DOCUMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA DON POLLO SAS ARMENIA

RICARDO ARANZALES PAVA
CARLOS ANDRÉS GIRALDO LONDOÑO

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE CIENCIAS EMPRESARIALES
ESPECIALIZACIÓN EN GESTIÓN DE LA CALIDAD Y NORMALIZACIÓN TÉCNICA
ARMENIA – QUINDÍO
2019

DOCUMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA DON POLLO SAS ARMENIA

RICARDO ARANZALES PAVA
CARLOS ANDRÉS GIRALDO LONDOÑO

Trabajo presentado como proyecto para optar al título de
ESPECIALISTA EN GESTIÓN DE LA CALIDAD Y NORMALIZACIÓN TÉCNICA

Director
ING. FERNANDO JAIME ESCOBAR BOTERO

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE CIENCIAS EMPRESARIALES
ESPECIALIZACIÓN EN GESTIÓN DE LA CALIDAD Y NORMALIZACIÓN TÉCNICA
ARMENIA – QUINDÍO
2019

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, software, hardware, soportes, edificios, personas...) que tenga valor para la organización.

AGR: Sigla utilizada para Análisis y Gestión del Riesgo

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGO: Uso sistemático de la información para identificar fuentes y estimar riesgos.

BACKUP: Copia de seguridad. Esta se realiza para prevenir una posible pérdida de información.

CIBERDELINCUENTE: Se refiere a la persona que comete delitos contra computadoras y sistemas de información, con el objetivo de lograr el acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo.

CIBERESPACIO: El ciberespacio se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir.

COMERCIO ELECTRÓNICO: De acuerdo con la Organización Mundial del Comercio - OMC, el comercio electrónico es la distribución, mercadeo, venta o entrega de bienes y/o servicios hecha con medios electrónicos.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTINUIDAD DEL NEGOCIO: Es un concepto ligado a la gestión de riesgos empresariales cuya finalidad es analizar los riesgos a que están expuestos los negocios y las operaciones, así como las consecuencias que provocarían dichos riesgos centrándose en el impacto de la interrupción del negocio, identificando cuales son los productos y servicios de los que la organización depende para su supervivencia.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información

por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DATO: Los datos son, así, la información (valores o referentes) que recibe el computador a través de distintos medios, y que es manipulada mediante el procesamiento de los algoritmos de programación. Su contenido puede ser prácticamente cualquiera: estadísticas, números, descriptores, que por separado no tienen relevancia para los usuarios del sistema, pero que en conjunto pueden ser interpretados para obtener una información completa y específica.

DATOS PERSONALES: Es cualquier información que pueda ser relacionada con una persona.

Ejemplo: Su nombre, la dirección de su casa, su información bancaria, número de documento de identidad, fotografía, etc.

DECLARACIÓN DE APLICABILIDAD: Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del ISMS.

DELITO INFORMÁTICO: Toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software a que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como Infracción Informática.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

EVALUACIÓN DE RIESGO: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significancia del riesgo.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

HACCP: Análisis de peligros y puntos críticos de control por sus siglas en inglés. Proceso sistemático preventivo para garantizar la inocuidad alimentaria.

IDS/IPS: Sistema de Prevención de Intrusos por sus siglas en inglés. Es un software que ejerce el control de acceso a una red.

IMPACTO: El coste para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros. Por ejemplo, pérdida de reputación, implicaciones legales, etc.

INCIDENTE DE SEGURIDAD: Uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

INGENIERÍA SOCIAL: Conjunto de técnicas que utilizan los ciberdelincuentes para engañar a los usuarios y extraer su información.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO: Sigla que hace referencia a “Organización Internacional de Normalización” (“International Organization for Standardization”, en inglés).

ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM): Sistema de administración de la seguridad de la información. Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

LOG: Se refiere a la grabación secuencial en un archivo o en una base de datos de todas las operaciones que afectan un proceso informático.

NAT/PAT: Traducción de Direcciones de Red por sus siglas en inglés. Permite que las redes IP privadas que usan direcciones IP no registradas se conecten a Internet.

NTC: Sigla que hace referencia a “Norma Técnica Colombiana”.

POLÍTICA: Una política es un comportamiento propositivo, intencional, planeado, no simplemente reactivo, casual. Se pone en movimiento con la decisión de alcanzar ciertos objetivos a través de ciertos medios: es una acción con sentido. Es un proceso, un curso de acción que involucra todo un conjunto complejo de decisiones y operadores.

POLÍTICA DE SEGURIDAD: La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

PROPIETARIO DEL RIESGO: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RISK ASSESMENT: Es un término utilizado para referenciar la evaluación de riesgos, que describe un proceso o método general para identificar los peligros y los factores de riesgo que pueden ocasionar algún daño.

SAGRLAFT: Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SEGURIDAD INFORMÁTICA: La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.

SGSI: Sistema de Gestión de la Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

TI: Sigla que hace referencia a Tecnologías de la Información. Dentro de las referencias al área de tecnologías en las empresas es común utilizar TI o TIC.

TIC: Sigla que hace referencia a Tecnologías de la Información y las Comunicaciones.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de mediciones para modificar el riesgo.

UTM: Gestión Unificada de Amenazas por sus siglas en inglés. Solución de seguridad en un único producto que ofrece varias funciones.

VALORACIÓN DE RIESGO: Totalidad de los procesos de análisis y evaluación de riesgo.

VPN: Red Privada Virtual por sus siglas en inglés. Permite la extensión segura de la red de área local sobre una red pública no controlada como internet.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

INTRODUCCIÓN

La información es un valioso activo del que depende el buen funcionamiento de La empresa, mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de negocio.

En la actualidad el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios e interactuar con la sociedad, a la vez que ha aumentado los riesgos para las empresas, exponiéndolas a nuevas amenazas.

Es por esto que ha sido importante desde tiempos inmemorables implementar los medios necesarios para evitar el robo y manipulación de los datos confidenciales. Es así como la Empresa Don Pollo SAS Armenia empezará un proceso de diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) lo cual otorgará un beneficio en la implantación de las políticas y controles resultado de este proyecto. Las políticas son determinadas a raíz de la gestión de cada uno de los riesgos que comprometen de alguna manera la seguridad de la información dentro de la Empresa, dando una asignación formal de responsabilidades a cada uno de los involucrados, permitiendo así la continuidad dentro del negocio en caso de algún evento que pueda perjudicar este valioso activo.

Como complemento esencial del desarrollo del proyecto, se requiere la incorporación de un método sistemático para la valoración y tratamiento de los riesgos de los activos de la información. Se ha considerado utilizar los modelos suministrados en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2015 y la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT 3.0 de España.

1. PLANTEAMIENTO DEL PROBLEMA

El avance tecnológico ha traído consigo cambios significativos en los hábitos de la sociedad, la generación de conocimiento e información se ha convertido en la principal fuente de productividad, poder y trascendencia en el mercado, las grandes cantidades de información que a diario se generan y se procesan han creado un universo virtual soportado en los grandes almacenes de datos y las infraestructuras tecnológicas; ese universo intangible que rompe barreras de espacio y tiempo ha desplazado y modificado procesos como la imprenta, mano de obra, producciones cinematográficas y musicales, comercio, relaciones interpersonales, etc. Aunque muchos aspectos han cambiado, la información la han considerado como el alma de las empresas y de su forma de hacer negocios. Este preciado activo llamado información se ha convertido en el más importante de las organizaciones y las amenazas hacia él aumentan cada día, así como la manera crear, difundir y almacenarla. Los datos son intangibles y no se puede estimar hasta cuándo y cuánto va a crecer, así como determinar si estamos en la capacidad de dar tratamiento y gestión a toda esta información de tal manera que se pueda preservar su confidencialidad, integridad y disponibilidad.[1]

La implementación de herramientas informáticas a través de las décadas ha generado alta dependencia y evolución permanente en las infraestructuras y tecnologías utilizadas; anteriormente las redes de computadoras eran simples y desarrollaban tareas muy básicas que se monitoreaban bajo la supervisión de unas pocas personas en una misma área definida dentro de las empresas. En la década de los años 60 surge la primera red de computadoras a raíz de una estrategia militar, llamada ARPANET, luego se impulsó con la motivación de realizar prácticas académicas y científicas; se puede decir que este fue el punto de partida para la red de redes hoy llamada INTERNET, así mismo fue aumentando la cantidad de computadoras interconectadas, los sistemas de almacenamiento de datos y sus métodos de transferencia.

El cambio de paradigma y la transformación digital se ha incorporado en la sociedad cambiando la economía y la cultura para siempre. La generación, procesamiento, distribución y almacenamiento del conocimiento y de la información son la principal fuente de sostenimiento, poder y evolución de las empresas. Internet y las redes de telecomunicaciones evolucionaron de una manera que jamás se había imaginado; al principio los avances se daban lentamente y con sistemas de control adaptados al momento; hoy en día la innovación y la comunicación se producen a gran velocidad, las empresas y sus maneras de hacer negocios se enfrentan a un reto

[1] PORCELLI, Adriana Margarita. (Des) Protección del derecho de autor en la era digital. Principales tendencias legislativas, doctrinarias y jurisprudenciales argentinas sobre la denominada “piratería informática” / (DIS) protection of copyright in the digital age. Major argentine.... REVISTA QUAESTIO IURIS». Accedido 12 de abril de 2019. p. 14-18.

lleno de incertidumbres ya que los datos se encuentran en permanente cambio, transporte y hacia diferentes medios; la capacidad sensorial y de reacción del ser humano se percibe como lenta ante las múltiples formas de gestionar volúmenes de datos y tomar decisiones asistidas por computadoras.[2]

En la medida que el uso de los sistemas de información se expande y se apoyan en la tecnología, más personas dependen de su continuidad operativa. El crecimiento exponencial de las Tecnologías de la Información y Comunicación (TIC) dentro de las empresas ha generado nuevas necesidades de aprendizaje y conocimiento para la supervivencia de las mismas, cada día es más la dependencia de las herramientas tecnológicas en la operación de todos los procesos de negocio, las necesidades y expectativas de los clientes, así como de las partes interesadas han provocado la inmersión en los procesos informáticos y demostrar una actuación responsable, veraz y empoderada de las exigencias que esto conlleva.[3]

La masificación de dispositivos móviles de comunicación y la facilidad para acceder a los mismos ha creado una sociedad totalmente mediada por las relaciones computarizadas colocando en riesgo la privacidad de las personas y de la información que por allí se trasmite; esta evolución ha alcanzado tal magnitud que la historia de vida de las personas y sus datos personales se han puesto a disposición del mundo interconectado, esto hace que la delincuencia pase de un ambiente físico a un ambiente virtual. Los datos personales y la información crítica de las empresas se han convertido en un atractivo para extorsionar, dañar la imagen o reputación, interrumpir las actividades de negocio, hacer seguimiento de las rutinas e implementar cualquier método que pueda comprometer la integridad de las personas o la continuidad del negocio. Sin lugar a dudas, la información ya se posee un gran valor económico que las empresas no logran cuantificar.

La interconexión en el mundo digital ha ocasionado que las empresas se expongan ante la sociedad dejando rastros de sus características de negocio, estrategias de competitividad, estados financieros y un sin número de movimientos internos que puedan ser utilizados por la competencia y afectar negativamente el normal desarrollo en el mercado. La información está puesta al servicio de las redes de comunicación rompiendo barreras de tiempo, geolocalización y espacio, ahora la competencia no es solo local, la tendencia adicional es permanecer competitivos en internet. Algunas de las realidades que la empresa debería considerar para establecer un panorama e invertir en la seguridad de la información son:

[2] SERRANO COBOS, Jorge. Tendencias tecnológicas en internet hacia un cambio de paradigma. El Profesional de la Información vol 25, no 6 (14 de noviembre de 2016). p. 2.

[3] SOLANO RODRÍGUEZ, Omar Javier; GARCÍA PÉREZ, Domingo y BERNAL, Juan Jesús. El sistema de información y los mecanismos de seguridad informática en la pyme. Punto de Vista vol 7, no 11 (2016). p. 3.

- Filtrar la información empresarial por parte de la competencia ya no es muy exigente.

- Los medios de almacenamiento y gestión de la información son sensibles a deterioros y daños.

- Un evento natural puede afectar de tal manera el negocio que no se puede estimar cuánto tarde la recuperación de las operaciones.

- Las debilidades de la empresa están expuestas en internet, las comunidades virtuales aumentan las críticas y afectan la sostenibilidad.

- Los sistemas de protección de la información crean consigo un apetito de vulnerabilidad en los ciberdelincuentes.

- La información relacionada con los estados financieros puede ser falsa.

El reto es grande, el uso de los sistemas de información interconectados sigue creciendo para soportar actividades y procesos importantes de negocio; adoptar medidas que conlleven a la protección de la información debe ser un tema para incorporar en la planeación estratégica de las empresas, así como en la vida cotidiana de las personas. Hay una necesidad amplia de sensibilización y educación de las personas en temas de seguridad de la información; los sistemas de información siempre han sido desarrollados por personas y para interpretación de personas. Las amenazas y los delitos informáticos evolucionan a la par con los avances tecnológicos, el principal objetivo de los atacantes se ha volcado a los sistemas de información.[4]

En la actualidad la gran mayoría de las empresas no cuentan con políticas para el aseguramiento de la información, adicional a esto no poseen herramientas o procedimientos para dimensionar el crecimiento acelerado que se pueda presentar en los almacenes de datos y determinar cuán sensible se hace cada día; la empresa Don Pollo SAS Armenia no es ajena a esta realidad ya que dentro de sus planeaciones estratégicas de crecimiento tecnológico y comercial no se ha contemplado la incorporación de un método que permita establecer directrices, documentar y evaluar para mantener la continuidad del negocio desde los sistemas de información en caso de verse afectada por un incidente de seguridad de la información.[5]

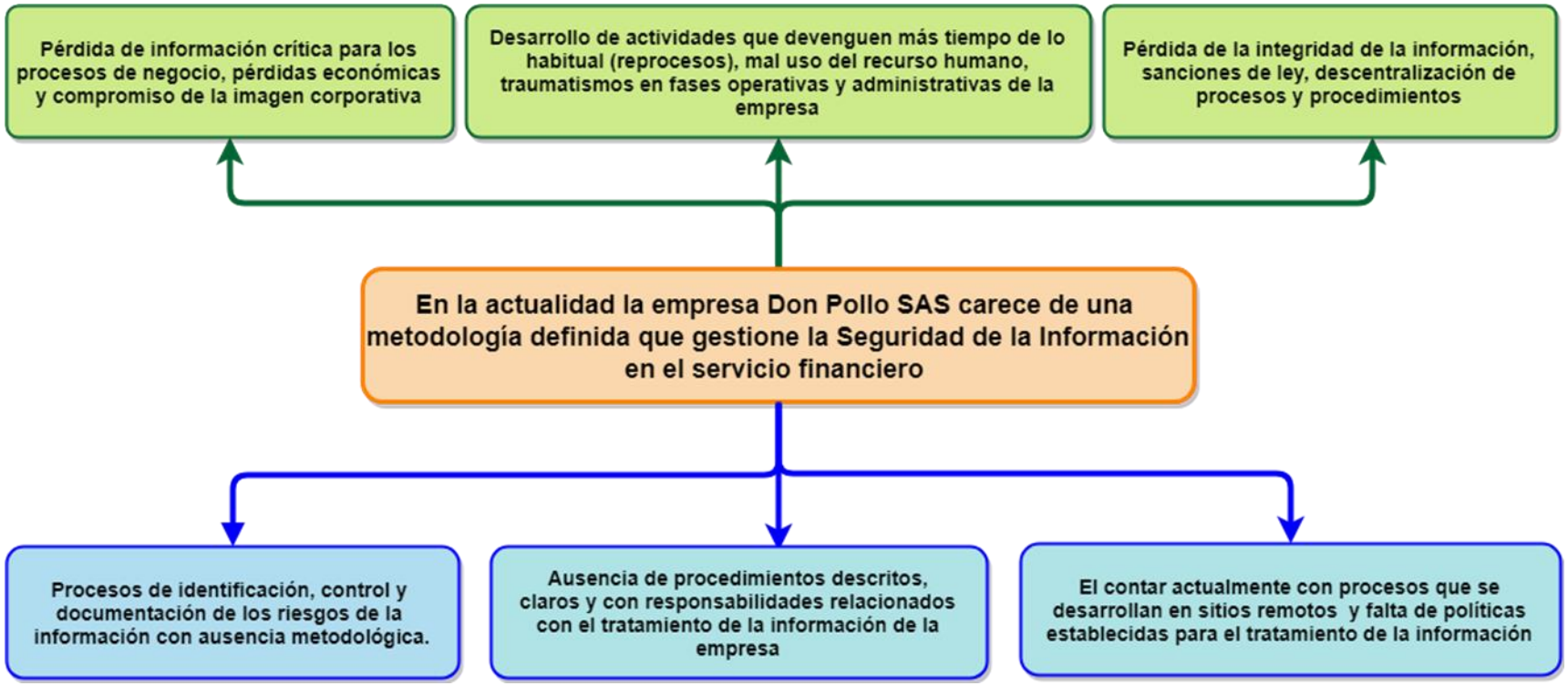
[4] GÓMEZ BARROSO, José Luis. Uso y valor de la información personal: un escenario en evolución. El Profesional de la Información vol 27, no 1 (12 de febrero de 2018). p. 2-4.
[5] JIMENEZ, Martín Antonio; ELOY, Vicente y ALFONSO, Mateos. Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, no 15 (junio de 2015). p. 4.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cuál es el Sistema de Gestión de Seguridad de la Información (SGSI) en el servicio de información financiero de la empresa Don Pollo SAS Armenia aplicando la Norma NTC-ISO-IEC 27001:2013?

