FRAMEWORK BAJO ARQUITECTURA ARM Y SOFTWARE GPLV3 CON SINCRONIZACIÓN A LA NUBE, PARA APOYAR EN EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMACIÓN – SGSI DE LA NORMA ISO/IEC 27001

EDUAR HERNÁN AGUIRRE AGUDELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

FRAMEWORK BAJO ARQUITECTURA ARM Y SOFTWARE GPLV3 CON SINCRONIZACIÓN A LA NUBE, CON BASE EN UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI EN LA NORMA ISO/IEC 27001

EDUAR HERNÁN AGUIRRE AGUDELO

Proyecto aplicado para optar al título de
Especialista en Seguridad Informática

Esp. Ing. Freddy Enrique Acosta
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cali, 05 de octubre de 2021

Inicialmente a Dios Todopoderoso, a la Virgencita por brindarme la fuerza, fortaleza, sabiduría y entendimiento para llevar a cabo este trabajo de forma exitosa. y a mi madre, esposa, hijo, hermana y demás seres queridos por su apoyo incondicional brindado en diferentes momentos al ir desarrollando la especialización de Seguridad informática y a la Universidad Nacional Abierta y a Distancia UNAD y sus docentes por el apoyo brindado oportunamente durante el desarrollo del presente proyecto.

Eduar Hernán Aguirre Agudelo

AGRADECIMIENTOS

Eduar Hernán Aguirre Agudelo expresa su agradecimiento a:

ESP. ING. Juan José Cruz y ESP. ING Christian Reynaldo Angulo, de la Universidad Nacional Abierta y a Distancia, por brindar asesoría en el desarrollo del proyecto de Seguridad informática 1 y su disponibilidad para enriquecer el trabajo realizado.

ESP. ING. Freddy Enrique Acosta por sus aportes y sugerencias brindadas durante el desarrollo del presente proyecto aplicado en su recta final y su disponibilidad para enriquecer el trabajo realizado.

ESP. ING Fernando Zambrano, de la Universidad Nacional Abierta y a Distancia, por valiosa formación en el campo de riesgo y control informático, al igual que las web conferencias que lidero desde el semillero de investigación de la UNAD.

ESP. ING Eduard Antonio Mantilla Torres de la Universidad Nacional Abierta y a Distancia, por sus valiosas observaciones como jurado de UNAD.

A la empresa BIDDA SAS, por permitirme crecer como profesional y ser humano, por financiarme parte de mi estudio como profesional, al igual que me han brindado espacios especiales en aras de avanzar con mis estudios profesionales.

A la profesional en Salud Ocupacional María Camila Aguirre, por su constante apoyo y comprensión.

A las Familias Burgos, Guevara y Vallejo por la comprensión y apoyo en la recta final de este proyecto.

A las Familias Agudelo, Vélez y Aguirre por la comprensión y apoyo desde siempre, en especial en la recta final de este proyecto.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

AMENAZA INFORMÁTICA: la aparición de una situación potencial o actual donde un atacante o no tiene la posibilidad de generar una agresión informática hacía el territorio nacional o las entidades políticas y población de Colombia. (Min de Defensa de Colombia)[1].

ARM: arquitectura “liviana” y económica de procesamiento.

BOTNET: conjunto de ordenadores infectados y que combinan sus recursos informáticas para realizar o ejecutar tareas enviadas desde su centro de comando de forma remota (FireEye – 2014)[2].

BCP: busca sostener en niveles previamente definidos y aceptados, los procesos críticos del negocio a través de la estructuración de procedimientos e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre[3].

DOS (Denial of Service): servicio no disponible ya sea de carácter público o privado, afectando un proceso o aplicación informática [4].

CIBERSEGURIDAD: conjunto de mecanismos dispuestos para proteger o minimizar el riesgo del conjunto de sistemas de la entidad u organización, ante amenazas o incidentes de tipo cibernéticos [5].

DRP: Plan de recuperación de desastres.

E-COMMERCE: Comercio electrónico.

INFRAESTRUCTURA: conjunto de sistemas computacionales, datos, información, redes privadas o públicas, telecomunicaciones, cuya inhabilidad o interferencia en

---

1 Conpes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. p. 2. [Consultado: 23 diciembre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

2 Centro de estudios estrátegicos y Marítimos. SISTEMA DE SEGURIDAD NACIONAL. p. 14. [Consultado: 23 diciembre 2020]. Disponible en: https://www.esup.edu.pe/descargas/dep_investigacion/SISTEMA CIBERSEGURIDAD NACIONAL 2014.pdf

3 ESAP. PLAN DE CONTINUIDAD DEL NEGOCIO BCP. p. 6. [Consultado 22 diciembre 2020]. Disponible en: http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf

4 Red iris. DDoS: Un campo de batalla abierto en la seguridad de Internet. [Consultado: 23 diciembre 2020]. Disponible en: https://www.rediris.es/difusion/publicaciones/boletin/57/enfoque2.html

5 Conpes 3701. Op. Cit., p. 39.

su plena operación pueda impactar la salud pública, economía, seguridad nacional o la combinación de estas. (Resolución CRC 2258 de 2009).[6]

FRAMEWORK: conjunto de mecanismos, metodologías que facilitan la realización de tareas complejas de forma modular.

HARDENING: endurecimiento.

ISO 27001:2003: estándar de seguridad de la información en su versión más reciente 20013.

KUBERNETS: “Para ser breves, es una plataforma open source que automatiza las operaciones de los contenedores de Linux”[7].

MALWARE: “Se trata de un software malicioso: es decir, de un programa informático cuya finalidad es provocar un daño en un sistema”[8].

PHVA: “Planear, Hacer, Verificar, Actuar”.[9]

PTR: Plan de tratamiento de riesgos.

RANSOMWARE: es un código malicioso creado para secuestrar datos o información, el atacante cifra los datos para exigir un pago por la clave de cifrado [10].

SGSI: sistema de Gestión de Seguridad de la Información.

