciones, evaluación y análisis en el área de auditoría de salud, ciencias económicas, empresariales, agrícolas y ambientales, educación y obras civiles, manteniendo un alto nivel de permanencia, para ser identificados como símbolo de excelencia y responsabilidad por la comunidad y el sector empresarial.

Misión

Nuestra misión es ofrecer servicios de alta calidad en auditorias, interventorías, asesorías y consultorías en las áreas de la salud, ciencias económicas, empresariales, agrícolas y ambientales, educación y obras civiles, con el fin de contribuir a la generación de valores agregados que nuestros clientes necesitan con un personal altamente especializado en diversos procesos.

Principios guías

La calidad. Para lograr la satisfacción de nuestros clientes y beneficiarios, la calidad de los servicios prestados es nuestra mayor prioridad.

Los clientes y beneficiarios como punto central de todo lo que hacemos. Nuestro trabajo se hace teniendo en cuenta los requerimientos de nuestros clientes, con una alta competencia y en búsqueda de su satisfacción.

El mejoramiento continuo es esencial para el éxito. Se trabaja continuamente para llegar a la excelencia en todos nuestros procesos, servicios, relaciones humanas y competitividad.

El sentido de pertenencia de los colaboradores de la empresa. Somos un equipo de trabajo basado en la confianza y el respeto, con el objeto de conseguir los mejores resultados.

Los proveedores son nuestros socios: La empresa mantiene relaciones que benefician tanto los proveedores como a sus asociados.

La integridad nunca se debe comprometer: La empresa busca ser socialmente responsable e imponer respeto e integridad para contribuir positivamente a la sociedad. Nuestras puertas están abiertas sin ningún tipo de desigualdad, discriminación y consideraciones de origen étnico o de creencias personales.

Experiencia

Capacitación, investigación y formación. Tenemos un record importante en la realización de capacitaciones donde le hemos servido a clientes como la Alcaldía Municipal de Albania, Riohacha, Maicao, San Juan del cesar, Villanueva, Dibulla, Barrancas y una gran cantidad de Empresas privadas donde sus Directivos, Empleados y Comunidad en general han encontrado en la Empresa la oportunidad de actualización y capacitación a través de la realización, Diplomados que desarrollamos en convenio con Universidades, Cursos, Seminarios,

Talleres, Congresos, Foros y Conferencias; Permitiéndoles la actualización, sensibilización y capacitación en la búsqueda permanente de conocimiento, coadyuvando al mejoramiento de la calidad Laboral y profesional de todos los asistentes y beneficiarios de nuestra labor.

Proyectos rurales y medioambientales. Formular, estructurar, desarrollar, ejecutar y/o evaluar planes, programas y proyectos orientados a la producción agropecuaria, pesquera, minera, industrial, microempresaria y comercialización de las mismas.

Formular, gestionar, ejecutar y evaluar planes, programas y/o proyectos referentes a cuidado y conservación del medio ambiente.

Obras civiles, infraestructuras e ingenierías. Formulación y/o realización de estudios de obras civiles, infraestructura e ingeniería. Formular gestionar, fomentar y ejecutar planes o proyectos para la adquisición y/o mejoramiento de vivienda de interés social, construcción de calles, andenes, zonas verdes.

Construcción de vías terciarias, diseños y construcción de canales de riego y drenaje, desarrollar programas y proyectos para la construcción de proyectos de saneamiento básico, estudios de suelos.

Asesorías, consultorías e interventorías. Contamos con un equipo multidisciplinario de profesionales vinculados a la docencia, investigación y al ejercicio de sus profesiones que nos permite Ofrecer y realizar asesorías, consultorías a entidades públicas y privadas en materia política, económica, contable, tributaria, financiera, jurídica, administrativa, organizacional, operativa y acciones de desarrollo institucional.

Realización de interventorías financieras, administrativas y técnicas a obras civiles, ingeniería, ambientales, entre otros

Ofrecer y desarrollar consultorías, asesorías, asistencia técnica y acompañamiento a entidades e instituciones del sector público en materia organizacional, administrativas, presupuestales, planeación, financiera, contables, legales.