1.2 ÁRBOL DEL PROBLEMA

Ilustración 1. Árbol del problema



Fuente: Autores

1.3 SISTEMATIZACIÓN DEL PROBLEMA

¿Cuál es el efecto de un incidente de seguridad de la información en el servicio financiero de la empresa?

¿Por qué adoptar buenas prácticas que vayan enfocadas en el tratamiento de la información del servicio financiero de la empresa?

¿Cuál es la ventaja de realizar la gestión del proceso financiero bajo unas políticas de seguridad de la información claras y definidas?

2. DELIMITACIÓN

Se ha determinado el alcance del proyecto SGSI a los procesos Dirección Financiera y Administrativa (DIRFIN) y Dirección de Tecnología de la Información y Comunicación (DIRTIC) de la empresa Don Pollo SAS en Armenia - Quindío. Se tendrán en cuenta los activos de información involucrados en la prestación del servicio de información financiero para estos procesos, con la orientación de la Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información MAGERIT 3.0. La información gestionada de las operaciones empresariales, corresponde a la vigencia del año 2019 y los resultados obtenidos son puestos a disposición de la empresa para que sea esta quien tome decisiones a partir de la entrega.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Documentar un Sistema de Gestión de Seguridad de la Información (SGSI) para el servicio de información financiero de la empresa Don Pollo SAS Armenia basados en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013 durante el año vigente 2019.

3.2 OBJETIVOS ESPECÍFICOS

- Definir una metodología de análisis y gestión de riesgos de la información.
- Documentar la estructura de procedimientos para la gestión de la seguridad de la información en el servicio financiero.
- Definir las políticas de seguridad para el tratamiento de la información en el servicio financiero.

4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Las empresas sean públicas o privadas día tras día están tomando mayor conciencia de la importancia de clasificar, valorar y salvaguardar todos sus activos de información, por la dinámica del negocio esta debe ser accedida en diferentes lugares y por diferentes personas lo cual genera un riesgo, por tal razón se deben proponer estrategias, procedimientos, controles, y protocolos concretos para disminuir la ocurrencia de amenazas que aprovechan las debilidades de las empresas, los riesgos se logran materializar ya que algunas empresas no cuentan con procesos que permitan dar tratamiento a las amenazas y riesgos, por tal razón se hace importante diseñar un SGSI que permita contar con directrices precisas, que permitan a las áreas de TIC (Tecnologías de la Información y la Comunicación) aplicar buenas prácticas de la seguridad de la información como la implementación de medidas que propendan por salvaguardar la integridad, la confidencialidad y la disponibilidad de la información, con el fin de asegurar la continuidad y la correcta operación de todos los procesos.[6]

Un Sistema de Gestión de Seguridad de la Información basado en la norma ISO-IEC 27001:2013, proveerá las condiciones necesarias para que la seguridad de la información apoye y agilice los objetivos estratégicos de la empresa, apoyando la debida gestión administrativa y operativa, adicionalmente generar sentido de pertenencia y apropiación sobre los temas de seguridad en los funcionarios de la empresa, logrando con ello la participación activa en las políticas, controles y medidas orientadas a salvaguardar la información, se conseguirá considerablemente minimizar el riesgo de que las funciones administrativas y operativas se vean afectadas mediante la ocurrencia de un suceso o evento que comprometa la información. Se hace necesario adoptar una metodología de análisis y gestión del riesgo de la información que permita establecer indicadores a través de una valoración objetiva sobre las vulnerabilidades que afectan el proceso de negocio.[7]

Para la Empresa Don Pollo SAS Armenia es importante contar con el diseño documental de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO-IEC 27001:2013 propuesto en este trabajo de investigación, el cual proveerá un marco de referencia para mantener la confidencialidad, integridad y disponibilidad de la información. La adopción de esta norma permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de la información de la empresa y que el tema de seguridad pase a ser de unas prácticas

[6] MUÑOZ, Mirna y RIVAS, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, no SPE3 (marzo de 2015). p. 13.

[7] ANGARITA, A. A.; TABARES, C.A. y RIOS, J.I. Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento. Entre Ciencia e Ingeniería vol 9, no 17 (junio de 2015). p. 2.

informales a un ciclo de vida metódico y controlado donde todos los integrantes de la empresa son partícipes y responsables.[8]

El método propuesto reconoce la importancia de las personas para la operación de los sistemas de información; empezar a concienciar las personas en temas de seguridad de la información es el punto de partida para que se vuelvan partícipes activos en todos los niveles de la empresa, identificando las barreras tecnológicas y desconocimientos que conllevan a cometer errores comunes, pero que se pueden ver representados en grandes pérdidas para la empresa, es el deber de la alta dirección hacer que sus colaboradores permeen cada uno de los procesos y actividades que se desarrollan a diario con el fin de que la seguridad de la información se convierta en una cultura y trascienda para el mejoramiento continuo y la permanencia competitiva en el mercado, generando confianza desde el interior de la empresa hacia sus clientes.

[8] GÓMEZ BARROSO, José Luis. Uso y valor de la información personal: un escenario en evolución. El Profesional de la Información vol 27, no 1 (12 de febrero de 2018). p. 2-4.

5. MARCOS

5.1 MARCO TEÓRICO, CONCEPTUAL O REFERENCIAL

5.1.1 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es parte vital de toda organización, constituyéndose en su principal garantía de confiabilidad, esta deberá protegerse de forma física y lógica. Físicamente con una sólida infraestructura tecnológica; y lógicamente por un sistema informático que debe asegurar su inviolabilidad, todo esto manejado a través de políticas establecidas.[9]

La seguridad de la información se caracteriza por la preservación de:

- Su confidencialidad, asegurando que solo quienes estén autorizados pueden acceder a la información.

- Su integridad, asegurando que la información y su manera de procesarla sean exactos y completos.

- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.[10]

Algunas ventajas de adoptar el uso de buenas prácticas en seguridad de la información son:

- Identificar, controlar y documentar los riesgos de la información con todas las consecuencias que pueda traer la materialización de una amenaza informática.

- Estructurar los procedimientos claros y con responsabilidades con respecto al tratamiento de la información de la empresa.

- Definir controles y objetivos de control de la seguridad de la información para otras unidades de negocio que se encuentran descentralizadas.

---

[9] CONTADURÍA GENERAL DE LA NACIÓN. Manual y Políticas del Sistema Integrado de Gestión Institucional - Contaduría General de la Nación. [Consultado: 11 de abril de 2019]. Disponible en internet: http://www.contaduria.gov.co/wps/portal/internetes/home/internet/contaduria/sistema-integrado-de-gestion/politica-sistema-integrado-gestion. p. 21.

[10] ICONTEC. ICONTEC e-Collection. [Consultado: 03 de abril de 2019]. Disponible en internet: https://ugc.elogim.com:2741/normavw.aspx?ID=74790.

- Realizar un inventario de activos de la información con cada una de sus dependencias y vulnerabilidades a los que se encuentran expuestos.

- Dimensionar en cifras o valores lo que pudiera representar para la empresa una pérdida o vulneración de la información.

5.1.2 SISTEMA DE GESTIÓN

Conjunto de componentes interconectados para lograr un objetivo determinado y entre los elementos que lo conforman se incluyen: la estructura, las políticas y prácticas organizativas, las personas, los recursos materiales y financieros y los procesos.[11]

5.1.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI), es una metodología que persigue la protección de los activos críticos de las organizaciones, con el fin de asegurar la continuidad del negocio ante cualquier incidente de seguridad. Aún más, el SGSI es el pilar sobre el que se basa la norma internacional UNE-ISO/IEC 27001: 2013, que los certifica. Pero esta mejora que podría parecer que afecta solo a la seguridad, implica y conlleva beneficios como: reducción de riesgos, ahorro, calidad a la seguridad, reducción de costes, optimizar los recursos y las inversiones en tecnología, protección del negocio, mejora la competitividad y cumplimiento legal y reglamentario en los procesos de manejo de la información; esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El propósito de un Sistema de Gestión de la Seguridad de la Información no es garantizar la seguridad (que nunca podrá ser absoluta) sino garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

Actualmente el ISO-27001:2013 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

[11] MEIZOSO VALDES, María del Carmen y GUERRA BRETAÑA, Rosa Mayelin. La implantación de sistemas integrados de gestión. Un reto a la empresa cubana. The implementation of integrated management systems: A challenge to the Cuban organizations. 7, no 2 (julio de 2010). p. 2.

El estándar ISO 27001 permite:

- Diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos.

- A la dirección gestionar las políticas y los objetivos de seguridad en términos de integridad, confidencialidad y disponibilidad.

- Determinar y analizar los riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.

- Prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- Sistemas de Gestión de Seguridad de la Información, por sus siglas en inglés ISMS (Information Security Management System).

- Valoración de riegos (Risk Assesment).

- Controles.

La metodología de los sistemas de gestión se basa en el Ciclo de Deming, el cual al representarse gráficamente abstrae el concepto de mejora continua por la retroalimentación del paso final al paso inicial.[12]

5.1.4 CICLO DEMING O PHVA

La norma ISO 27001 adopta el ciclo PHVA como metodología, siendo transversal su aplicación en todos los procesos que abarca el SGSI. Esta metodología se conoce por sus siglas como Planear, Hacer, Verificar y Actuar. El ciclo PHVA fue diseñado por el Dr. Walter Shewhart en 1920 y presentada por William Edwards Deming a partir de 1950 como herramienta universal de mejora continua.

La Organización Internacional de Normalización (ISO) recomienda la aplicación del ciclo PHVA con el fin de ayudar a alcanzar los objetivos y conseguir los resultados esperados por la empresa.

[12] ISO. ISO - International Organization for Standardization. [Consultado: 03 de abril de 2019]. Disponible en internet: http://www.iso.org/cms/render/live/en/sites/isoorg/home.html.

La descripción de cada una de las etapas PHVA en la norma ISO 27001 es la siguiente:

- Planificar; Se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.

- Hacer; se implantan los procesos.

- Verificar; se revisan y se evalúan tanto los servicios como los procesos comparándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.

- Actuar; comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión de Seguridad de la información de forma continua.[13]

Ilustración 2. Modelo PHVA en un SGSI

Fuente: http://audicaribe.com/sgsi-1/

[13] VILLENA AGUIRRE, Moisés Antonio. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Pontificia Universidad Católica del Perú, 30 de octubre de 2014. p. 10.

5.1.5 INFORMACIÓN

La información es un activo importante para la misión de una organización, para algunas empresas se ha convertido en su activo más importante, por lo tanto, necesita ser protegido de manera adecuada. Puede estar almacenada en medios físicos, electromagnéticos, así como la no estructurada en forma de conocimiento de los empleados.[14]

Puede existir de muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación; cualquiera que sea la forma de la información, esta necesita ser gestionada y trasmitida por algún medio, el cual debe contar con medidas de protección adecuada.[15]

5.1.6 SEGURIDAD DE LA INFORMACIÓN FRENTE A SEGURIDAD INFORMÁTICA

La diferencia entre seguridad informática y seguridad de la información radica en el tipo de recursos sobre el cual actúa cada una. La seguridad informática se enfoca en la tecnología propiamente dicha, en las infraestructuras tecnológicas que sirven para la gestión de la información. La seguridad de la información está directamente relacionada con la información en sí misma, como activo estratégico de la empresa para la adecuada toma de decisiones.[16]

- Seguridad Informática; características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

- Seguridad de la Información; protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.[17]

---

[14] SANTOS LLANOS, Daniel Elías. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Pontificia Universidad Católica del Perú, 1 de febrero de 2017. p. 20.

[15] ALIAGA FLORES, Luis Carlos. Diseño de un sistema de gestión de seguridad de información para un instituto educativo. Pontificia Universidad Católica del Perú, 2 de septiembre de 2013. p. 21.

[16] VALENCIA DUQUE, Francisco Javier y OROZCO ALZATE, Mauricio. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informacao, 1 de junio de 2017. p. 3-4.

[17] CONTADURÍA GENERAL DE LA NACIÓN. Manual y Políticas del Sistema Integrado de Gestión Institucional - Contaduría General de la Nación. [Consultado: 11 de abril de 2019]. Disponible en internet: http://www.contaduria.gov.co/wps/portal/internetes/home/internet/contaduria/sistema-integrado-de-gestion/politica-sistema-integrado-gestion. p. 21.

5.1.7 ESTÁNDARES DE SEGURIDAD DE LA SERIE ISO 27000

La Organización Internacional de Estandarización (ISO) recoge un extenso número de normas dentro de la familia de ISO 27000. A continuación, se hace un breve resumen del contenido de las principales normas de la serie 27000 ya publicadas o en proceso de publicación final. Partiendo del fundamento de que el trabajo de investigación se desarrolla en base al estándar ISO/IEC 27001, el cual indica qué requisitos deben conformar un SGSI, pero no cómo cumplirlos, algunas de las normas que conforman la serie 27000 pueden servir en la orientación para documentar mejores prácticas en aspectos o incluso cláusulas concretas de la norma ISO/IEC 27001 de modo que se evite reinventar la rueda con el sustancial ahorro de tiempo en la implantación.[18]

Tabla 1. Normas de la familia ISO 27000

TÍTULO	DESCRIPCIÓN
ISO-IEC 27000	Proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.
ISO-IEC 27001	Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

[18] PORTAL ISO 27001 ESPAÑOL. ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. [Consultado: 03 de abril de 2019]. Disponible en internet: http://www.iso27000.es/iso27000.html.