SOA: declaración de aplicabilidad.

VULNERABILIDAD: debilidad de un control o activo informático que puede ser explotada debido a una o múltiples amenazas del sistema. [UNE-ISO/IEC 27000:2014][11].

ZOMBIES: ordenadores infectados de manera remota con algún tipo de software que le permite a un tercero hacer uso del mismo ejecutando actividades ilícitas a través de la Red[12].

---

6 Ibid., p. 39.

7 Red Hat. ¿Qué es Kubernetes?. [Consultado 20 diciembre 2020]. Disponible en: https://www.redhat.com/es/topics/containers/what-is-kubernetes

8 Definición.de. DEFINICIÓN DE MALWARE. [Consultado 22 noviembre 2019]. Disponible en: https://definicion.de/malware/

9 Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. [Citado 16 diciembre 2020]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/

10 CCN-CERT. Glosario. [Consultado 12 octubre 2019]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=967.html

11 Ibid

12 Ibid

RESUMEN

El presente proyecto aplicado que busca plasmar un Framework o modelo a seguir que sea fácilmente repetible y escalable de un Sistema de Gestión de la Seguridad Informática – SGSI basados en la familia de normas ISO IEC 27001, soportado en una plataforma de código libre que corre bajo arquitectura ARM, facilitando la sincronización de información a las nubes y delegación permisos o gestión de roles en forma jerárquica, para el cumplimiento de los pilares de la Seguridad Informática: Disponibilidad, Integridad y Confidencialidad de la información.

La plataforma de Gestión Documental de código libre y bajo Arquitectura ARM (Advanced RISC Machine), cumplirá a cabalidad con los requisitos mínimos y dará valor agregado por sus características principales como son: sincronización de ficheros desde cualquier plataforma ya que su interfaz web le permite ser multi plataforma, adicionalmente facilitara el control y la gestión de permisos, al igual que cada acción o actividad realizada por un usuario deja una huella de auditoría, incluso si este comparte, descarga o borra información, su estructura tipo bosque brinda un potente motor de búsqueda documental que podríamos compararlo con el servicio de búsqueda de Google a nivel privado para las organizaciones que utilicen el Framework y lo mejor aún se utiliza mecanismos y técnicas de Hardening (Endurecimiento del sistema, Servicio, Aplicación, Hardware, etc) que reducen o mitiguen el riesgo de vulneración del sistema o su estructura, también contara con mecanismos del cifrado a la hora de mover, almacenar la información entre los usuarios, externos o hacia la nube, gracias a esta última, es también posible tener de primera mano el inicio de un sistema de recuperación de desastres DRP o un plan de continuidad del negocio BCP.

Palabras clave: Comercio Electrónico, Framework, ISO IEC 27001, Riesgos, Seguridad Informática, SGSI.

ABSTRACT

The present applied project that seeks to capture a Framework or model to be followed that is easily repeatable and scalable of an Information Security Management System - ISMS based on the ISO IEC 27001 family of standards, supported in an open source platform that It runs under ARM architecture, facilitating the synchronization of information to the clouds and delegation of permissions or management of roles in a hierarchical way, for compliance with the pillars of Information Security: Availability, Integrity and Confidentiality of the information.

The open source Document Management platform under ARM Architecture (Advanced RISC Machine), will fully comply with the minimum requirements and will give added value due to its main characteristics such as: file synchronization from any platform since its web interface allows it to be multi-platform, additionally it will facilitate the control and management of permissions, just as each action or activity carried out by a user leaves an audit trail, even if it shares, downloads or deletes information, its forest-like structure provides a powerful search engine documentary that we could compare it with the Google search service at a private level for organizations that use the Framework and the best thing is still using Hardening mechanisms and techniques (Hardening of the system, Service, Application, Hardware, etc.) that reduce or mitigate the risk of violation of the system or its structure, it will also have encryption mechanisms at the time of move, store information between users, external or to the cloud, thanks to the latter, it is also possible to have first-hand the start of a DRP disaster recovery system or a BCP business continuity plan.

Keywords: Computer security, Electronic Commerce, ISMS, ISO IEC 27001, Framework, Risks.

INTRODUCCIÓN

La seguridad informática de las organizaciones que utilizan recursos digitales sigue siendo un factor muy importante debido al sin número de ataques, malware e infecciones en la red que nacen día a día, según mi experiencia personal de 6 años en el mundo de la seguridad informática, esto es muy preocupante teniendo en cuenta lo que indica *PricewaterhouseCoopers. PwC* en su informe del año 2017, "Proyectamos que la economía mundial casi que doblará su tamaño para el 2042, creciendo a una tasa promedio anual cercana al 2,6% entre el 2016 y el 2050"[13].

Se constató que sitios de e-commerce o compra y venta de servicios o productos a utilizando medios informáticos, desde la Internet u otras redes privadas; estos deben controlar y proteger sus puertas informáticas, tales como: Servicios web, de almacenamiento, autenticación, pasarelas de pago, bases de datos y en general cualquier sistema que preste el comercio electrónico para entidades públicas, privadas o usuarios finales. Los servicios pueden o no estar publicados a la Internet. se pretende elaborar un framework como herramienta facilitadora en los procesos del SGSI como identificación de activos informáticos, riesgos, amenazas y vulnerabilidades, soportado por un sistema de Gestión Documental que corre bajo licenciamiento GPLv3 y arquitectura ARM, siendo estos de bajo coste adquisitivo. Sabemos que en Colombia todas las entidades públicas deben adoptar el MSPI Modelo de Seguridad y Privacidad de la Información, basados en la norma ISO IEC 27001:2013. El Min TIC en su Guía de gestión de riesgos, dicta: "Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC"[14].