Proyectos para municipios, gobernaciones y demás entes descentralizados. Asesorías a entes territoriales relacionadas con la implementación de bancos de proyectos para la inversión pública. Brindar asesorías, acompañamiento y/o ejecución de acciones para la formulación, estructuración, ejecución, y evaluación de planes departamentales, distritales y municipales de desarrollo y en planes, programas y proyectos sectoriales.

Brindar asesorías, acompañamiento y asistencia profesional y técnica a entidades territoriales y empresas sociales del estado en la formulación y adopción de programas de saneamiento fiscal, financiero y contable.

Brindar asesorías, asistencia técnica y/o acompañamiento a entidades territoriales en organización, gestión y manejo de los fondos territoriales de salud y demás fondos especiales creados por el legislador en aspectos legales, administrativos, presupuestales, contables, manejo de tesorería, entre otros.

Formular, elaborar y/o actualizar estatutos presupuestales y contractuales. Estructurar y desarrollar estudios de eficiencia a instituciones de los sectores de salud, educación, agua potable, saneamiento básico, entre otras.

Programas de apoyo y ejecuciones en el sector salud. Realizar auditorías financieras, contables, cuentas de cobro, administrativas y la prestación de servicios de salud a empresas sociales del estado e instituciones prestadoras de servicio de salud pública y privada.

Gestionar y realizar estudios y análisis a la gestión, organización, presupuestario, prestación de servicios, eficiencia y viabilidad financiera de las E.S.E e instituciones prestadoras de servicio de salud. Mediante acuerdo de voluntades, outsourcing o cualquier forma de tercerización gestionar, realizar y/o mejorar los procesos de facturación de la prestación de servicios de salud en las E.S.E e instituciones prestadoras de salud. Cobro y recuperación de cartera. Realizar interventoría a los contratos de aseguramiento y afiliación a SGSSS del régimen subsidiado de salud firmados con las entidades territoriales.

Brindar acompañamiento y asistencia profesional y técnica en lo referente al sistema de gestión de calidad, acompañamiento y asesoramiento a los procesos de habilitación y acreditación para la prestación de servicios de salud. Formulación, coordinación ejecución y/o evaluación de planes, programas y proyectos en salud pública.

Dotaciones oficinas y papelería en general. Gestión & Negocios Administrativos SAS apoyando el sector empresarial ofrece el suministro para dotación de toda clase de muebles, enseres y equipos de oficina.

Así, como equipos tecnológicos de comunicación, computación e impresión, de sonidos, audiovisuales, proyectores, cámaras, videograbadoras, demás elementos requeridos para el buen funcionamiento empresarial.

Además del suministro de papelería y elementos de uso administrativo en las oficinas.

Dotaciones de personal y suministro de elementos de seguridad industrial y seguridad en el trabajo. Gestión & Negocios ofrece el suministro de toda clase de dotaciones industriales y ocupacional, materiales de seguridad en el trabajo y protección industrial a nivel Administrativo y Operativo.

Así como los elementos necesarios para prevención y seguridad en las instalaciones de trabajo y de primeros auxilios.