TÍTULO	DESCRIPCIÓN
ISO-IEC 27002	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.
ISO-IEC 27003.	Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
ISO-IEC 27004	Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
ISO-IEC 27005	Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
ISO-IEC 27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSI. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.
ISO-IEC 27007	Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
ISO-IEC TR 27008	Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

TÍTULO	DESCRIPCIÓN
ISO-IEC 27009	Define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.
ISO-IEC 27010	Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.
ISO-IEC 27011	Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.
ISO-IEC 27013	Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
ISO-IEC 27014	Consiste en una guía de gobierno corporativo de la seguridad de la información.
ISO-IEC TR 27015	Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005. Desde 24 de Julio, de 2017 se anuncia que no será actualizada en relación a las novedades de la norma ISO/IEC 27002:2013 aunque sigue disponible para su adquisición por parte de los interesados.
ISO-IEC TR 27016	Es una guía de valoración de los aspectos financieros de la seguridad de la información
ISO-IEC 27017	Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
ISO-IEC 27018	Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

TÍTULO	DESCRIPCIÓN
ISO-IEC TR 27019	Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Actualizada como ISO/IEC 27019:2017 en Octubre de 2017 para su alineación con ISO/IEC 27002:2013, además de la aplicación a los sistemas de control de procesos (p.ej. PLCs) utilizados por la industria de la energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor y para el control de los procesos de soporte asociados, también incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en ISO/IEC 27001:2013 a la orientación específica del sector de servicios de energía.
ISO-IEC 27021	En desarrollo; desarrolla los requisitos de las competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información.
ISO-IEC 27023	Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.
ISO-IEC 27031	Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.
ISO-IEC 27032	Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

TÍTULO	DESCRIPCIÓN
ISO-IEC 27033	Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 6 partes: 27033-1, conceptos generales (Publicada el 15 de Diciembre de 2009 y revisada el 10 de Octubre de 2015); 27033-2, directrices de diseño e implementación de seguridad en redes (Publicada el 27 de Julio de 2012); 27033-3, escenarios de referencia de redes (Publicada el 3 de Diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (Publicada el 21 de Febrero de 2014); 27033-5, aseguramiento de comunicaciones mediante VPNs (Publicada el 29 de Julio de 2013); 27033-6, securización de redes IP wireless (Publicada en Junio de 2016).
ISO-IEC 27034	Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 7 partes: 27034-1, conceptos generales (Publicada el 21 de Noviembre de 2011); 27034-2, marco normativo de la organización (Publicada el 15 de Agosto de 2015); 27034-3, proceso de gestión de seguridad en aplicaciones (publicada en Mayo 2018); 27034-4, validación de la seguridad en aplicaciones (en fase de desarrollo); 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (Publicada el 09 de Octubre de 2017); 27034-6, guía de seguridad para aplicaciones de uso específico (Publicada en Octubre de 2016); 27034-7, marco predictivo de en la seguridad (publicada en Mayo 2018).
ISO-IEC 27035	Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes: 27035-1, Principios en la gestión de incidentes (Publicada en noviembre de 2016); 27035-2, guías para la elaboración de un plan de respuesta a incidentes (Publicada en noviembre de 2016); 27035-3, guía de operaciones en la respuesta a incidentes.
ISO-IEC 27036	Guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos (Publicada el 24 de marzo de 2014); 27036-2, requisitos comunes (Publicada el 27 de febrero de 2014); 27036-3, seguridad en la cadena de suministro TIC (Publicada el 08 de noviembre de 2013); 27036-4, guía de seguridad para entornos de servicios Cloud (Publicada en octubre de 2016).

TÍTULO	DESCRIPCIÓN
ISO-IEC 27037	Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.
ISO-IEC 27038	Es una guía de especificación para seguridad en la redacción digital.
ISO-IEC 27039	Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
ISO-IEC 27040	Es una guía para la seguridad en medios de almacenamiento.
ISO-IEC 27041	Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
ISO-IEC 27042	Es una guía con directrices para el análisis e interpretación de las evidencias digitales.
ISO-IEC 27043	Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales
ISO-IEC 27050	Norma desarrollada en tres partes sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis y producción: 27050-1, conceptos generales (Publicada en noviembre de 2016); 27050-2, Guía para el gobierno y gestión (En desarrollo); 27050-3, código de buenas prácticas (En desarrollo).
ISO-IEC TR 27103:2018	Norma desarrollada Primera edición para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.
ISO-IEC 27799	Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Fuente: http://www.iso27000.es/iso27000.html

5.1.8 GESTIÓN DE RIESGOS

Comprende la identificación de problemas potenciales antes de que éstos ocurran, tal que se pueden planificar actividades para gestionar los riesgos, las cuales pueden ser invocadas a través de todo el ciclo de desarrollo de un producto o proyecto, tal que puedan ser mitigados los impactos adversos que impidan el logro de los objetivos. El objetivo es trazar un marco de acción para saber qué aspectos gestionar y cómo hacerlo. La gestión tiene que ver, sobre todo, con la cuantificación de los riesgos, para lo cual es fundamental definir dos elementos dentro de este proceso:[19]

- Consecuencia o impacto; la norma define la consecuencia como los efectos o aquellos elementos que se derivan directa o indirectamente de otros. En este caso, se trata de evaluar los riesgos que cumplen con la premisa de causa-efecto. Es cierto que no siempre se pueden prever las consecuencias de una acción o decisión, pero este solo acto es el origen de cualquier Sistema de Gestión de Riesgos. Sin un mínimo grado de consecuencia, cualquier acción en la materia resultará insuficiente.[20]

- Probabilidad; este segundo término habla de la posibilidad de que un hecho se produzca. Para la Gestión de Riesgos, es fundamental que las empresas contemplen la irrupción de hechos que puedan derivarse o no de las decisiones de la empresa. Nunca se está del todo preparado para los acontecimientos, sobre todo si éstos provienen de factores externos, pero el sólo hecho de pensar en su materialización ya es un buen indicador de la Gestión de Riesgos.[21]

5.1.9 MAGERIT 3.0 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes

[19] DIAZ, Oswaldo y MUÑOZ, Mirna. Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización mexicana. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, no 26 (marzo de 2018). p. 3.
[20] ISO TOOLS. ISO 31000 Software ISO. [Consultado: 03 de abril de 2019]. Disponible en internet: https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000.
[21] Ibid.

para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[22]

5.1.10 NORMA TÉCNICA COLOMBIANA NTC 31000:2018 GESTIÓN DEL RIESGO. DIRECTRICES

Esta norma proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto. Su adopción facilita la gestión de cualquier tipo de riesgo y no es específico de una industria o un sector. Como marco de referencia puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.[23]

5.1.11 REGULACIÓN PARA EL CRECIMIENTO EXPONENCIAL DEL CONTENIDO DIGITAL

Con el aumento de la dependencia de la tecnología para desarrollar las actividades de la empresa, crece de manera incontrolable el almacenamiento de contenidos digitales, representados en bits. Se aumenta la necesidad de garantizar su integridad, confidencialidad y disponibilidad. Se estima que alrededor del 70% de la información generada y almacenada deja de consultarse a partir de los 90 días, la legislación de cada país obliga a guardarlos por un periodo de tiempo superior, dependiendo del carácter de los mismos, los sistemas de backup cada día se hacen más complejos y sensibles por su aumento en el volumen de los datos. Para orientar en buenas prácticas la digitalización de archivos, se dispone de la Norma ISO/TR 13028 Información y documentación - Pautas de implementación para la digitalización de registros, establece pautas para crear y mantener registros solo en

[22] GOBIERNO DE ESPAÑA. PAe - Portal de Administración Electrónica. [Consultado: 06 de abril de 2019]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home.html#.
[23] ICONTEC. ICONTEC e-Collection. [Consultado: 11 de abril de 2019]. Disponible en internet: https://ugc.elogim.com:2741/normavw.aspx?ID=74790.

formato digital, donde el papel original u otro registro de fuente no digital se ha copiado mediante digitalización.[24]

5.1.12 SOFTWARE QUE AUTOMATIZA LA OPERACIÓN DE UN SGSI

Se han identificado las siguientes herramientas de software que automatizan la implementación y operación de un SGSI:

- ISO TOOL

Es una herramienta web producida por ISO TOOLS Perú, que automatiza el cumplimiento de algunos requisitos del estándar 27001. Incorpora elementos de otros estándares como la ISO 9001 o de modelos BPM, los cuales no son necesariamente obligaciones del estándar de seguridad de información. No está estrictamente enfocado en el cumplimiento del estándar 27001.

- E-GAM

Este software, producido por EGAMBPM, es un workflow de BPM genérico, adaptable a distintos estándares ISO; al igual que en el caso anterior, presenta una solución compleja, con una estructura más útil para organizaciones que cuentan con un sistema integrado de gestión.

- INMUNO SUITE

Este sistema web, producido por M&T, cuenta con un módulo de gestión de riesgos complejo y un módulo de operación del SGSI, el cual ha sido modelado específicamente para el cumplimiento del estándar 27001, ya que guarda correlación con todos los requisitos, aunque no los llega a automatizar completamente.

- E-PULPO

Es un sistema de escritorio producido por INGENIA, implementado con un enfoque de cumplimiento del estándar 27001 y que se integra al software EAR/PILAR del gobierno español, el cual usa para atender los requisitos de gestión de riesgos.

[24] GIRALT, Olga; VIDAL PIJOAN, Carmen y PÉREZ SOLER, Carlos. Seguridad de Los Documentos de Archivo: Estudio de Caso Del Archivo Del Ayuntamiento de Barcelona. Journal article (Paginated). El profesional de la información, marzo de 2011. p. 2.

- EAR PILAR

Es una herramienta de gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) de España, que implementa la metodología MAGERIT de análisis y gestión de riesgos, cuenta con licencias libres para organismos de la administración pública española.[25]

- CONFORMIO

Es una solución de software en línea lista para su utilización que proporciona a su pequeña o mediana empresa pasos claros para implementar proyectos de cumplimiento y privacidad, y le ayuda a mantener sus documentos y procesos de cumplimiento en un solo lugar.[26]

- KAWAK

Software para ISO 27001 – Los insumos que se necesitan para tomar las medidas preventivas y reactivas sobre la confidencialidad, disponibilidad e integridad de la información. Entre sus principales características se encuentran la gestión de los riesgos y activos de información, dinamiza la declaración de aplicabilidad y gestiona los incidentes de seguridad de la información y los procesos críticos para la continuidad del negocio.[27]

[25] SANTOS LLANOS, Daniel Elías. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Pontificia Universidad Católica del Perú, 1 de febrero de 2017. p. 20.
[26] CONFORMIO. Software de cumplimiento con el RGPD e ISO 27001 para pequeñas empresas. [Consultado: 11 de abril de 2019]. Disponible en internet: https://advisera.com/conformio/es/.
[27] KAWAK. Software en la nube para sistemas de gestión ISO. [Consultado: 11 de abril de 2019]. Disponible en internet: https://kawak.net/.

5.2 MARCO INSTITUCIONAL

5.2.1 RESEÑA HISTÓRICA, BUSCANDO ABEJAS NACIÓ DON POLLO

Palabras del fundador Luis Felipe Uribe Henao:

"El tema del pollo surgió porqué yo estaba buscando qué hacer, qué actividad realizar, viendo posibilidades, y me acerqué al Comité de cafeteros en esa época, ya que financiaba proyectos agropecuarios, de pollo, de peces, de apicultura y a mí la verdad me llamaba la atención la apicultura, las abejas. Les dije que estaba interesado en montar un apiario y que necesitaba ser partícipe de esa línea que ellos patrocinaban para que la gente montara su negocio en las fincas. Me recibieron y dijeron que lo primero que tenía que hacer era ir a ver las abejas, que me dejara picar para saber si era lo que yo quería para mi negocio o no.

Los acompañé entonces a hacer unas visitas, estuve todo el día con ellos y durante los recorridos fuimos aun apiario en donde además tenían pollos. En ese momento me llamaron mucho la atención los pollos porque recordé que mi papá tenía esos galpones, comederos, bebederos, y yo vi eso como una oportunidad. Ya había terreno abonado y llevábamos esa parte agrícola en la sangre porque nacimos en ese ambiente y en cierta forma uno se familiariza con el ámbito avícola. Entonces dese ahí yo no llegué a la casa con el proyecto de las abejas sino de los pollos. Le conté a mi mamá y ella esa noche le dijo a mi papá. Ella le siguió insistiendo, entonces al otro día al desayuno ese fue el tema de conversación. Mi mamá le decía a mi papá que me ayudara, que abriera un crédito donde a él le fiaban el concentrado para las gallinas, y solo me prestara la plata para los pollos. Mi papá siempre reacio, pero a lo último ante tanta insistencia, mi mamá lo convenció. Ella fue siempre mi apoyo y motivación, hablaba con mi papá para tratar de facilitar todos temas."

5.2.2 EMPRESA DON POLLO SAS

La Empresa Don Pollo SAS está presente en los procesos de incubación, nacimiento, levante, alimentación, sacrificio y comercialización del pollo, desde la fabricación del alimento que se produce exclusivamente para el consumo de la propia empresa en una planta de alimentos concentrados que produce y abastece a las diferentes granjas de la empresa con un alimento de calidad que cumple todas las características y parámetros necesarios para el sano crecimiento de las aves, este se consume tanto en las granjas de reproductoras como en las granjas de levante. La fase de reproducción e incubación es llevada a cabo por la empresa y cuenta con todos los estándares de calidad para entregar a Don Pollo SAS un pollo

sano que cumpla todas las exigencias físicas y de inocuidad necesarias para su óptimo desarrollo y crecimiento.

Como se especifica anteriormente, Don Pollo SAS es una empresa con presencia en todos los sectores de la economía y con gran experiencia en la industria avícola, llegando a diferentes segmentos del mercado con productos de óptima calidad.

Creada en 1988, esta empresa con aproximadamente 30 años en el mercado colombiano se encarga del engorde, el levante, el beneficio y la comercialización de sus propias aves, además de ofrecer servicio de maquila a otras empresas de orden nacional.

La planta de beneficio cuenta con tecnología de punta Stork Marel única en Colombia y tiene la capacidad de procesar 12.500 aves por hora con una capacidad total de 43.000.000 aves/año. Cuenta con presencia permanente (24 horas) por parte de INVIMA (Instituto Nacional de Vigilancia de Medicamentos y Alimentos) con el fin de garantizar los más altos estándares de calidad en el mercado nacional.

La principal actividad es comercializar proteína cárnica de alta calidad teniendo presencia en Antioquia, Valle, Tolima Grande, Bogotá y Eje Cafetero con más de treinta puntos de venta y centros de abastecimiento en Colombia, esta empresa se enfoca únicamente en el mercado nacional.

La empresa Don Pollo SAS tiene su sede principal en la ciudad de Armenia Quindío ubicada en la calle 21 # 16-40 edificio torre Colseguros (sede administrativa), así como también cuenta con sus plantas propias de incubación, alimentos y beneficio, donde adicionalmente cuenta con 38 granjas propias para el levante de pollo y garantizando 1139 empleos fijos a nivel nacional entre personal operativo y administrativo.

5.2.3 VALORES INSTITUCIONALES

Los valores invitan pensar y actuar de tal forma aportar al crecimiento propio y de la empresa Don Pollo SAS:

- Gente C4: Confiable, Comprometida, Competente y en Crecimiento permanente.
- Integridad: Coherencia entre lo que yo soy y lo que yo hago.
- Respeto: amor por los demás.
- Responsabilidad: Administrar con respeto nuestros actos.

- Calidez humana: Ser cordial y afectuoso con los demás.
- Equidad: Justo equilibrio en todos los campos de nuestra actuación.

5.2.4 IMAGEN INSTITUCIONAL

Ilustración 3. Logo empresarial

Fuente: Registro fotográfico empresa Don Pollo SAS

5.2.5 SITIO WEB

La empresa tiene actualmente visibilidad en la web a través de la siguiente dirección URL: https://www.grupodonpollo.com.co/sitio/.

5.2.6 MISIÓN

En la Empresa Don Pollo SAS tomamos de la naturaleza lo mejor, generando experiencias superiores para enriquecer la vida de nuestros clientes y colaboradores a través de un proceso integrado y controlado.