El framework se vuelve indispensable para casi todo tipo de organizaciones como por ejemplo las que ofrezcan servicios de e-commerce, al facilitar gestión, control y sincronización entre las diferentes áreas de la organización como son: Proveedores y Recursos humanos, quienes son parte fundamental en la adopción y apropiación de los procesos asociados al SGSI. Una vez desplegado lograremos reducir los costos asociados de generación, actualización, mantenimiento y gestionar documentos que componen sus procesos; el bajo costo operativo, financiero al igual que facilitar la toma de decisiones ya sea que pretendan auditar el SGSI o certificarse en el mismo. Ayudará organizaciones aunando sus esfuerzos para desplegar, actualizar y mantener un SGSI al preocuparse únicamente de ejecutar el PDS y alineándose con la estrategia de negocios de la organización.

---

13 PWC. HAWKSWORTH JHON, AUDINO HANNAH.CLARRY ROB. El mundo en el 2050, Una mirada al futuro. ¿Cómo cambiará el orden económico mundial para el 2050?. 2017. p. 6. Disponible en: https://www.pwc.com/co/es/assets/document/el_mundo_en_2050.pdf

14 MIN TIC, Guía No 7. Guía de gestión de riesgos. Seguridad y Privacidad de la información. Bogotá 2016. p. 4. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Con el Framework del SGSI el lector podrá enfocarse en la adopción de las familias de la norma ISO 27000, permitiendo un enfoque temprano y de procesos ya que al detectar las amenazas que puede o no, aprovechar un delincuente informático u organizaciones dedicadas a lucrarse y enfocadas en materializar las vulnerabilidades que logran exponer los activos de la organización y causan un impacto económico debido a los riesgos no detectados o tratados en función de las actividades de negocio de la compañía más críticas como fase inicial del proceso de adopción temprana.

Los procesos anteriores giran en torno a la identificación del riesgo, con lo cual resulta sencillo enfocar los esfuerzos en realizar requerimientos de seguridad informática a las diferentes áreas de la compañía, en especial al talento humano y al departamento de las TICs, previamente autorizados por la gerencia o el comité designado para tal, el siguiente paso consiste en definir e imponer los controles diseñados en aras de lograr reducir esos riesgos materializados o no y por ende logrando de forma “involuntaria” que las Amenazas más críticas y principalmente las que afecten el CORE de la organización y que puedan detener su sistema productivo o facturación se reduzcan y mitiguen.

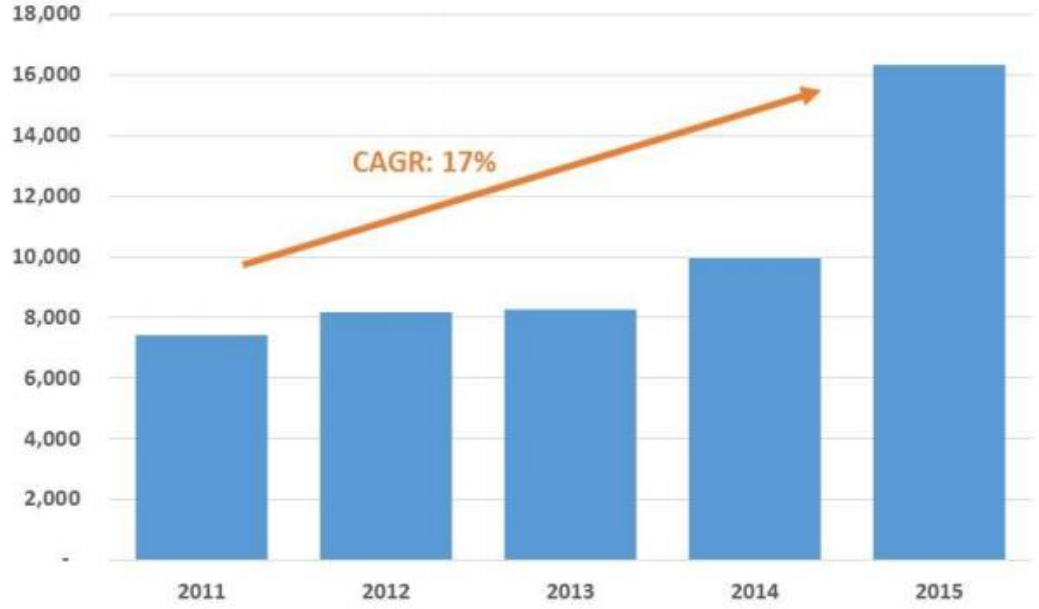
Uno de los referentes en cuanto a Framework de un SGSI es ISO Tools, si bien gran parte del material como plantillas, formatos, etc, es de carácter público existen costos sustancialmente grandes como el de la consultoría y todo lo que conlleva el trazado de una ruta a seguir, así como la resolución de posibles dudas o conflictos al interior de la organización, al plantear las mejores opciones de resolución u adopción de la ISO IEC 27000 y sus familias de normas, esto es muy bueno por que servirá como referente y base para establecer un marco genérico enfocado a solventar el planteamiento de los requisitos mínimos de la fase uno (1) de SGSI, se pretende llegar a ser un referente de la aplicabilidad y facilidad en la adopción del estándar a nivel local en las organizaciones, también se espera que sea un medio para alcanzar, mantener y mejorar el SGSI.

1. DEFINICIÓN DEL PROBLEMA

La creciente demanda y uso de las tecnologías de la información gracias a la democratización de la Internet ha permitido que las empresas abran sus vitrinas al mundo para ofrecer sus productos o servicios, volviéndose imperativo el poder ofrecer transacciones electrónicas (pagos o compras) e intercambio de productos o servicios "en línea".

En la figura 1 la SIC presenta su análisis para el Comercio Electrónico en Colombia y su crecimiento durante 2011 a 2015. "De acuerdo con los resultados del primer y del segundo estudio contratado por la CCCE a PwC y del tercer estudio contratado a KPMG, las ventas de comercio electrónico en Colombia ascendieron a US$8.283 millones en 2013 y a US$9.961 millones en 2014, con un crecimiento del 20%. Para el 2015 las ventas ascendieron a US$16.329 millones, con un incremento de 64% frente al 2014. Lo anterior representa el 2.19% del Producto Interno Bruto - PIB para 2013, 2.62% del PIB para 2014 y 4.08% para 2015. Para este último año, 56% de las transacciones se originaron en tarjetas de crédito y 44% en tarjetas débito"[15].