Nuestros clientes

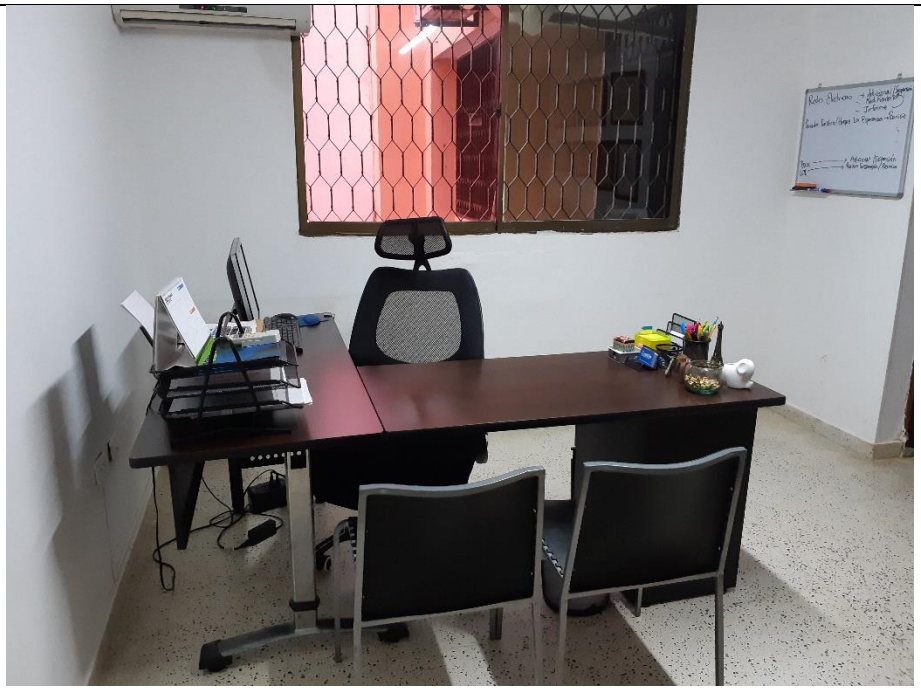
Los clientes son el mayor patrimonio de Gestión & Negocios, dentro de los cuales tenemos:

- Departamento de La Guajira
- Departamento del Cesar
- Municipio de Albania
- Municipio de Barrancas
- Municipio de Dibulla
- Distrito de Riohacha
- Municipio de Maicao
- Municipio de Manaure
- Municipio de Villanueva
- Municipio de San Juan del Cesar
- Municipio de San Diego - Cesar

- RGO Soluciones Integrales
- Fundación Nueva Vida
- Fondo de Desarrollo Empresarial de Barrancas “FONDEBA”
- Anas Wayuu E.P.S.I. Entidad Promotora de Salud Indígena
- Asociación de Trabajadores Independientes – ASOTRAINDAL
- Entre otros…