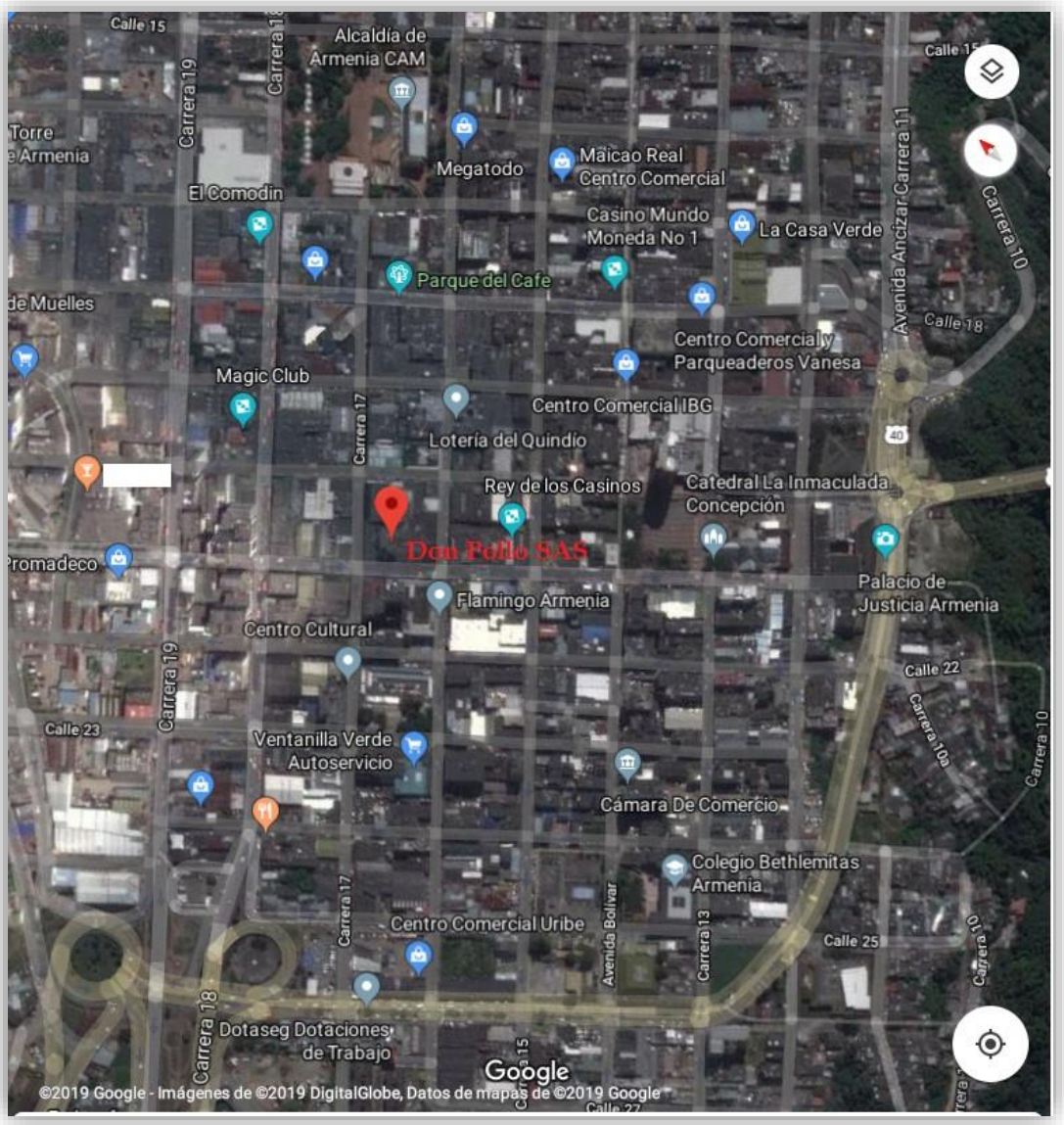
5.2.7 VISIÓN

Seremos la empresa que fundamenta su excelencia en prácticas líderes, enfocado en nuestra Meta Grande y Ambiciosa (MEGA) para 2023.

5.3 MARCO ESPACIAL

El ámbito donde se realiza el estudio de investigación es en la Empresa Don Pollo SAS, en su sede administrativa ubicada en la calle 21 N° 16-40 edificio torre Colseguros, Armenia Quindío. Sitio web http://www.grupodonpollo.com.co/sitio/ El alcance del proyecto dentro de la Empresa es el servicio de información financiera.

Ilustración 4. Ubicación geográfica de las oficinas administrativas, Armenia Quindío



Fuente: Google Maps 2019

Ilustración 5. Sede administrativa, Armenia Quindío

Fuente: Google Maps 2019

5.4 MARCO TEMPORAL

El trabajo de investigación se desarrolla con vigencia del año 2019; durante el segundo semestre se consolidan y entregan los resultados a todas las partes interesadas pertinentes.

5.5 MARCO NORMATIVO

Tabla 2. Normograma para el proyecto

JERARQUÍA	NÚMERO / FECHA	DESCRIPCIÓN
INTERNOS		
REGLAMENTO	Interno de trabajo	Reglamento interno para Don Pollo SAS.
MANUAL	Interno de políticas y procedimientos relativos al tratamiento de datos personales del Grupo Empresarial Don Pollo	Determina el funcionamiento del programa de protección de datos personales al interior de la empresa, dando cumplimiento al régimen normativo de la protección de datos personales y las instrucciones impartidas por la Superintendencia de Industria y Comercio.
POLÍTICA	Tratamiento de datos personales, diciembre 26 de 2017	Política de tratamiento de datos personales del Grupo Don Pollo.
EXTERNOS		
NORMA	NTC-ISO/IEC 27001:2013	Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información. Requisitos
NORMA	NTC-ISO/IEC 27005:2009	Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
NORMA	NTC-ISO/IEC 31000:2018	Gestión del riesgo. Directrices.
GUÍA TÉCNICA	GTC-ISO/IEC 27002:2015	Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información
LEY	1712 de 6 de marzo de 2014	Por medio de la cual se crea la ley de trasparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones
LEY	1581 del 17 de octubre de 2012	Por el cual se dictan disposiciones generales para la protección de datos personales.
LEY	1273 del 05 de enero de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
LEY	594 , julio 14 de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
CONSTITUCIÓN	95/1991	Constitución Política de Colombia 1991.
METODOLOGÍA	MAGERIT 3.0, Octubre de 2012	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
POLÍTICA	Política Nacional de Seguridad Digital (documento CONPES 3854 de 2016)	Política Nacional de Seguridad Digital.
MARCO	Marco Regulatorio del Comercio Electrónico, mayo 24 de 2018	Marco constitucional y legal del comercio electrónico, así como las obligaciones que deben cumplir las tiendas online para evitar errores que puedan vulnerar los derechos de los consumidores.

Fuente: Autores

6. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

La metodología para desarrollar el presente proyecto, se encuentra descrita dentro de la Norma NTC-ISO 27001:2013, la cual es de aplicación universal en cualquier tipo de organización. Las herramientas planteadas para abordar la documentación dentro de la Empresa Don Pollo SAS son de fácil aplicación y con base en herramientas informáticas de uso común.

Cada una de las etapas para la documentación del SGSI, vienen descritas en la estructura de alto nivel de la norma y se fundamenta en el ciclo PHVA.

La documentación de un Sistema de Gestión de Seguridad de Información se estructura de la manera más adecuada y determinando un alcance dentro de la empresa. El modelo utilizado se basa en una investigación descriptiva la cual consiste en llegar a conocer las situaciones actuales y predominantes a través de la descripción exacta de las actividades, procesos y personas que intervienen en el proceso financiero de la Empresa Don Pollo SAS Armenia. Los activos de información del proceso definen el alcance para el presente proyecto.

Las etapas representativas del estudio son:

- El análisis y evaluación del riesgo que se tomen alrededor de los activos de información identificados.

- La identificación de amenazas que indiquen un evento potencial no deseado.

- La identificación de vulnerabilidades que puedan hacer que una amenaza afecte un activo.

- La identificación de procesos que se caractericen críticos en el manejo de la información y la normatividad aplicable.[28]

Los resultados del trabajo de investigación permiten determinar la situación actual en materia de seguridad de la información sobre el alcance definido y sirven como referencia para el desempeño de la organización y su perfeccionamiento en el tiempo.

[28] MEDINA HERNÁNDEZ, Diana Carolina. Diseño del sistema de gestión de seguridad de la información en Angelcom S.A. reponame: Repositorio Institucional Universidad Libre, 22 de noviembre de 2017. p. 31.

6.1 TIPO DE INVESTIGACIÓN

Se realiza una investigación aplicada, descriptiva y documental. Al momento de iniciar con este proyecto en la empresa Don Pollo SAS Armenia no se poseen datos de referencia relacionados con la seguridad de la información.

6.2 RECOLECCIÓN DE LA INFORMACIÓN

La información es recolectada con el apoyo de los instrumentos mencionados más adelante en el numeral 11.7.

Con la información recolectada se establece un diagnóstico inicial de cumplimiento frente a la Norma NTC-ISO-IEC 27001:2013 y a partir de esto se realiza un esquema documental para utilizarlo como marco de referencia en el servicio financiero de la empresa.

Fuentes de información primarias:

- Personas involucradas en el tratamiento de la información financiera.

Fuentes de información secundarias:

- Artículos científicos de bases de datos indexadas en internet.
- Normatividad publicada por ICONTEC.
- Documentos bibliográficos en las bibliotecas institucionales.
- Tesis almacenadas en bases de datos institucionales y relacionadas con el tema de investigación.

Las técnicas utilizadas para recolectar la información son:

- Entrevistas con personal de la empresa.
- Encuestas dirigidas al personal pertinente con el fin de establecer algunos estados y valores de activos de la información, así como el diagnóstico inicial de cumplimiento de la norma.
- Observación de las áreas involucradas en el alcance del proyecto con el fin de poder analizar vulnerabilidades y factores de riesgo.

6.3 POBLACIÓN

- El personal administrativo y operativo de la empresa Don Pollo SAS Armenia que interviene en el tratamiento de la información del servicio financiero.

- Las bases de datos que soportan el servicio de información financiera.

6.4 ESQUEMA TEMÁTICO

A continuación, se describen las categorías principales del proyecto de investigación:

Tabla 3. Esquema temático

ETAPAS	PASOS	DOCUMENTO / HERRAMIENTA DE APOYO PRINCIPAL
Recolección de la información	Estado del arte	Bases de datos indexadas. Repositorios digitales.
	Definición del Problema	Árbol del problema
	Justificación	
	Objetivos	
	Marco teórico	Bases de datos indexadas. Repositorios digitales. Sitios web oficiales.
	Referencias normativas	FAMILIA ISO 27000
	Referencias metodológicas	MAGERIT 3.0
Trabajo de campo	Definición del alcance	Descripción del proceso financiero
	Diagnóstico inicial de ISO 27001	Nivel de cumplimiento ISO 27001
	Modelo de política de seguridad de la información	Norma NTC-ISO 27001:2013
	Inventario de activos de información	MAGERIT 3.0
	Valoración de activos	MAGERIT 3.0
Análisis	Análisis y evaluación del riesgo de los activos de información.	MAGERIT 3.0
	Selección de controles de seguridad	Anexo A

ETAPAS	PASOS	DOCUMENTO / HERRAMIENTA DE APOYO PRINCIPAL
	Modelo de declaración de aplicabilidad	Norma NTC-ISO 27001:2013
	Conclusiones	
	Recomendaciones	
Difusión	Entrega de resultados	Acta de entrega a la dirección
	Socialización	Permiso de la dirección

Fuente: autores

6.5 UNIDAD DE ANÁLISIS

Al tratarse de un trabajo fundamentado en la seguridad de la información, la unidad de análisis está determinada en los datos y una de sus principales características es que es intangible. Para este ejercicio la unidad de análisis es el dato.

6.6 VARIABLES

Tabla 4. Variables del proyecto de investigación

OBJETIVOS	VARIABLES	DEFINICIÓN
Definir una metodología de análisis y gestión de riesgos de la información.	MAGERIT 3.0	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
	ISO-IEC 27005	Gestión de Riesgos de la Seguridad de la Información.
	ISO 31000:2018	Gestión del riesgo. Principios y Directrices.
Documentar la estructura de procedimientos para la gestión de la seguridad de la información empresarial.	NTC-ISO-IEC 27001:2013	Sistemas de Gestión de Seguridad de la Información. Requisitos.
Definir las políticas de tratamiento de la información financiera.	NTC-ISO-IEC 27001:2013	Sistemas de Gestión de Seguridad de la Información. Requisitos.

Fuente: autores

6.7 CRITERIOS DE VALIDEZ DEL INSTRUMENTO DE LA INVESTIGACIÓN

Se implementa un instrumento que permite realizar el diagnóstico inicial de cumplimiento frente a la Norma Técnica Colombiana NTC-ISO-IEC-27001:2013. Este diagnóstico será ejecutado dentro del alcance del proyecto, el cual es el servicio de información financiero de la empresa.

El instrumento contiene las instrucciones para su diligenciamiento y será dirigido a las personas que intervienen en el tratamiento de la información financiera de la empresa.

Para el análisis y gestión del riesgo se utilizarán las plantillas suministradas en la Metodología MAGERIT 3.0 y así poder llegar al diseño de un panorama de riesgos informáticos. La valoración de activos, del riesgo y sus impactos se basa en una tabulación escalar, siendo de menor valor e impacto de acuerdo a un orden ascendente numérico.

Ilustración 6. Fragmento del instrumento para el diagnóstico inicial en NTC-ISO-IEC 27001:2013

Fecha de diligenciamiento: DD/MM/AAAA											
Nombre de la empresa: Don Pollo SAS Armenia											
Alcance: Servicio de información financiero											
ITEM	**NUMERAL-LITERAL ISO 27001**	**REQUISITO**	**NA**	**NO**	**SI**				**TOTAL**	**OBSERVACIONES**
					IDEA	**DOCUMENTADO**	**IMPLEMENTADO**	**REGISTROS DE IMPLEMENTACIÓN**		
4. CONTEXTO DE LA ORGANIZACIÓN										
	4.1	**CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO**	**0**	**0**	**1**	**0**	**0**	**0**	**25%**	
1	Gr	¿Tiene determinado las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos del SGSI?			1					Aquí se colocan las observaciones de lo que posee la empresa o el proceso
	4.2	**COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS**	**0**	**0**	**0**	**2**	**0**	**0**	**50%**	
2	a	¿Tiene determinada las partes interesadas que son pertinentes al SGSI?				1				
3	b	¿Tiene determinado los requisitos de las partes interesadas pertinentes a seguridad de la información?				1				
	4.3	**DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**	**0**	**0**	**1**	**0**	**1**	**3**	**80%**	
4	Gr	¿La organización tiene determinados los límites y la aplicabilidad (exclusiones) del SGSI para identificar su ámbito de aplicación?					1			Aquí se colocan las observaciones de lo que posee la empresa o el proceso
5	a	¿Considera las cuestiones externas e internas referidas en el numeral 4.1?			1					
6	b	¿Considera los requisitos referidos en el numeral 4.2?						1		
7	c	¿Considera las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones?						1		
8	Gr	¿El alcance está disponible como información documentada?						1		

Fuente: Autores

Ilustración 7. Fragmento del instrumento para la valoración de activos

EMPRESA DON POLLO SAS
ARMENIA - QUINDÍO
DEPARTAMENTO DE TECNOLOGÍA E INFRAESTRUCTURA
RELACIÓN Y VALORACIÓN DE ACTIVOS A CONSIDERAR EN EL DESARROLLO DEL PROYECTO AGR
AÑO 2019

OBJETIVO: Identificar los activos que componen el dominio, determinando sus características, atributos y clasificación en los tipos determinados según el catálogo de elementos - Magerit 3.0

PREGUNTA: ¿Un deterioro o perdida en el activo X como impacta la confidencialidad, integridad y TIponibilidad en el Servicio de Información Financiero SIF?

Calificar valores entre 1 y 5; siendo 1 el valor correspondiente a un impacto mínimo y 5 el valor correspondiente al impacto máximo.