Figura 1: Comercio Electrónico en Colombia, Comportamiento en cifras de millones de Dólares entre 2011–2015.



Fuente: Los años 2011 y 2012 se basan en: Superintendencia de Industria y Comercio. Los años 2013, 2014 y 2015 se basan en el Primer, Segundo y Tercer Estudio de comercio electrónico en Colombia. Disponible en: https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf

[15] SIC. El Comercio Electrónico en COLOMBIA. Análisis Integral y Perspectiva Regulatoria. Bogotá 2017. p. 33. Disponible en: https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf

1.1 PLANTEAMIENTO DEL PROBLEMA

Los comercios electrónicos tienen la base fundamental y componente principal un servicio web, tal y como lo establece el código de comercio de Colombia en su artículo 86. La página web o sitio de Internet hace parte del establecimiento de comercio[16], resultando fundamental su protección y resguardo en términos de ciberseguridad, sabemos que un sitio web tiene componentes tecnológicos que pueden estar operando en sitio (instalaciones de la entidad) o en la nube informática pública o privada, generalmente se obvian los testeos o pruebas de vulneración a los sistemas tecnológicos o servicios web estáticos o dinámicos, para evitar la indisponibilidad del servicio web de cara a sus consumidores y dejando posibles brechas de seguridad sin identificar.

De tal manera que la creciente demanda de las organizaciones y usuarios por utilizar plataforma de transacciones comerciales o financieras a través de portales web y las políticas del gobierno nacional de Colombia y por garantizar que las entidades prestadoras de este tipo de servicio tengan los mecanismos mínimos de seguridad en su infraestructura, dejan entre ver la necesidad de facilitar el proceso de adopción de la familia de normas de la ISO 27001 en su actual versión 2013, está enfocada en garantizar la mejora continua de la seguridad informática en las organizaciones que la adopten.

Este trabajo se llevará a cabo en la ciudad Santiago de Cali, Valle del Cauca, Colombia, No existe un framework que ayude a las organizaciones que están obligadas a dar cumplimiento a la legislación exigida por el gobierno y liderada por el Ministerio de las TIC, para llevar resolver la problemática planteada utilizaremos un sistema de gestión documental bajo arquitectura ARM y de código libre que sincronizara a una nube garantizando el respaldo de la información reutilizable y cambiante de un SGSI. Utilizaremos diferentes tipos de software libre con parámetros de configuración a la medida que optimizan el recurso tecnológico de tipo físico y agreguen varias capas de seguridad, robusteciendo Framework de Gestión Documental del Sistema de Gestión de Seguridad de la Información o FGD-SGSI.

Las entidades continúan generando datos día tras día, de carácter público y privado. La información se mantiene como activo primordial en las entidades (Piattini & Del Peso, 2001), siempre y cuando sea precisa, este actualizada y completa, resulta de vital importancia en la toma de decisiones. La relevancia de la información es fundamentada en la teoría de las entidades u organizaciones, siendo un sistema

---

[16] MORENO GÓMEZ, G. A. (2017). El Estatuto Del Consumidor Como Forma De Corregir La Asimetría De La Información en La Adquisición De Productos O Servicios en Páginas Web en Colombia. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 17, 1–35. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=126901313&lang=es&site=eds-live&scope=site

construido por materiales, recursos, información o personas; donde existe una aceptación sobre el concepto de información y sus estrechos vínculos "el 'orden y el caos' entre los individuos, los recursos y en la interrelación personas-recursos" (Aja, 2002); de tal forma que, debemos considerar a las entidades como sistemas de información[17], que necesitan ser gestionados, controlados, actualizados y asegurados periódicamente.

Aun así, estos sistemas cada vez que se utilizan; almacenan, modifican, generan o consultan información, dejan en entrever la integridad los datos; riesgos, que pueden llegar del exterior o incluso del interior de la entidad (INTECO, 2010). El phishing, virus, ingenieros sociales o gusanos entre otros son amenazas latentes y constantes que podrán atentar contra integridad o disponibilidad de la información (Susanto et al, 2011a). Un Delincuente informático, puede causar pérdidas considerables en una entidad, tales como, espiar y comercializar la estrategia de negocio, robo de datos de proveedores o clientes (Susanto et al, 2011b)[18]. Las implicaciones anteriores hacen notar la necesidad de las organizaciones en la adopción control y regulaciones aplicables a los activos de la información que posean.

La súper intendencia financiera en su circular externa 007 de 2018, delimita que las organizaciones deben incluir en su plan de continuidad del negocio, el mecanismo de recuperación, respuesta y que la operación debe continuar en modo contingencia, así la restauración de sus sistemas tome su tiempo, a causa de una posible materialización de un ataque informático.[19] Que pueda materializarse o no, aún sin importar si este pudiera catalogarse como catastrófico en términos de vulneración a los sistemas o afectación de la privacidad de los datos e información de carácter privado.

Toda organización que quiera prestar los servicios de E-commerce para sus clientes debe aplicar las mejores políticas de seguridad de la información a sus activos informáticos, ejecutando los procesos que conlleva de la mano de recursos humanos, en pro de garantizar un marco adecuado y seguro en las transacciones, dado lo anterior y por conveniencia en cuanto a posicionamiento en el mercado y niveles de seguridad altos, resulta imprescindible y debe ser parte del horizonte alcanzable de estas compañías la implantación de un Sistema de Gestión de Seguridad de la Información - SGSI.