Anexo 4. Registro fotográfico

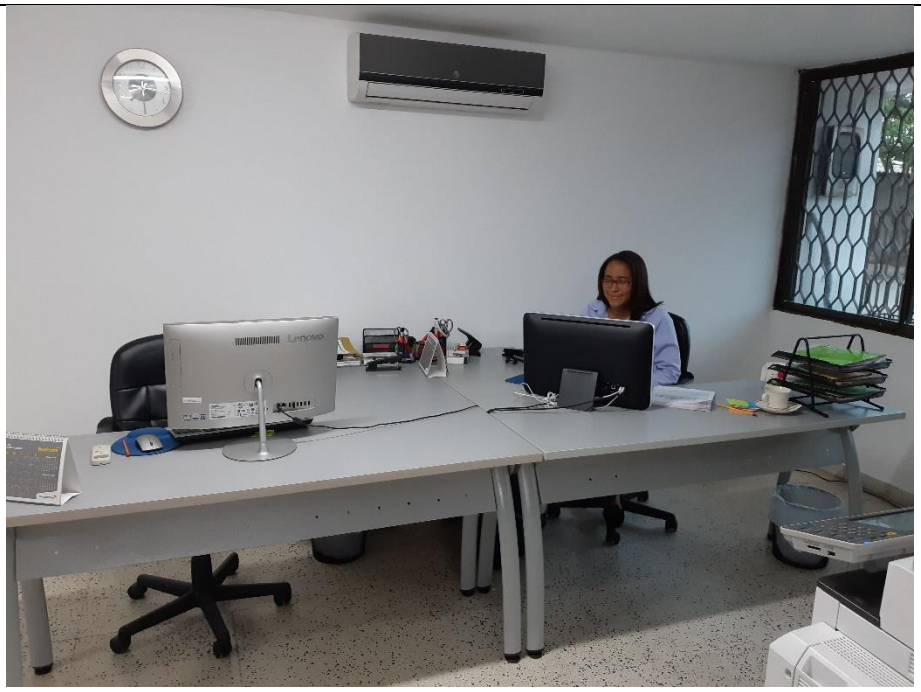
Área de Archivo



Gerencia

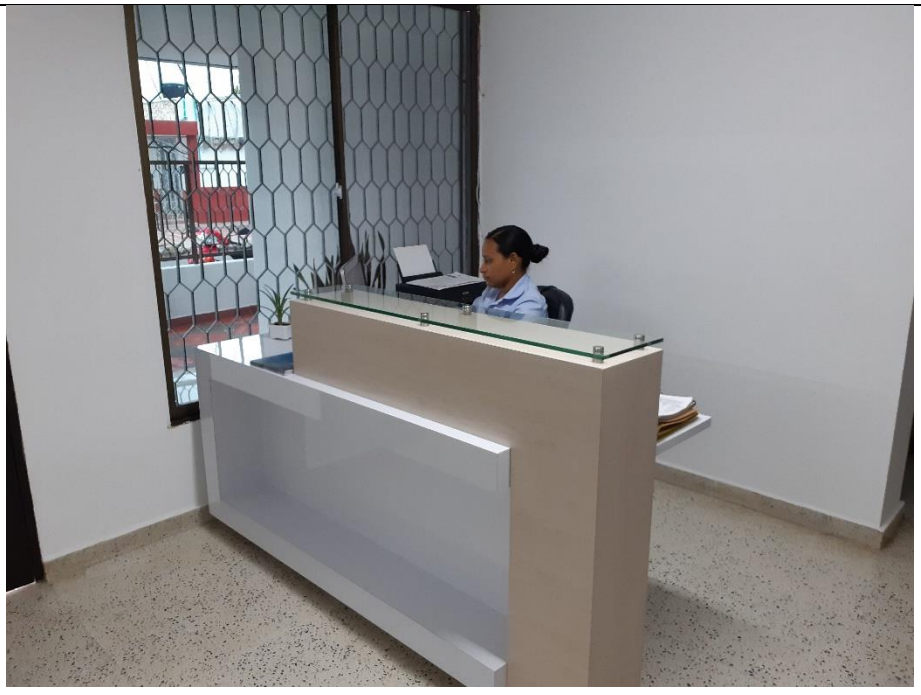
Sala de juntas

Centro de copiado e impresión



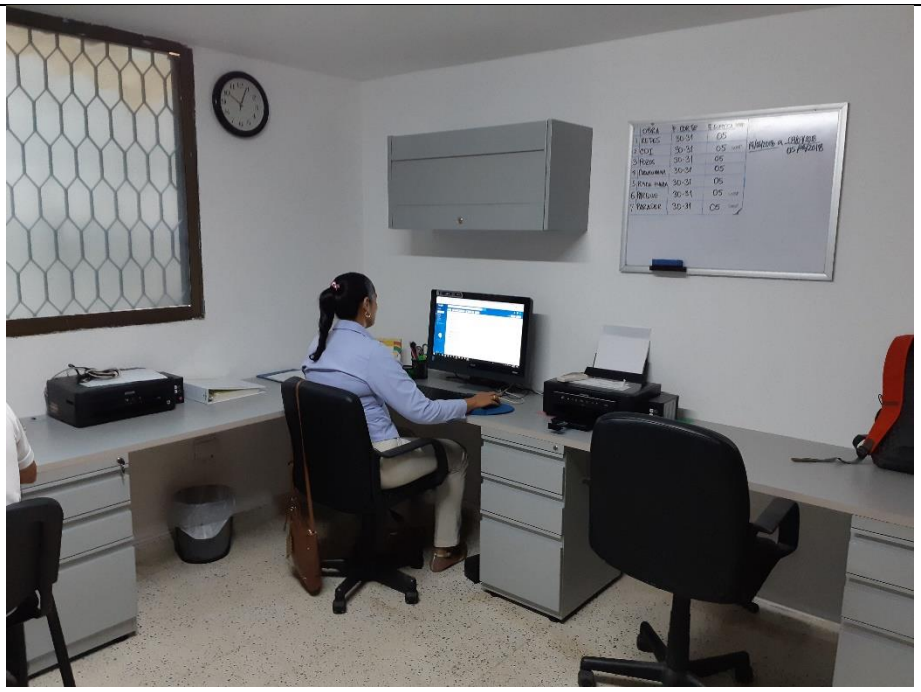
Puestos de trabajo

Puestos de trabajo



Puestos de trabajo

Puestos de trabajo



Puestos de trabajo