Nombre de quien realiza la valoración: Carlos Andrés Giraldo Londoño

Nombre	Tipo	Subtipo	Descripción	Ubicación	Usuario encargado	Confidencialidad	Disponibilidad	Integridad	Total
Instructivos de uso para el Sistema de Información Financiero	D	Multimedia	Presentaciones PPT para inducciones, PDF con paso a paso dentro del sistema, Video manejo inicial del sistema	Oficina TI	Administrador del SIF	2	2	2	**3**
Código fuente producción	D	Source	Código en .NET, en ASP,HTML, código o scripts de BD, estructura de BD, Mantis (mesa de ayuda)	Oficina TI	Administrador del SIF	5	5	5	**10**
Código fuente respaldo	D	Source	Código en .NET, en ASP,HTML, código o scripts de BD, estructura de BD	Oficina TI	Administrador del SIF	4	4	4	**9**
Fuentes de proveedor	D	Source	Java(Aplicativo Web), Postgres(BD)	Oficina TI	Administrador de BD	2	3	2	**4**
Scripts de Copias de Seguridad	D	Source	Tareas programadas del Sistema Operativo enlazando a base de datos	Equipo Administración SIF	Administrador del SIF	4	4	4	**9**
Instaladores Servidores	D	exe	S.O(Windows 2003 Server), Motor de BD(Oracle 9i), Aplicación .NET 2003,Cualquier copia de seguridad del aplicativo, Scripts de tares programadas para copia de seguridad.	Área de servidores	Administrador de Redes y Correo Electrónico	2	3	2	**4**
Instaladores Clientes desarrollo	D	exe	.NET, Navegadores (IE, Chrome, Firefox), S.O. (Windows 7 SP1, Windows XP SP3)	Área de servidores	Mantenimiento y Soporte Técnico	2	2	2	**3**
Datos de configuración	D	conf	Datos de configuración o requisitos técnicos para poder ejecutar las aplicaciones(Características del servidor, aplicaciones que se instalan, interconexión, etc.)	Equipo Administración SIF	Mantenimiento y Soporte Técnico	4	2	3	**6**
Logs de auditoria	D	log	Logs de interacción con el sistema de ventas, de modificación en BD, los generados por el servidor, logs de interacción en mesa de ayuda.	Servidor SIF	Administrador del SIF	5	3	4	**9**
Usuario para pruebas	D	test	Usuario definido por el desarrollador para pruebas de las aplicaciones	Equipo Administración SIF	Administrador del SIF	5	5	5	**10**
Aplicativo Jooomla	SW	std	Aplicativo para la administración de la pagina web (Resuelve la presentación de la página web).	Servidor Pagina web	Administrador Página Web	3	4	4	**8**
Navegador	SW	Browser	Navegador de internet (IE, Chrome, Firefox)	Equipo Administración SIF	Mantenimiento y Soporte Técnico	1	4	1	**3**

Fuente: Autores

Ilustración 8. Fragmento del instrumento para la valoración de riesgos e impactos

Escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo

ESTIMACION DE IMPACTO

IMPACTO		DEGRADACION		
		1%	10%	100%
VALOR	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Valor		
MB: muy bajo	0	Imperceptible a la organización
B: bajo	1-3	Daño menor a la organización
M: medio	4-6	Daño importante a la organización
A: alto	7-9	Daño grave a la organización
MA: muy alto	10	Daño muy grave a la organización

ESTIMACION DEL RIESGO

RIESGO		FRECUENCIA			
		PF	FN	F	MF
IMPACTO	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

MF:	muy frecuente (a diario)
F:	frecuente (mensual)
FN:	frecuencia normal (anual)
PF:	poco frecuente (cada varios años)

Fuente: Autores

6.8 CONFIABILIDAD

El instrumento de la investigación se fundamenta en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013 y la Metodología de análisis y gestión de riesgos de los Sistemas de Información MAGERIT 3.0, específicamente en su componente de catálogo de elementos.

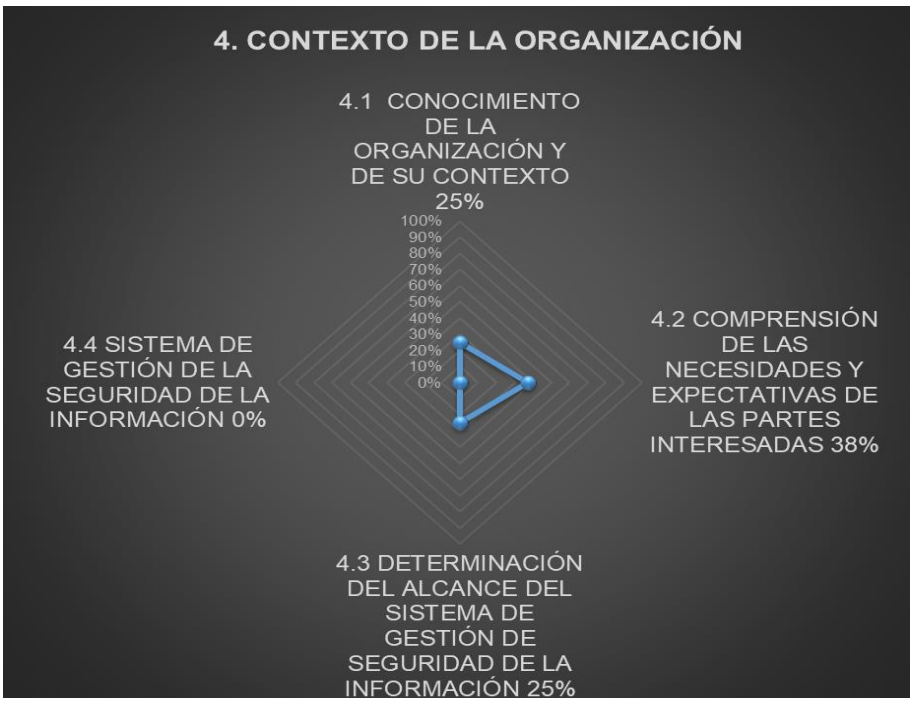
7. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

7.1 DOCUMENTACIÓN DEL SGSI EN BASE A LA NORMA NTC-ISO-IEC 270001:2013

7.1.1 DIAGNÓSTICO INICIAL DE CUMPLIMIENTO RELACIONADO CON LA NORMA NTC-ISO-IEC 27001:2013

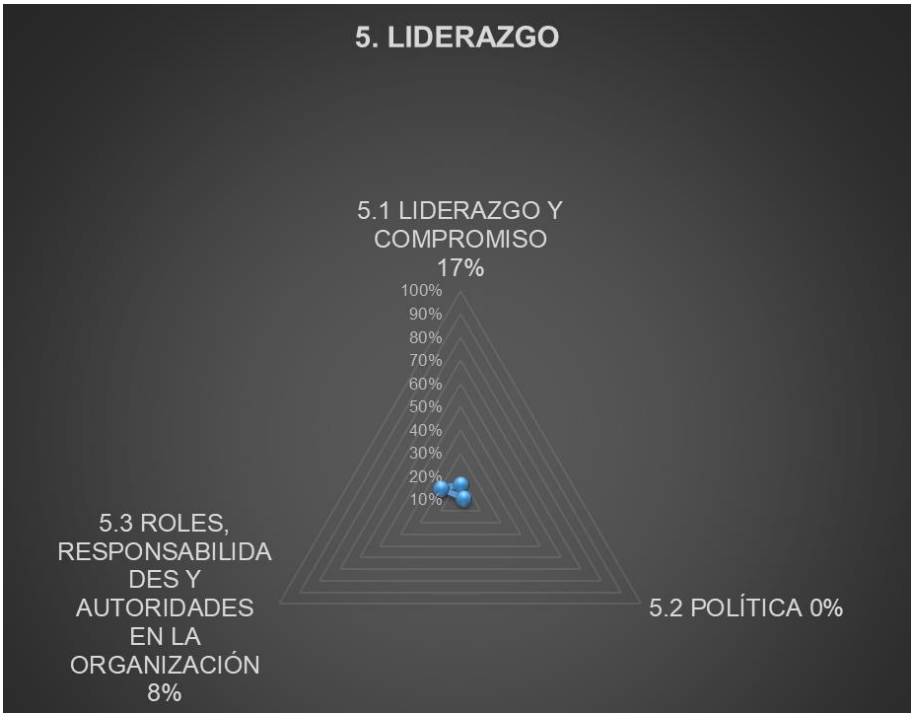
Se presentan a continuación cada uno de los resultados obtenidos del diagnóstico inicial en gráficos de radar, distribuido por cada uno de los numerales de la norma:

Ilustración 9. Resultados del diagnóstico en el numeral 4



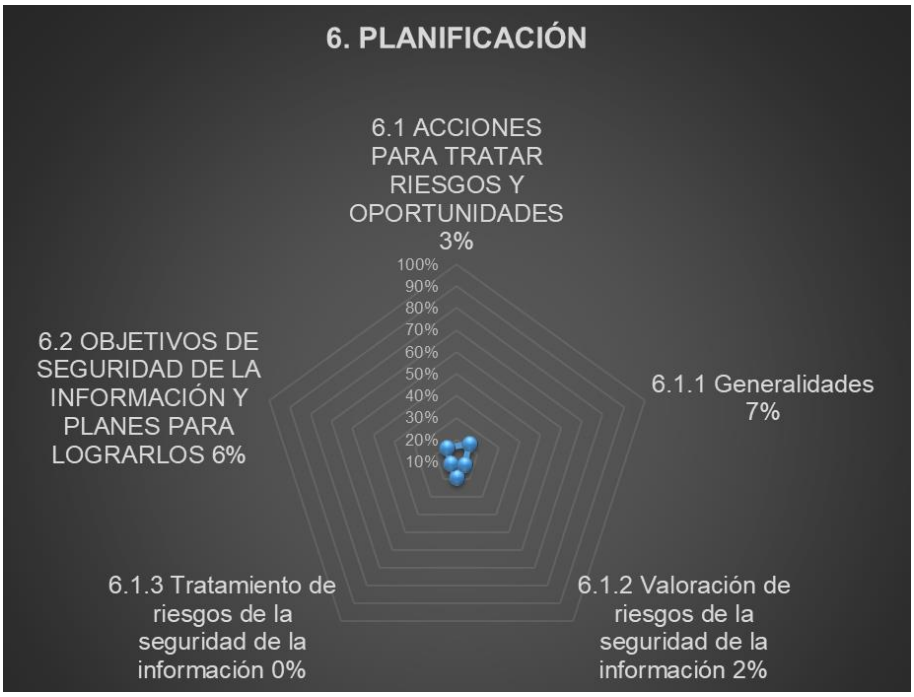
Fuente: Autores

Ilustración 10. Resultados del diagnóstico en el numeral 5



Fuente: Autores

Ilustración 11. Resultados del diagnóstico en el numeral 6



Fuente: Autores

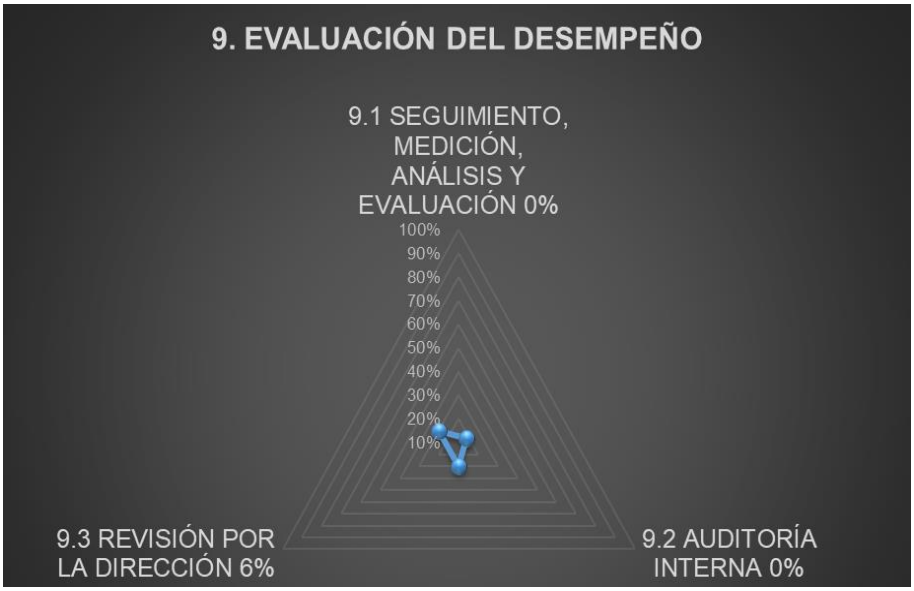
Ilustración 12. Resultados del diagnóstico en el numeral 7