---

17 Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información Tecnológica, 26(2)*, 129–134. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=108732548&lang=es&site=eds-live&scope=site

18 Ibid

19 Super Intendencia Financiera de Colombia, Circular Externa 007 de 2018, Bogotá. Disponible en línea: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc

Es importante resaltar que las pasarelas o administradoras de pago, por el momento son entidades no vigiladas o supervisadas por la Superintendencia Financiera de Colombia aun así prestan sus servicios en la aplicación del comercio electrónico para procesando, almacenando y/o transmitiendo el pago correspondiente a operaciones de venta en línea[20]. Sin embargo, las entidades que decidan conectar su sitio web con una pasarela de pago deben cumplir con mecanismos mínimos pero avanzados en términos de ciberseguridad, siendo el SGSI el sinónimo que buscaran.

Como lo indica (Velasco 2008). El crecimiento del comercio electrónico está determinado por la cantidad de consumidores, de tal manera que para conseguir la confianza de éste es necesario primar por sus derechos, y concientizar a entidades o personas naturales que comercializan bienes y servicios a través de la red de redes, teniendo éstos obligaciones y deberes para con los consumidores[21]. Siendo importante para cada entidad y más aún generar confianza para sus consumidores es imperativo mejorar la seguridad de la información aplicando las mejores prácticas normativas.

En (figura 2). La RUES indicó las cantidades de Unidades productivas o empresas, asociaciones registradas en Colombia para el año 2017, fueron creadas en el país 323.265 unidades productivas; 253.243 personas naturales y 70.022 sociedades, con un crecimiento del 7,3% en el total entidades creadas con respecto al año inmediatamente anterior[22].

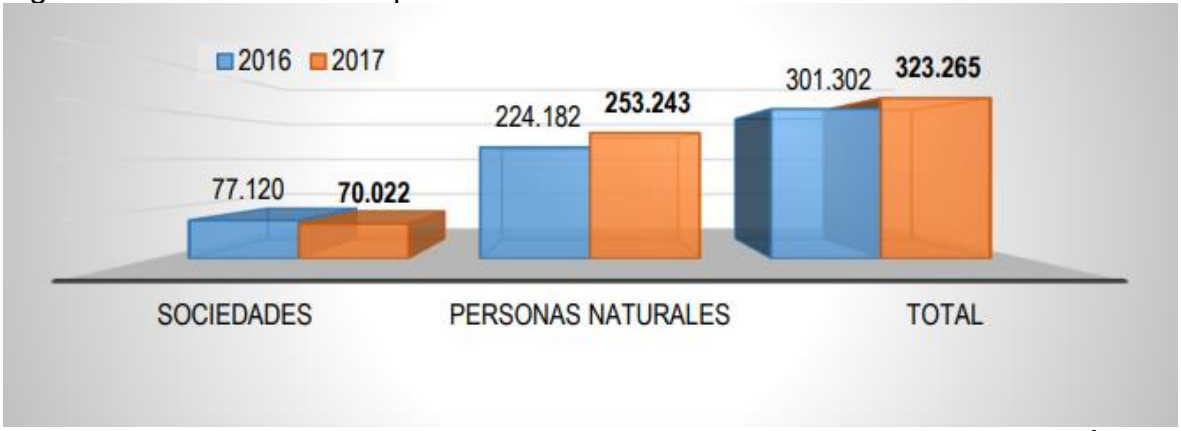
---

[20] Super Intendencia Financiera de Colombia, Circular Externa 008 de 2018, Bogotá. Disponible en línea: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031742/ce008_18.doc

[21] Velasco Melo, A. H. (2008). El Derecho Informático Y La Gestión De La Seguridad De La Información Una Perspectiva Con Base en La Norma Iso 27001. Revista de Derecho, P. 29, 333–366. Disponible en línea: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=34969402&lang=es&site=eds-live&scope=site

[22] Confecámaras. INFORME DE DINÁMICA EMPRESARIAL EN COLOMBIA. Bogotá.2017. p. 2. Disponible en línea: https://incp.org.co/Site/publicaciones/info/archivos/Informe-de-Dinamica-Empresarial-2017-17012018.pdf

Figura 2 Total de unidades productivas creadas 2017/16



Fuente: RUES – Registro único Empresarial y Social. INFORME DE DINÁMICA EMPRESARIAL EN COLOMBIA. Bogotá.2017. p. 2. Disponible en línea: https://incp.org.co/Site/publicaciones/info/archivos/Informe-de-Dinamica-Empresarial-2017-17012018.pdf

Si comparamos la cantidad de sociedades o empresas registradas al año 2017 (ver figura 2) vs la cantidad de compañías certificadas al mismo año 2017 en la norma ISO/IEC 27001:2013 (ver figura 8) obtenemos una tasa inferior al 1% de sociedades o empresas que cuentan está certificación y tienen implantado el SGSI; estas consideraciones fundamentan mi propuesta de proyecto aplicado para la Implementación de un sistema de Gestión de Seguridad de la información ISO 27001:2013 soportado en software de gestión documental con licenciamiento GPLv3 o Framework de Gestión Documental del Sistema de Gestión de Seguridad de la Información – FGD-SGSI, utilizando arquitectura ARM o liviana en pro de la democratización de una solución que almacene, gestione, garantice y controle los datos generados por el SGSI, los datos estarán en continua actualización. El desarrollo de este proyecto se hace en el Valle del Cauca - Colombia y quizá en un futuro no muy lejano sea a nivel nacional e incluso de talla mundial a futuro más lejano.

Este proyecto es un esquema base y modular para la creación de un framework que facilite la implantación de un Sistema de Gestión de Seguridad de la Información – SGSI de la mano de la Norma ISO IEC 27001:2013, en Colombia únicamente son 148 las Compañías o Sociedades certificadas en el estándar internacional para el año 2017, a nivel de latino américa son 620 compañías: (ver Figura 8).