Fuente: Autores

Ilustración 13. Resultados del diagnóstico en el numeral 8

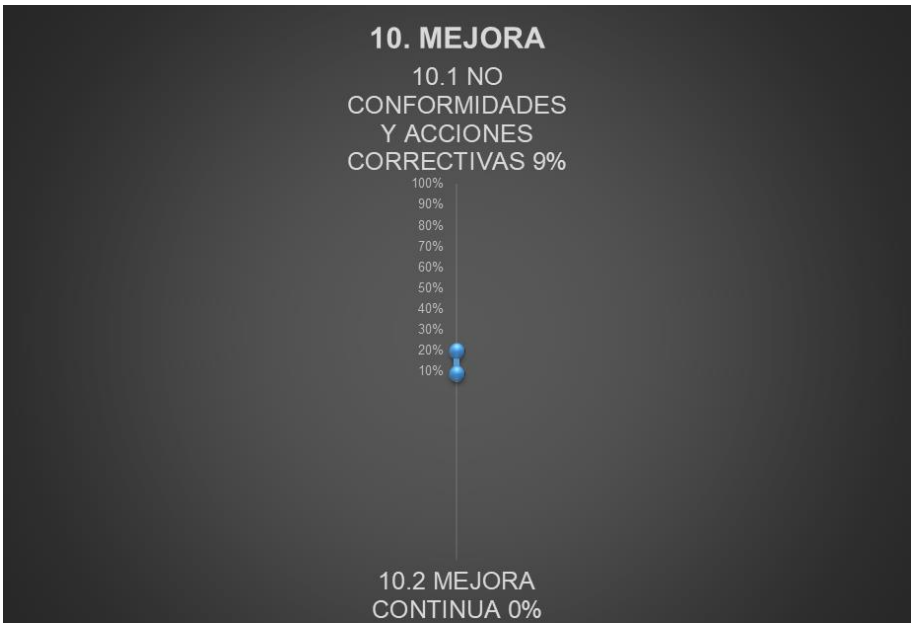
Fuente: Autores

Ilustración 14. Resultados del diagnóstico en el numeral 9



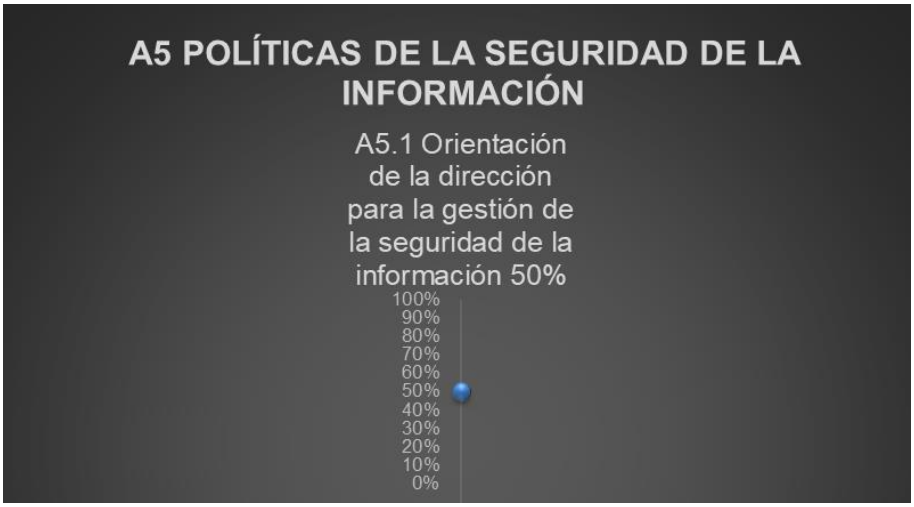
Fuente: Autores

Ilustración 15. Resultados del diagnóstico en el numeral 10



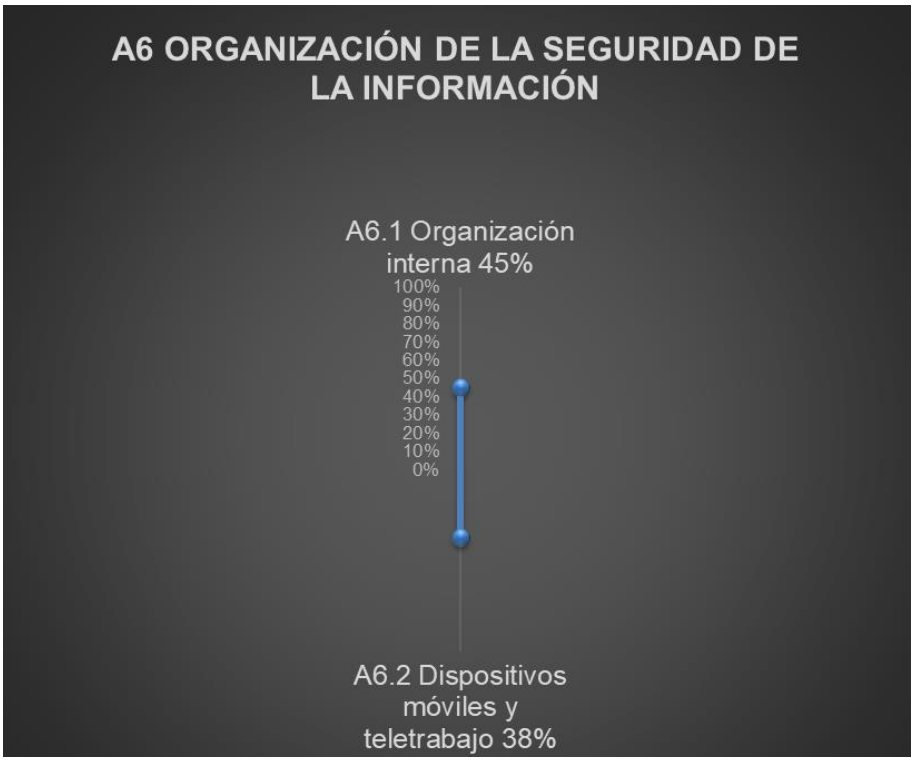
Fuente: Autores

Ilustración 16. Resultados del diagnóstico en el anexo A5



Fuente: Autores

Ilustración 17. Resultados del diagnóstico en el anexo A6

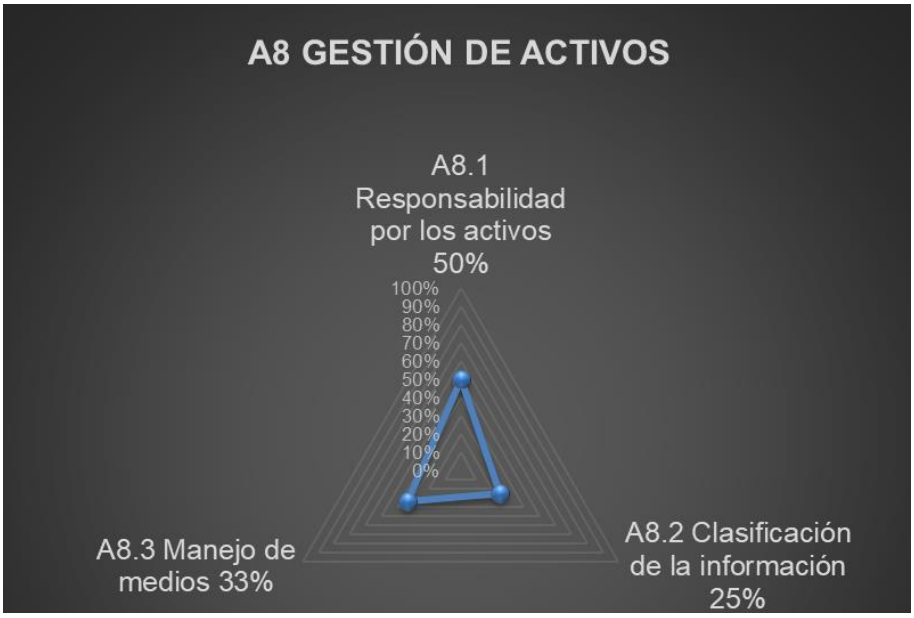


Fuente: Autores

Ilustración 18. Resultados del diagnóstico en el anexo A7

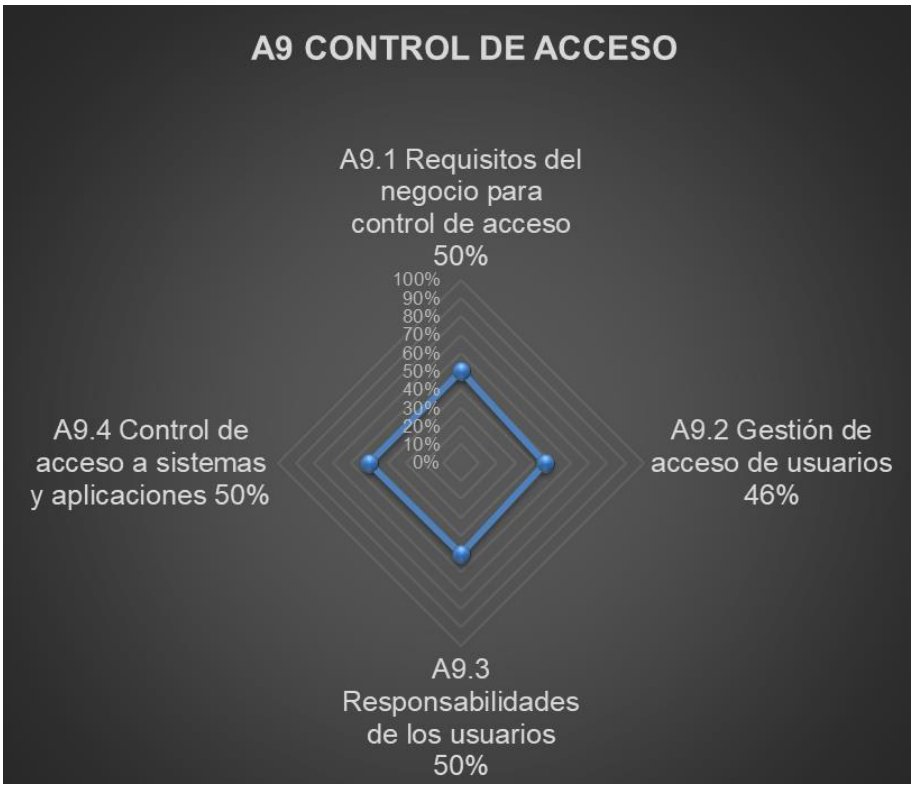
Fuente: Autores

Ilustración 19. Resultados del diagnóstico en el anexo A8



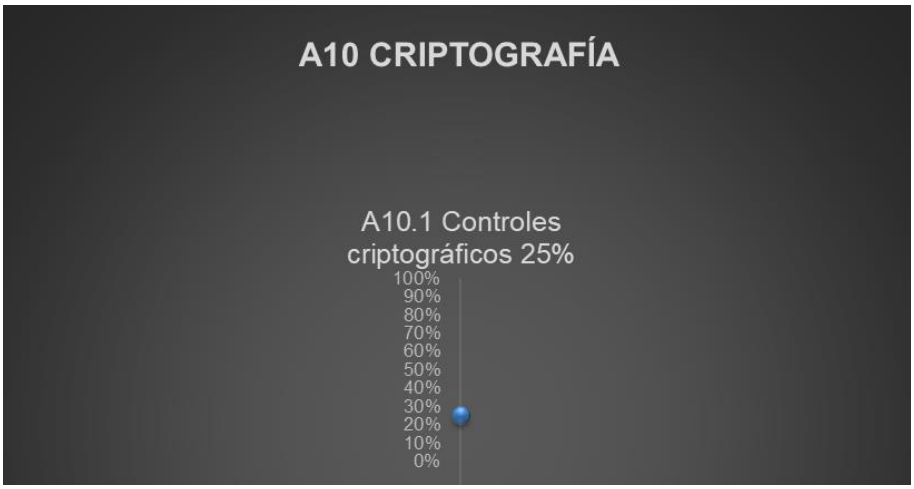
Fuente: Autores

Ilustración 20. Resultados del diagnóstico en el anexo A9



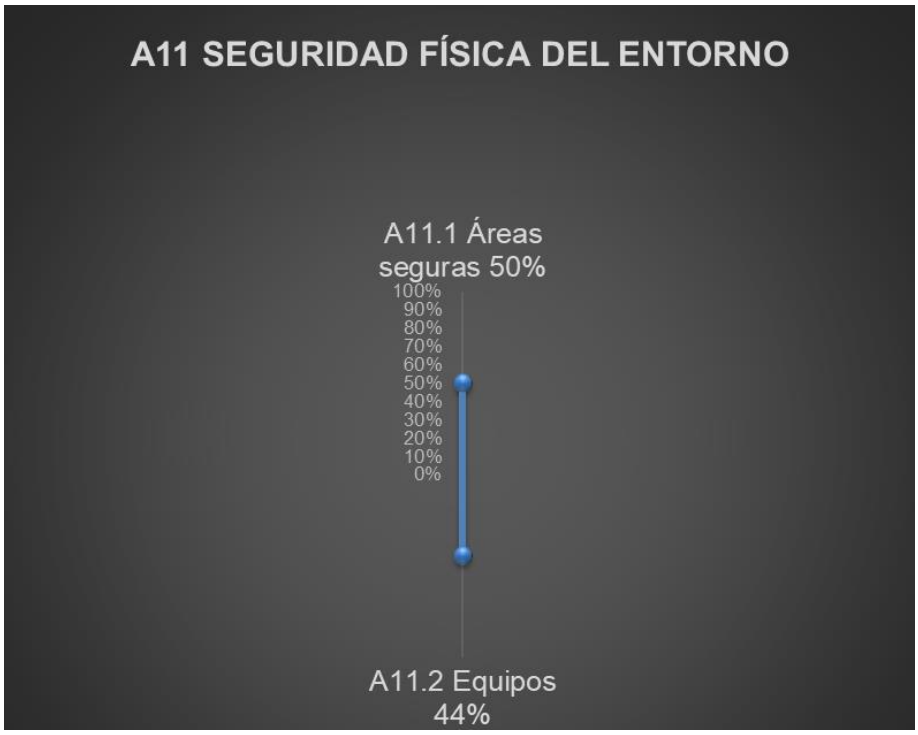
Fuente: Autores

Ilustración 21. Resultados del diagnóstico en el anexo A10



Fuente: Autores

Ilustración 22. Resultados del diagnóstico en el anexo A11

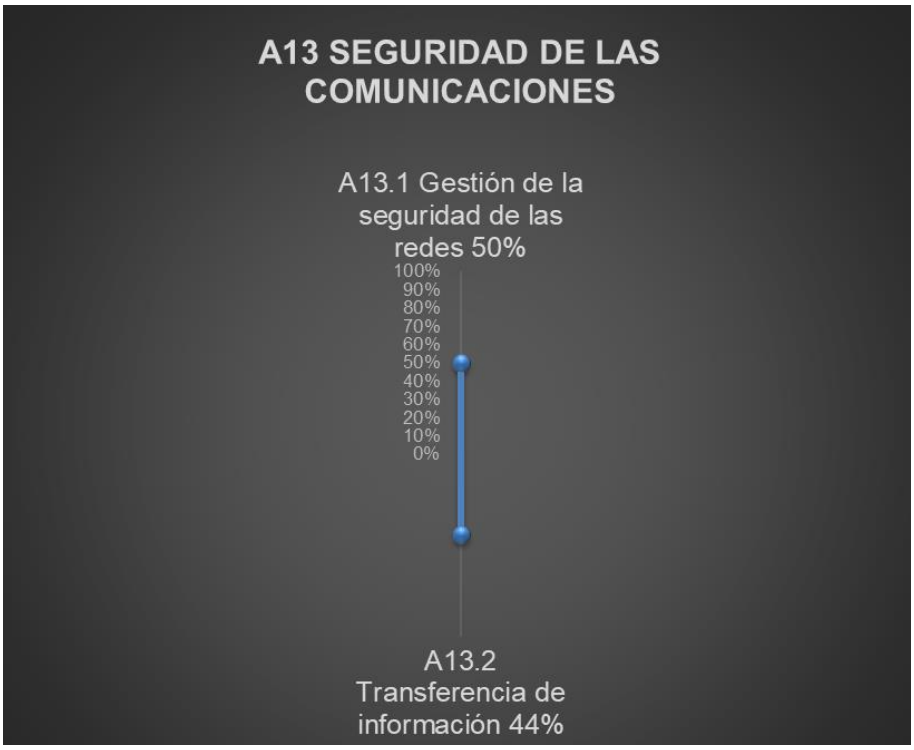


Fuente: Autores

Ilustración 23. Resultados del diagnóstico en el anexo A12

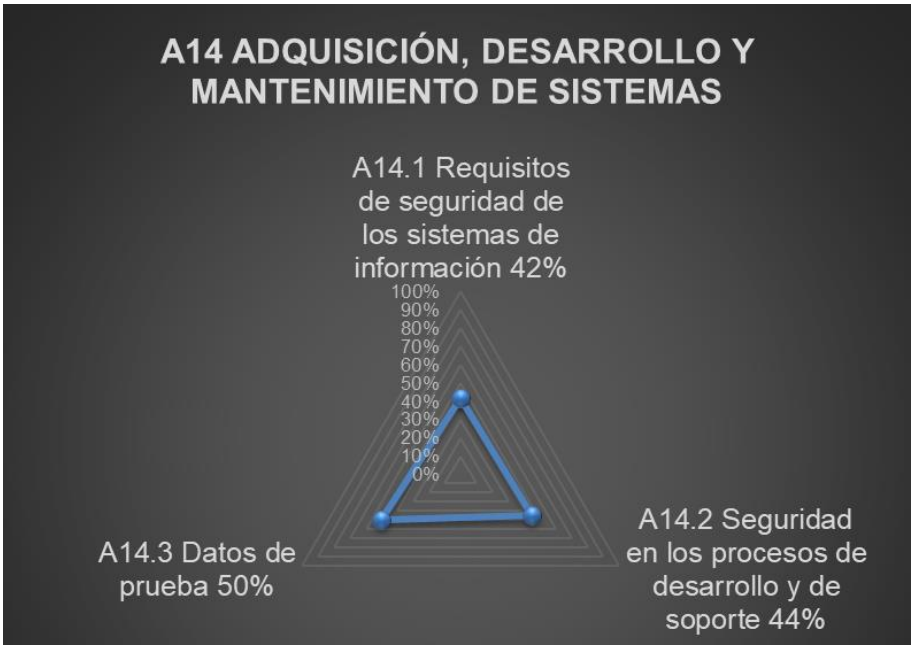
Fuente: Autores

Ilustración 24. Resultados del diagnóstico en el anexo A13



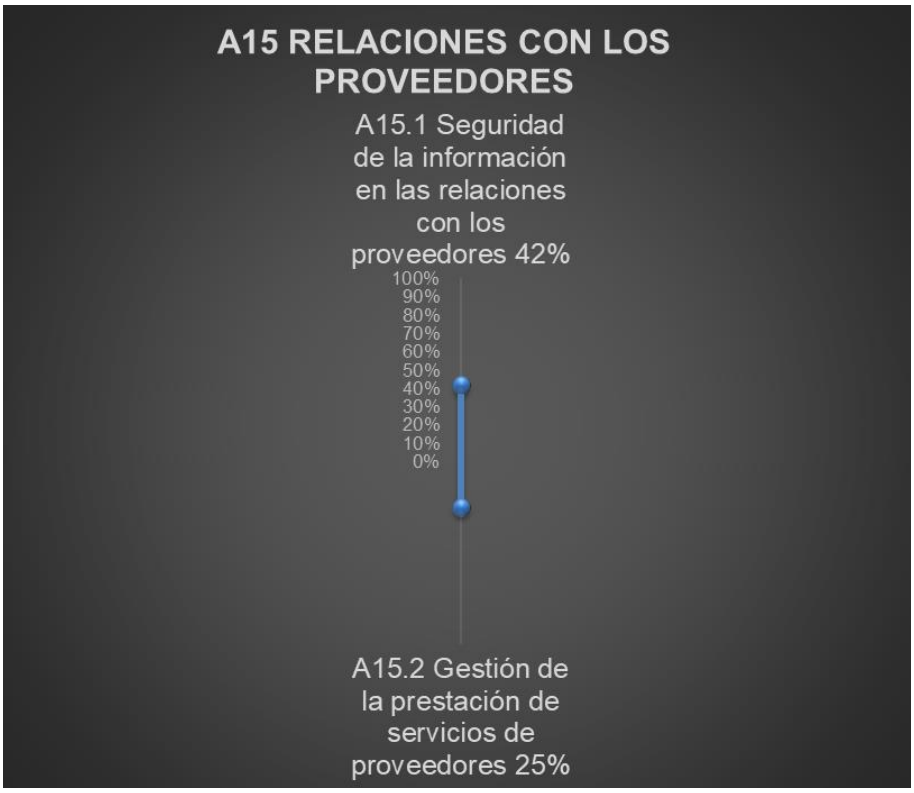
Fuente: Autores

Ilustración 25. Resultados del diagnóstico en el anexo A14



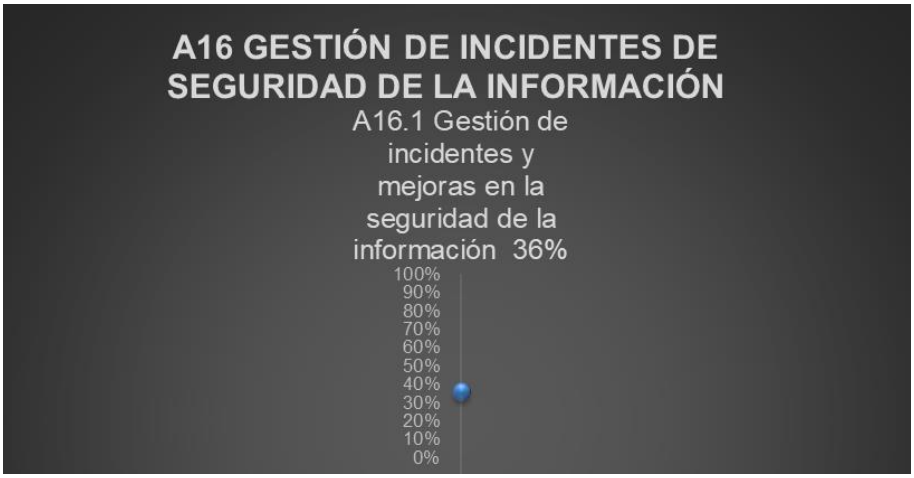
Fuente: Autores

Ilustración 26. Resultados del diagnóstico en el anexo A15



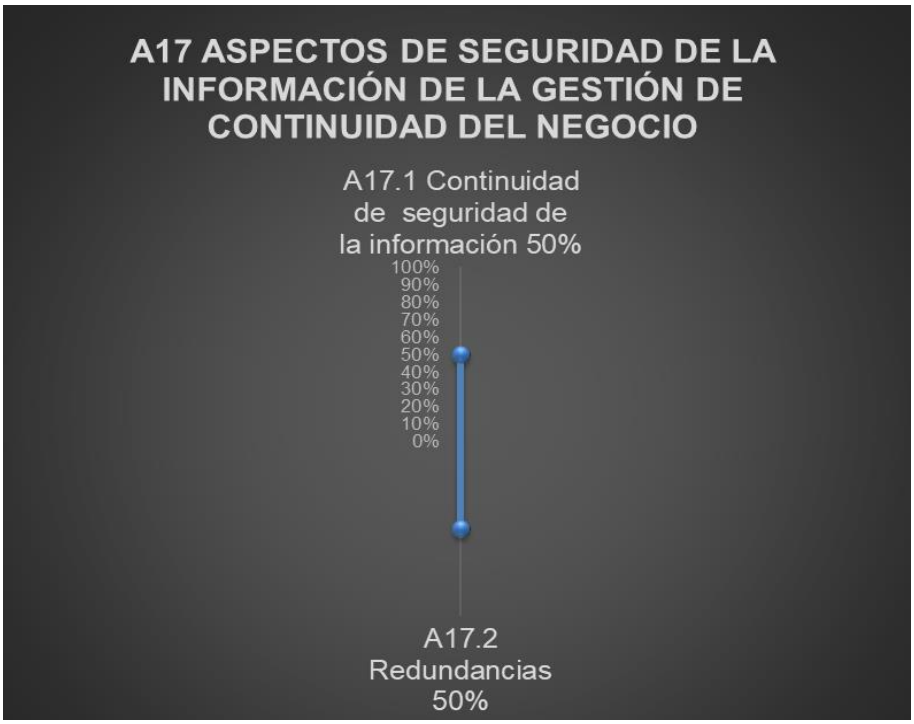
Fuente: Autores

Ilustración 27. Resultados del diagnóstico en el anexo A16



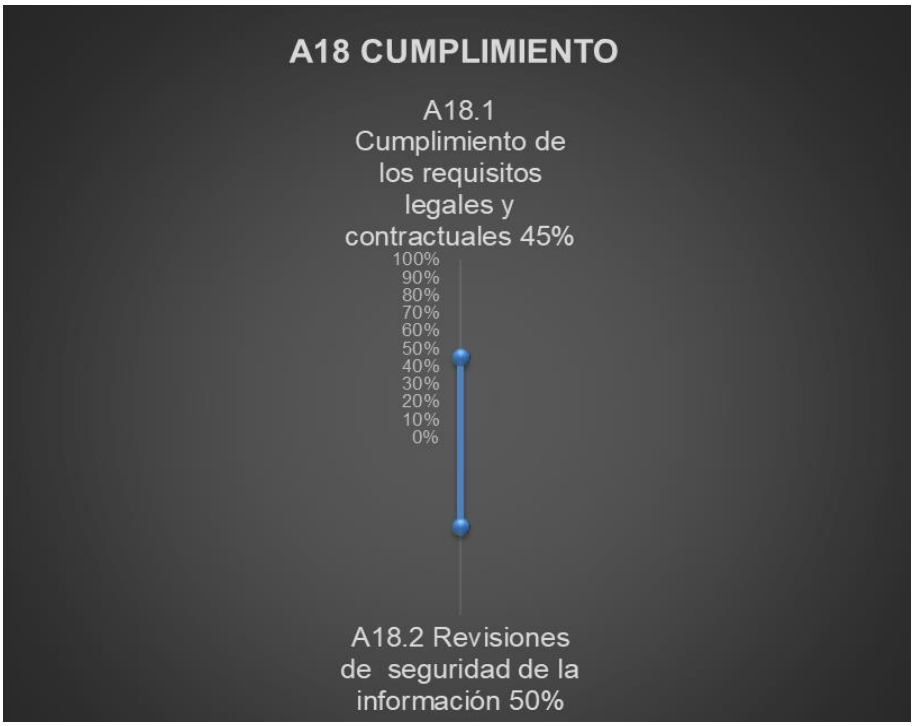
Fuente: Autores

Ilustración 28. Resultados del diagnóstico en el anexo A17



Fuente: Autores

Ilustración 29. Resultados del diagnóstico en el anexo A18



Fuente: Autores

Se realiza este análisis gráfico anterior con la intención de conocer el grado de implementación o de trabajo actual de los requisitos para el SGSI bajo los parámetros establecidos por la norma NTC-ISO-IEC 27001:2013. El diagnóstico se realiza bajo el modelo de una lista de chequeo donde se verifican cada uno de los numerales que debe tener implementados cualquier organización desde el capítulo cuatro (4) al diez (10) y del Anexo A (Objetivos de control y controles).

Los resultados generales de implementación en el alcance definido para la empresa Don Pollo SAS Armenia de los requisitos de la norma NTC-ISO-IEC 27001:2013 son:

- Implementación de los numerales cuatro (4) al diez (10) en un 10%.

- Implementación de los controles del anexo A en un 43%.

El resultado del diagnóstico sirve de facilitador para el futuro fortalecimiento de las actividades en caminadas a proteger la información en cada una de sus tres dimensiones de seguridad, como lo expresa la Norma NTC-ISO-IEC 27001:2013. La empresa a través del personal responsable de la seguridad de la información puede utilizar esta herramienta como monitor para su evaluación en el tiempo, acerca del grado de cumplimiento de cada uno de los requisitos. Ver la herramienta de diagnóstico inicial **Anexo G**.

7.1.2 DOCUMENTACIÓN DEL SGSI

Los documentos generados como soporte para el SGSI en el servicio de información financiera de la empresa Don Pollo SAS Armenia son:

- Documentación guía del SGSI; comprende la descripción del cómo se abordaron cada uno de los requisitos de la Norma NTC-ISO-IEC-27001:2013.

- Desarrollo de la metodología de análisis y gestión del riesgo; comprende la descripción de la aplicación de la metodología MAGERIT 3.0 en el alcance definido.

Luego de haber definido el alcance del SGSI y haber realizado un diagnóstico inicial de cumplimiento frente a la Norma NTC-ISO-IEC-27001:2013, se procede a elaborar el documento guía que comprende cada uno de los requisitos establecidos por esta norma y cada una de las herramientas sugeridas como soporte y apoyo en la implementación. Es importante destacar que elaborar este modelo del SGSI conlleva a elaborar un documento robusto adicional que corresponde al modelo de metodología de análisis y gestión de los riesgos adoptada. Los detalles de estos dos documentos, los cuales son la columna vertebral del proyecto, se encuentran

en el **Anexo H** (Basado en la Norma ISO-IEC-27001:2013) y **Anexo I** (Basado en la metodología MAGERIT 3.0)

7.2 RESULTADOS DEL PROCESO DE ANÁLISIS Y GESTIÓN DEL RIESGO

Como resultado del proceso de este proceso, se presenta a continuación el mapa de riesgos residual, también llamado mapa de calor, donde se relacionan cada uno de los identificadores de las amenazas con respecto a su probabilidad de ocurrencia y su impacto en el alcance del modelo de seguridad definido.

Tabla 5. Mapa de riesgo residual. Luego de evaluación de salvaguardas

RIESGO RESIDUAL			PROBABILIDAD				
			Muy poco frecuente	Poco frecuente	Normal	Frecuente	Muy frecuente
			0,010	0,100	1,000	10,000	100,000
IMPACTO	MA: muy alto	24,001 - 30,000					
	A: alto	18,001 - 24,000				E.19, A.7,	
	M: medio	12,001 - 18,000	N.1,	A.19, N.2, N.*, I.1, I.*, I.11, A.26,	E.2, A.6, E.15, E.18, A.15, I.2,	A.5,	
	B: bajo	6,001 - 12,000	I.4, E.3, A.3,	A.18, I.3, A.23, E.24, A.24, A.28, A.4,	I.5, I.7, E.23, E.25, A.25, A.29,	I.6, A.13, E.7, E.28, A.30,	E.1,
	MB: muy bajo	0,000 - 6,000	A.11, A.9, A.10, A.27, A.14, A.8,	A.12, E.20, A.22, I.10,	E.4, I.9, E.9, E.10, E.21,	I.8, E.8,	

Fuente: Autores

Se aplica el proceso de análisis y gestión de los riesgos de la información con la adopción de la metodología MAGERIT 3.0, los resultados se encuentran descritos en los documentos **Anexo I** y **Anexo M**. El análisis y gestión de los riesgos es el proceso crucial para la operación del SGSI, esta es la base para que la empresa determine su modelo de seguridad de la información. El resultado final se consolida en el mapa de riesgos, el cual se convierte en el principal monitor para que la empresa continúe activamente con la madurez del SGSI.

7.3 ESTRUCTURA DE PROCEDIMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información se constituye en un conjunto de políticas, procesos y procedimientos; la empresa Don Pollo SAS recibe el documento guía del SGSI, basado en la Norma NTC-ISO-IEC 27001:2013 con cada uno de los componentes y/o herramientas que describen procedimentalmente las actividades a seguir para la gestión de la seguridad de la información. Como resultado de este proyecto, se entregan quince (15) herramientas anexas en formato Excel que soportan el SGSI dentro de todo su ciclo PHVA. Para su comprensión se recomienda interpretarlas o utilizarlas en base a la lectura del documento guía para el SGSI y del documento del desarrollo de la metodología de análisis y gestión del riesgo.

Tabla 6. Listado de herramientas para el soporte del SGSI

HERRAMIENTAS UTILIZADAS PARA EL SOPORTE DEL SGSI	
NOMBRE	**DESCRIPCIÓN**
Anexo G. Diagnostico_Inicial_Cumplimiento_ISO_27001.xlsx	Corresponde a la descripción de cada numeral de la Norma NTC-ISO-IEC 27001:2013 y del Anexo A (objetivos de control y controles) con su respectivo indicador de implementación en la empresa.
Anexo J. Contexto_De_La_Organizacion_Matriz_Cruzada.xlsx	Análisis DOFA cruzada con las respectivas valoraciones de debilidades, oportunidades, fortalezas y amenazas que permiten determinar estrategias empresariales y priorizarlas. Contiene el plan de acción para la ejecución de las estrategias.
Anexo K. Partes_interesadas_Necesidades_Expectativas.xlsx	Relación de cada una de las partes interesadas (internas y externas) con su respectiva valoración de poder e interés que representan para el alcance del SGSI. Contiene el plan de acción para la ejecución de las estrategias y el modelo gráfico de poder - interés.
Anexo L. Matriz_Juran_Politica_Objetivos.xlsx	Matriz de ponderación de la importancia asignada a las necesidades y expectativas de las partes interesadas (internas y externas), de donde su evaluación y análisis determinan los objetivos y la política de seguridad de la información.
Anexo M. Analisis_De_Riesgos.xlsx	Herramienta que comprende todo el proceso de análisis, valoración y gestión de los riesgos de la información, con el respectivo mapa de calor. Aquí se ejecutan todos los cómputos que determinan el impacto sobre la operación del negocio en su alcance definido.
Anexo O. Valoraciones_De_Activos_Area_TIC.xlsx	Valoración de cada uno de los activos de información (inventario de activos) en cada una de las dimensiones de seguridad (confidencialidad, integridad y disponibilidad). Es el punto de partida para el análisis y gestión de los riesgos de la información.

HERRAMIENTAS UTILIZADAS PARA EL SOPORTE DEL SGSI	
NOMBRE	**DESCRIPCIÓN**
Anexo Q. Declaracion_De_Aplicabilidad.xlsx	Describe cada uno de los controles y objetivos de control descritos en el Anexo A de la Norma NTC-ISO-IEC 27001:2013 con cada una de las actividades que la empresa aplica para darle cumplimiento a cada objetivo y la declaración de lo que se debe implementar si la empresa no lo posee o tiene deficiencias.
Anexo R. Plan_Estrategico_De_Capacitacion_Sensibilizacion_Comunicacion.xlsx	Planificación de cada uno de los objetivos y estrategias de formación y comunicación dentro de la empresa para establecer, mantener y mejorar el SGSI. Aquí se describen los mecanismos de evaluación para cada objetivo definido.
Anexo S. Proyeccion_Presupuesto_Recursos_TI_SGSI.xlsx	Determinación de gastos e inversiones del área de TI para el periodo siguiente (anual), considerando mantener y mejorar el SGSI.
Anexo T. Programa_Plan_De_Auditoria.xlsx	Herramienta para programar y llevar a cabo los ciclos de auditorías internas. Contiene el alcance, los objetivos y la lista de verificación. Es una de las herramientas bases para llevar a cabo la ejecución de acciones correctivas y de mejora en el SGSI.
Anexo U. Acciones_Correctivas_Y_Oportunidades_De_Mejora.xlsx	Herramienta para realizar el seguimiento a los hallazgos, a través de su análisis de causas, cronograma de resolución y plan de acción.
Anexo V. Requisitos_Cliente_Legales_Organizacionales.xlsx	Matriz que describe la legislación aplicable y demás requisitos de las partes interesadas.
Anexo W. Anexo_W_Relacion_Documentacion_Empresarial.xlsx	Contiene la codificación y nombres de los documentos de tipo procedimientos, instructivos, manuales, políticas, formatos, entre otros, pertinentes para la gestión de la seguridad de la información.