La Comisión de Regulación de Comunicaciones – CRC, recalca que “Es función del Estado intervenir en el sector de las TIC, para promover condiciones de seguridad del servicio al usuario final”.[23] Teniendo y girando en torno a los datos procesados

[23] Comisión de Regulación de Comunicaciones, República de Colombia. 2015. p 77.) [Consultado 12 septiembre 2020]. Disponible en:

pretendemos utilizar el framework del SGSI y su Gestión documental donde reposaran dichos datos como una herramienta útil para las entidades a la hora de gestionar la información que genere el e-commerce de los usuarios finales que consuman servicios digitales ya sean entidades legalmente conformadas o individuos que consuman servicios de comercio electrónico en el territorio nacional de Colombia.

https://www.crcom.gov.co/recursos_user/Documentos_CRC_2015/Actividades_regulatorias/Ciberseguridad/Doc_Ciberseguridad28_07_15.pdf

1.2 FORMULACIÓN DEL PROBLEMA

¿Es posible mejorar la seguridad informática de las entidades en Colombia que utilicen la Internet mediante un framework, sistema o modelo de gestión documental y que sea fácilmente repetible o escalable para el SGSI de la norma ISO IEC 27001:2013 utilizando software y hardware libres, cumpliendo con apartados de ciberseguridad en la normatividad colombiana?.

1.3 ALCANCE Y LIMITACIONES

1.3.1 Alcance

El presente proyecto se ubica entre los proyectos de gestión de seguridad informática y lo que pretende es presentar información recolectada de diversas fuentes bibliográficas académicas, institucionales, artículos digitales y mi experiencia propia a la hora de desplegar el sistema de gestión documental donde reposara toda la información concerniente al SGSI de la norma ISO IEC 27001:2013.

Desplegar la plataforma o framework de gestión documental que gira en torno al marco del SGSI, su utilización resulta una tarea ardua para los líderes de los procesos y quienes deben estar en constante actualización, modificación y/o mejora de plantillas, formatos, lineamientos, políticas de seguridad de la información, así como sus objetivos de control, auditorías internas, mitigación e identificación de riesgos o amenazas a las que está expuesta la organización y sus procesos de negocio; estos documentos deben reposar en un lugar seguro, que facilite el acceso controlado y deje registro detallado de la interacción de los usuarios o líderes que en algún momento deban utilizarlos, lo anterior garantizando el No repudio, confidencialidad, integridad y disponibilidad de la información.

1.3.2 Limitaciones

Es conveniente resaltar que el desarrollo del proyecto no abarcara temáticas como las presentadas en el siguiente listado:

- La información presentada del framework es de carácter exploratoria y teórica en su gran mayoría, pretendemos entregar las bases para utilizar la plataforma de gestión documental sobre software y hardware libres.
- Creación de documentos detallados del paso a paso del proceso de despliegue, donde se evidencien las salidas de cada comando ejecutado, sin embargo, se darán los pasos o comandos mínimos para dejar operativa la plataforma de gestión documental.
- Creación de plantillas o formatos específicos para el SGSI.

- Realizar auditoría o presentar información asociada a sus resultados.
- Detallar paso a paso los procedimientos realizados a nivel de configuración.
- Detallar los procedimientos de Hardening recomendados y aplicados en el Framework.
- Detallar los procedimientos de Debug realizados, hasta dejar operativa la plataforma.
- Proceso de creación de Roles y Usuarios.
- Pruebas de estrés o carga del sistema.
- Publicación del framework a la Internet o al público en general.
- Entregar copia de archivos de configuración una vez opere la base del Framework.
- El documento final se considera o deberá ser de Carácter privado y no público.
- El documento y su contenido son propiedad del autor.
- Procedimientos de auditorías internas o externas.
- Registro detallado de la interacción de los usuarios.
- Publicación de amenazas.

1.4 JUSTIFICACIÓN

En Colombia sería de gran ayuda contar con un software que permita contribuir al control y gestión de los documentos generados durante y después del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). La solución debe recibir, almacenar, administrar y organizar los documentos generados en todo momento por las actividades de implantación o mejora continua del SGSI.

Soportar dicho software requiere de un diseño o modelo que define o implementa acciones de gestión como requisito para la revisión, actualización, aprobación, fases y accesos a los documentos antes y durante todo el ciclo de vida del SGSI.

Lo anterior, produjo como resultado un módulo para gestión documental que permite el control de documentos[24]. Y los roles, permisos, accesos, modificaciones o huella de auditoría dejada en cada interacción o acceso de los usuarios del sistema al framework.

Tal como lo indica (Gómez, 2019). "El e-commerce o comercio electrónico tiene en su proceso cinco fases interrelacionadas y una fase transversal a las actividades realizadas a lo largo de toda la cadena: (i) Acceso al portal de compra, (ii) Compra en línea, (iii) Gestión del pago, (iv) Logística de entrega, (v) Postventa y (vi) Fase transversal- uso de las TIC"[25]. Se constató que el comercio electrónico a nivel mundial se aceleró a causa de la pandemia global, lo que nos lleva a la clara necesidad de aportar a las entidades mecanismos que permitan mejorar continuamente su seguridad informática.

Al igual que la infraestructura adyacente que soportan los servicios tecnológicos de la entidad prestos en atender las necesidades de los usuarios en el uso de sus servicios digitales.

Teniendo en cuenta el gran auge y crecimiento continuo de servicios tecnológicos que deben prestar las organizaciones en casi cualquier ámbito (Salud, Gobierno, Financiero, Alimentos, Hotelería, Software, Telecomunicaciones, entre otras) a sus clientes internos o externos y los lineamientos mínimos exigidos por el Gobierno Local, Superintendencia Financiera, Mercados Internos o Externos que van de la mano de los lineamientos apoyados y promovidos por Ministerio de las tecnologías de la información y las comunicaciones de Colombia- (Tic).

---

[24] Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129–134. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=108732548&lang=es&site=eds-live&scope=site

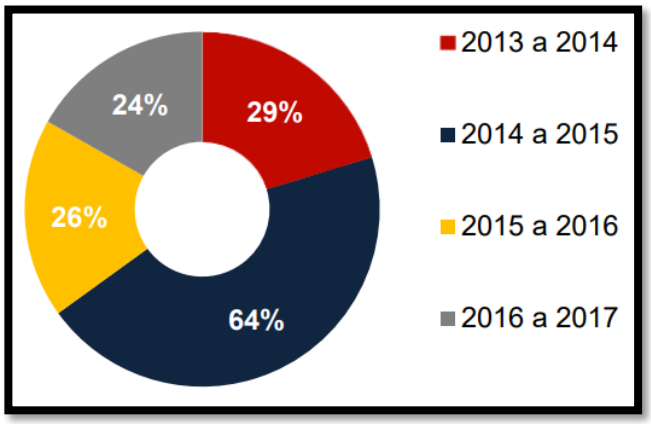
[25] GÓMEZ CASTRO SANTIAGO. E-Commerce, crecimiento y ecosistema digital en Colombia. Edición 1213. Bogotá 2019. p. 1. Disponible en: https://www.asobancaria.com/wp-content/uploads/1213.pdf

Principalmente a la hora de ofrecer transacciones o intercambios con los múltiples sistemas financieros, pasarelas de pago, conexiones a entidades bancarias, criptomonedas y en general el comercio electrónico, hace ver la necesidad de implantar controles, objetivos, mejora continua, gestión de la seguridad informática, de tal forma que deben estar alineados con la metodología de la norma internacional ISO 27000 y sus familias de estándares en las organizaciones al igual que con las metodologías de gestión informáticas y sus riesgos, especialmente MAGERIT.

Desde el punto de vista del control jerárquico de documentos, cada organización podrá tener una capa de seguridad adicional o reforzada que permita identificar que ha sucedido con cada documento o archivo sincronizado en el sistema.

En la (figura 3) se pude observar que Colombia hace parte de esta nueva tendencia mundial por tal razón se ha pronunciado un crecimiento exponencial del comercio electrónico en el país. Las cifras muestran un crecimiento de 24% en los últimos 65 años, lo que permite prever que para finales del 2021 el país alcanzará ventas superiores a los $26.073 dólares, expresados en millones"[26].

Figura 3. Crecimiento del Comercio Electrónico en Colombia



Fuente: Asobancaria. Reporte de industria: El E-Commerce en Colombia 2018/2019. Disponible en línea: https://www.asobancaria.com/wp-content/uploads/1213.pdf

Para la entidades que tengan comercio electrónico, el tener un SGSI les permitirá tener una posición adecuada y diferenciadora en el mercado frente a sus competidores, desde los ámbitos de la seguridad informática hemos visto la gran cantidad y variedad de ataques informáticos, pasando por el Ransomware, malware, phishing, explotación de servicios basados en web, aplicaciones móviles, la nube privada o pública, el Internet de las Cosas (IoT) e incluso el escritorio remoto.

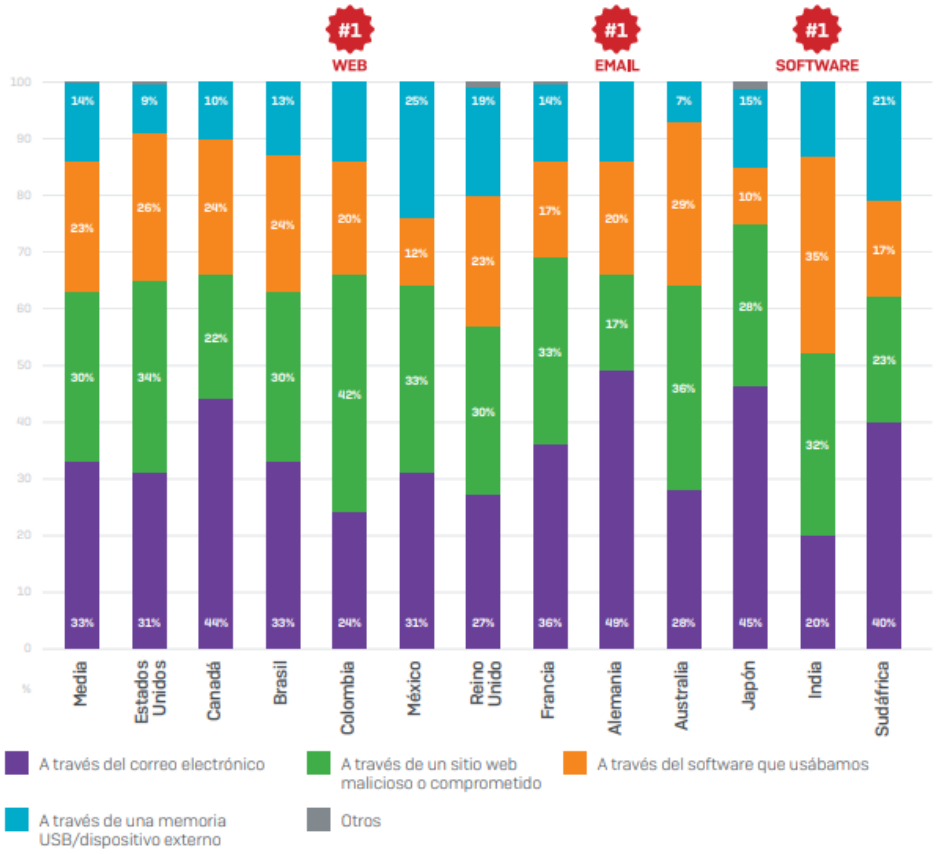
---

[26] GÓMEZ CASTRO SANTIAGO. E-Commerce, crecimiento y ecosistema digital en Colombia. Edición 1213. Bogotá 2019. p. 1. Disponible en línea: https://www.asobancaria.com/wp-content/uploads/1213.pdf

EL SGSI, exige a las entidades tener mejores controles iniciando desde el mismo conocimiento e inventariado de los dispositivos de red y servicios que ofrecen al público en general, en la Intranet o los que son compartidos con otras entidades (terceros).