Fuente: Autores

7.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para el establecimiento de la política de la seguridad de la información se tienen en cuenta las necesidades y expectativas de las partes interesadas, de allí surgen las directrices que orientan su estructuración y para cada una de estas directrices se establece un objetivo de seguridad de la información con su respectiva meta.

La política posee total correspondencia con la planeación estratégica de la empresa y enmarca los principios de seguridad que guían las actividades que se desarrollan dentro de la misma. Ver archivo **Anexo B**.

Como resultado del proceso de análisis y gestión de riesgos, se procede a diseñar el conjunto de políticas específicas de seguridad de la información, las cuales se presentan en la tabla siguiente. Ver archivo **Anexo X**.

Para conocer la herramienta que se utilizó en la definición de la política ver archivo **Anexo L**.

Tabla 7. Listado de las políticas de seguridad de la información

NOMBRES Y TIPOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
POLÍTICA GENERAL
POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN
CON RELACIÓN A LA ORGANIZACIÓN DE LA SEGURIDAD
COMITÉ OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN
ASIGNACIÓN DE ROLES Y RESPONSABILIDADES
AUTORIZACIÓN PARA OPERAR ESTACIONES DE PROCESO DE LA INFORMACIÓN
PROMOCIÓN Y ASESORAMIENTO EN EL MODELO DE SEGURIDAD DE LA INFORMACIÓN
CON RELACIÓN AL OTORGAMIENTO DE ACCESO A TERCERAS PARTES
IDENTIFICACIÓN DE RIESGOS DEL ACCESO DE TERCERAS PARTES
REQUERIMIENTOS DE SEGURIDAD EN LA VINCULACIÓN CON TERCERAS PARTES
CON RELACIÓN A LA CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN
INVENTARIO DE ACTIVOS
CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN
VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN
CON RELACIÓN A LA SEGURIDAD DEL PERSONAL

NOMBRES Y TIPOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
INCORPORACIÓN DE LA SEGURIDAD EN LOS PUESTOS DE TRABAJO
COMPROMISO DE CONFIDENCIALIDAD
TÉRMINOS Y CONDICIONES DE EMPLEO
SENSIBILIZACIÓN, FORMACIÓN Y CAPACITACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN
REPORTE DE INCIDENTES RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN
COMUNICACIÓN DE DEBILIDADES EN MATERIA DE SEGURIDAD
TRATAMIENTO DE NOVEDADES DEL SOFTWARE
RETROALIMENTACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN
CON RELACIÓN A LA SEGURIDAD FÍSICA Y AMBIENTAL
PERÍMETRO DE SEGURIDAD FÍSICA
CONTROLES DE ACCESO FÍSICO
PROTECCIÓN DE AREAS LOCATIVAS
DESARROLLO DE LAS ACTIVIDADES LABORALES EN ÁREAS PROTEGIDAS
AISLAMIENTO DE ÁREAS ADMINISTRATIVAS ADICIONALES
UBICACIÓN DE ACTIVOS FÍSICOS
SUMINISTRO DE ENERGÍA
SEGURIDAD DEL CABLEADO DE RED
MANTENIMIENTO DE EQUIPOS
SEGURIDAD DE LOS EQUIPOS POR FUERA DE LAS INSTALACIONES
REUTILIZACIÓN O REASIGNACIÓN DE EQUIPOS
ESCRITORIO LIMPIO
RETIRO Y BAJA DE ACTIVOS
CON RELACIÓN A LA GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES
DOCUMENTACIÓN DE LAS ACTIVIDADES OPERATIVAS
CONTROL DE CAMBIOS EN LAS OPERACIONES
MANEJO DE INCIDENTES
LABORATORIOS Y ESCENARIOS DE PRUEBAS
GESTIÓN DE INSTALACIONES EXTERNAS
PLANIFICACIÓN DE LA CAPACIDAD
CONTROL CONTRA SOFTWARE MALICIOSO
RESGUARDO DE LA INFORMACIÓN
CONTROLES EN LA RED
ADMINISTRACIÓN DE MEDIOS DE ALMACENAMIENTO
ADMINSITRACIÓN DE MEDIOS DE ALMACENAMIENTO REMOVIBLES

NOMBRES Y TIPOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
ADMINISTRACIÓN DEL CORREO ELECTRÓNICO
ACCESOS REMOTOS
CON RELACIÓN AL CONTROL DE ACCESOS
POLÍTICA DE CONTROL DE ACCESOS
ADMINISTRACIÓN DE USUARIOS
GESTIÓN DE PRIVILEGIOS
GESTIÓN DE CONTRASEÑAS
ACCESO A INTERNET
CONTROL DE ACCESO A LAS APLICACIONES
MONITOREO Y LOGS DE USO DE LOS SISTEMAS
CON RELACIÓN A LA CONTINUIDAD DE LAS OPERACIONES
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
ANÁLISIS DE IMPACTOS Y TIEMPOS DE RECUPERACIÓN
CON RELACIÓN AL CUMPLIMIENTO
CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE
PROTECCIÓN DE DATOS PERSONALES
CUMPLIMIENTO DE LOS REQUSITOS DE SEGURIDAD DE LA INFORMACIÓN
SANCIONES POR INCUMPLIMIENTO

Fuente: Autores

La formulación de políticas se convierte en una práctica imprescindible para gestionar la seguridad de la información, establecen un marco de operación, con los lineamientos para alcanzar los objetivos de seguridad planteados y determinar conductas esperadas en el desarrollo de las actividades de la empresa.

8. CONCLUSIONES

- Modelar un esquema de SGSI bajo un estándar certificado a nivel mundial no representa que la empresa se encuentre en un nivel avanzado de seguridad. Las dificultades de seguridad de la información no se resuelven solo con implementar cada una de las herramientas y métodos descritos en este trabajo; el modelo debe trascender los aspectos tecnológicos dentro de la empresa, involucra cambios en el comportamiento de las personas, pensamiento sistémico para todas las operaciones y actividades, desarrollar actividades que aporten valor y una dirección comprometida y capaz de aumentar el nivel de madurez del SGSI.

- En el proceso de análisis y gestión del riesgo, las personas representan el eslabón más débil dentro de la cadena, es por ello que se convierten en el principal punto de atención para el ciclo de vida del SGSI. Muchos de los factores que afectan la disponibilidad e integridad de la información involucran al personal como parte de las causas. No se puede desligar la operación de los sistemas informáticos de la manipulación humana, ya que estos sistemas son creados por personas para ser configurados y/o ejecutados por personas.

- La metodología de análisis y gestión del riesgo adoptada por la empresa como complemento de la implementación de un SGSI se constituye en su principal soporte, ya que allí se identifican los activos, sus amenazas y vulnerabilidades, para que a partir de ello se elaboren y ejecuten los planes de tratamiento, con la intención de minimizar o eliminar los riesgos. Es el monitor principal del estado del esquema de seguridad de la información de la empresa.

- Aplicar el enfoque basado en procesos dentro de las operaciones de la empresa, genera valor para la misma, ya que se gestionan y controlan cada una de las interacciones y se determinan las jerarquías funcionales. Esta gestión por procesos determina grados de complejidad que, al estar alineados con la planeación estratégica de la empresa, son aporte importante en la toma de decisiones.

- La política de seguridad de la información es la principal directriz para los procesos de seguridad de la información, siendo esta el punto de referencia para determinar controles o medidas a implementar. Debería ser interiorizada dentro de la empresa, de tal manera que se convierta en parte de la determinación del comportamiento de las personas dentro de las operaciones.

9. RECOMENDACIONES

Luego de la entrega de esta estructuración de documentación para el SGSI en la empresa Don Pollo SAS, se considera continuar con el concepto de sistema de gestión, donde a través del aprovechamiento del trabajo realizado y de unas adecuadas decisiones, este sea el insumo para el mejoramiento continuo operacional. Se describe a continuación algunas de las recomendaciones:

- Implantación del SGSI: La empresa pudiera considerar dentro de su planeación estratégica la implantación del SGSI. Comenzando por el alcance definido en este trabajo y luego expandiéndolo a todos los procesos. El estándar internacional ISO 27001 se ha convertido en el más extendido a nivel mundial para el diseño e implementación de un SGSI y permite obtener certificación internacional.

- Integración con otros sistemas de gestión: Los sistemas de gestión permiten a las empresas estructurar de una manera sistemática sus operaciones para mejorar su control; en el caso que la empresa tenga estructurado otro sistema de gestión basado en un estándar de la ISO, como el de la calidad, ambiental, seguridad y salud en el trabajo, entre otros, existe un enfoque común definido en el Anexo SL (Estructura de alto nivel) de estos estándares, el cual utiliza títulos idénticos de numerales, texto idéntico y definiciones comunes. Lo anterior facilita la puesta en funcionamiento de un único sistema de gestión que cumpla con los requerimientos de dos o más estándares, a esto es lo que le conoce comúnmente como sistema integrado de gestión.

- Análisis y gestión de los riesgos de la información continuamente: Los riesgos cambian con la evolución de la empresa al surgir nuevas modalidades de amenazas y aparición de vulnerabilidades; el proceso de análisis y gestión del riesgo debería realizarse constantemente, al ritmo de adaptación de la empresa al entorno. El acelerado crecimiento de las tecnologías de la información trae consigo cambios en la manera de exposición al riesgo, también la empresa dentro de su crecimiento y posicionamiento nacional ha aumentado la dependencia de estas tecnologías para la correcta operación de sus procesos. El proceso de gestión de los riesgos si no se convierte en repetitivo, tiende a quedar obsoleto.

- Implementación de escenarios de prueba: El inventario de activos es la herramienta que se utiliza como punto de partida para el ejercicio de análisis y gestión de los riesgos de la información; se recomienda plantear escenarios donde se simule la materialización de un incidente de seguridad de la información, así como los simulacros de ejecución de planes de continuidad. Lo anterior para validar la eficiencia y eficacia del SGSI.

- Ampliar el alcance a otros procesos: El tema de la estructuración y operación de un SGSI no debería quedar centralizado en las unidades de administración de TI, a medida que se la mejora continua va madurando el sistema, se hace necesario establecer mecanismos colaborativos dentro de la empresa para que trascienda a todos los procesos de negocio y aporte verdadero valor organizacional.

- Preparar la empresa para auditorías externas: La correcta implementación y uso de las herramientas expuestas en el desarrollo del presente trabajo, facilita llevar a cabo un proceso de auditoría por una entidad externa a la empresa y de esta manera establecer un indicador de suficiencia frente al cumplimiento de los requisitos.

- Actualización de la documentación en base a la evolución de las normas y metodologías: Dentro de los procesos de mejora continua, la empresa debería consultar constantemente en los sitios o proveedores oficiales de las normas técnicas y metodologías utilizadas acerca de las actualizaciones que se realicen y posterior a ello planificar la incorporación de los cambios. La empresa también puede explorar métodos alternativos que complementen todo el trabajo desarrollado a la fecha.

BIBLIOGRAFÍA

ALEXANDER, Alberto. Diseño de un Sistema de Gestión de Seguridad de la Información. Alfaomega, edición 1 (05 de noviembre de 2007). 176 p.

ANGARITA, A. A.; TABARES, C.A. y RIOS, J.I. Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento. Entre Ciencia e Ingeniería vol 9, no 17 (junio de 2015). 10 p.

GOBIERNO DE ESPAÑA. PAe - Portal de Administración Electrónica. [Consultado: 06 de abril de 2019]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home.html#.XLFoXegzbcs.

GÓMEZ BARROSO, José Luis. Uso y valor de la información personal: un escenario en evolución. El Profesional de la Información vol 27, no 1 (12 de febrero de 2018). 14 p.

ICA. MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI. [Consultado: 29 de noviembre de 2019]. Disponible en internet:https://www.ica.gov.co/getattachment/Modelo-de-P-y-G/Eficiencia-Administrativa/Procesos-y-Procedimientos/ManualSGSI-Agosto-2018.pdf.aspx?lang=es-CO. 53 p.

ICONTEC. ICONTEC e-Collection. [Consultado: 03 de abril de 2019]. Disponible en internet: https://ugc.elogim.com:2741/normavw.aspx?ID=74790.

ISO. ISO - International Organization for Standardization. [Consultado: 03 de abril de 2019]. Disponible en internet: http://www.iso.org/cms/render/live/en/sites/isoorg/home.html.

JIMENEZ, Martín Antonio; ELOY, Vicente y ALFONSO, Mateos. Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, no 15 (junio de 2015). 18 p.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información. MAGERIT 3.0, LIBRO I – Método (octubre de 2012). 127 p.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información. MAGERIT 3.0, LIBRO II – Catálogo de elementos (octubre de 2012). 75 p.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información. MAGERIT 3.0, LIBRO III – Guía de Técnicas (octubre de 2012). 42 p.

MINTIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - Guía de Mejora Continua. [Consultado: 11 de noviembre de 2019]. Disponible en internet:https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf. 10 p.

MUÑOZ, Mirna y RIVAS, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, no SPE3 (marzo de 2015). 15 p.

PORCELLI, Adriana Margarita. (Des) Protección del derecho de autor en la era digital. Principales tendencias legislativas, doctrinarias y jurisprudenciales argentinas sobre la denominada “piratería informática” / (DIS) protection of copyright in the digital age. Major argentine.... REVISTA QUAESTIO IURIS. [Consultado: 12 de abril de 2019]. 38 p.

PORTAL ISO 27001 ESPAÑOL. ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. [Consultado: 03 de abril de 2019]. Disponible en internet: http://www.iso27000.es/iso27000.html.

SERRANO COBOS, Jorge. Tendencias tecnológicas en internet hacia un cambio de paradigma. El Profesional de la Información vol 25, no 6 (14 de noviembre de 2016). 8 p.

SOCIAL. Documento Conpes 3854, Política Nacional de Seguridad Digital. [Consultado: 11 de abril de 2019]. Disponible en internet: http://bibliotecadigital.ccb.org.co/handle/11520/14856.

SOLANO RODRÍGUEZ, Omar Javier; GARCÍA PÉREZ, Domingo y BERNAL, Juan Jesús. El sistema de información y los mecanismos de seguridad informática en la pyme. Punto de Vista vol 7, no 11 (2016). 20 p.

VILLENA AGUIRRE, Moisés Antonio. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Pontificia Universidad Católica del Perú, 30 de octubre de 2014. 59 p.

ANEXOS

Anexo A. Estado del arte.

Anexo B. Política de seguridad de la información.

Anexo C. Declaración de aplicabilidad.

Anexo D. Metodología MAGERIT v3. Método 2012.

Anexo E. Metodología MAGERIT v3. Catálogo de elementos 2012.

Anexo F. Metodología MAGERIT v3. Guía de técnicas 2012.

Anexo G. Diagnóstico inicial de cumplimiento de la Norma NTC-ISO-27001:2013.

Anexo H. Documentación guía del SGSI en la empresa Don Pollo SAS Armenia.

Anexo I. Desarrollo de la metodología de análisis y gestión del riesgo.

Anexo J. Matriz cruzada como identificación del contexto.

Anexo K. Determinación de las partes interesadas, necesidades y expectativas.

Anexo L. Matriz Juran para la construcción de la política y objetivos de la seguridad de la información.

Anexo M. Análisis y gestión de los riesgos de la información.

Anexo N. Formato para la valoración de activos.

Anexo O. Valoraciones de los activos de la información en el área de administración TIC.

Anexo P. Simulación de impacto con probabilidad de ocurrencia normal.

Anexo Q. Estructura de la declaración de aplicabilidad.

Anexo R. Plan estratégico de capacitación, sensibilización y comunicación.

Anexo S. Proyección presupuestal de recursos TI para el SGSI.

Anexo T. Programa y plan de auditoría.

Anexo U. Tratamiento de acciones correctivas y oportunidades de mejora.

Anexo V. Matriz de requisitos del cliente, legales, intrínsecos y organizacionales.

Anexo W. Relación de tipos de documentos para la gestión de la empresa.

Anexo X. Políticas de seguridad de la información.