Se evidenciaron las cifras entregadas por El fabricante SOPHOS, quien realizó una encuesta independiente a 1685 compañías y 3100 directores de TI en 12 países y lo público en su informe del 2019: El rompecabezas imposible de la ciberseguridad. "Los encuestados cuyas empresas habían sido víctimas de un ciberataque revelaron que habían sufrido una amplia gama de ataques durante el último año" (Ver figura 4)[27]. En Colombia la mayoría de los ataques informáticos utilizaron sitios web maliciosos o comprometidos y en segundo lugar usaron el correo electrónico.

Figura 4: Los ataques proceden de múltiples direcciones



Fuente: SOPHOS Ltd. El rompecabezas imposible de la ciberseguridad. Reino Unido 2019. P. 8, Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

---

27 SOPHOS Ltd. El rompecabezas imposible de la ciberseguridad. Reino Unido 2019. p. 8. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

SS360 S.A.S. desplego el Framework de Gestión documental del SGSI, en la infraestructura de un par de sus clientes activos, garantizando que se cumplan los tres pilares de la seguridad informática: Disponibilidad, Integridad y Confidencialidad, al igual que el No repudio, buscando reducir el impacto que puedan causar los delincuentes informáticos sobre los activos informáticos de las entidades o sobre su información; en el framework reposaran los datos del SGSI, como lo por ejemplo controles de seguridad, políticas de la información, procesos y directrices de la alta gerencia que garantizaran la correcta adopción e implantación del SGSI en la organización ya sé que tenga e-commerce funcionando, o se estén preparando para su despliegue a futuro.

Otra tendencia importante en el comercio electrónico es el incremento en uso de los smartphones. Según cifras la plataforma Mercado Libre, indica que el 70% de las personas en Colombia utilizan sus teléfonos para navegar en su plataforma (figura 5).

Figura 5: Tipo de dispositivo usado para la compra

Fuente: Asobancaria. Medición de indicadores de consumo del Observatorio de E-Commerce. Disponible en línea: https://www.asobancaria.com/wp-content/uploads/1213.pdf

El acelerado desarrollo de apps y portales web pone a disposición de los consumidores colombianos la posibilidad de realizar compras de sus productos a través de las diversas plataformas digitales, teniendo en cuenta que, actualmente, los smartphones son elementos electrónicos de uso cotidiano en los hogares de la nación. De acuerdo con Nielsen, el 76% de los colombianos tiene un teléfono móvil inteligente, esto los ubica en la cima de dispositivos predilectos posterior a ellos se encuentran las computadores, Tablet o televisores inteligentes.[28]

[28] GÓMEZ CASTRO SANTIAGO. E-Commerce, crecimiento y ecosistema digital en Colombia. Edición 1213. Bogotá 2019. p. 1. Disponible en línea: https://www.asobancaria.com/wp-content/uploads/1213.pdf

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Elaborar un Framework que sea fácilmente repetible y escalable bajo arquitectura ARM y Software GPLv3 con sincronización a la nube, para apoyar el diseño de un Sistema de Gestión de la Seguridad Información en la norma ISO/IEC 27001, en la empresa Seguridad Sincronizada 360 (SS360).

2.2 OBJETIVOS ESPECÍFICOS

- Establecer requisitos mínimos con base en el Sistema de Gestión de la Seguridad Información – SGSI en la norma ISO/IEC 27001, que permita el diseño de un framework bajo arquitectura ARM y software GPLV3 con sincronización a la nube.
- Diseñar el Framework bajo la arquitectura ARM y Software GPLv3 con sincronización a la nube, en la empresa Seguridad Sincronizada 360 (SS360).
- Formular un plan de mejora continua que permita concientizar al personal de la empresa Seguridad Sincronizada 360 (SS360) en las buenas prácticas de seguridad de la información.

3. MARCO DE REFERENCIA

3.1 MARCO TEÓRICO

La seguridad informática la podemos definir, como la preservación de la integridad, la disponibilidad y confidencialidad, de los sistemas de información[29], la data creada, los activos informáticos, los servidores y la infraestructura subyacente son parte integral de los objetivos de protección en el marco de la seguridad informática.

Dependiendo del entorno de la entidad, se pueden presentar diferentes amenazas que pueden comprometer los activos informáticos de las entidades, la entidad tiene tres alternativas: transferir el riesgo, aceptar el riesgo o hacer algo que permita disminuir la posibilidad de materialización del riesgo.

A los mecanismos o salvaguardas empleados para disminuir un riesgo se les denomina controles de seguridad[30]. Siendo el proceso de mejora continua y constante empoderamiento, una carga extra y demandante participación de todos y cada uno de los colaboradores de la organización, en pro de buscar, mantener, preservar los pilares de la seguridad informática entre otros lineamientos organizacionales.

Los controles que se determinen deben estar integrados y articulados para que cumplan con la efectividad esperada[31]. Todos y cada uno de controles serán alineados a los objetivos trazados en la entidad, durante la fase de arquitectura y diseño de la seguridad informática, y como parte de las actividades de análisis de riesgos en la entidad, por lo cual se comprenden los siguientes pasos:

- Definir o identificar los activos informáticos de la entidad a analizar.
- Identificar las amenazas que puedan comprometer la seguridad de los activos informáticos; Determinar la probabilidad de materialización de amenazas cibernéticas.
- Determinar el nivel de afectación de las amenazas informáticas, que permitan establecer y priorizar dichas amenazas.

---

29 TIPTON, 2006 Harold F. Tipton, Micki Krause (eds.), Information Security Management Handbook, 5th Ed., CRC Press, 2006. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=115870&lang=es&site=eds-live&scope=site

30 Michael E. Whitman, & Herbert J. Mattord. (2017). Principles of Information Security, Edition 6. Cengage Learning. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=2639438&lang=es&site=eds-live&scope=site

31 Information security architecture; an integrated approach to security in the organization, 2d ed. (2006). SciTech Book News. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.142887097&lang=es&site=eds-live&scope=site

- Recomendar controles pueden disminuir la probabilidad de ocurrencias de los riesgos.
- Documentar en todo momento el proceso.

Sabemos que la dependencia actual y futura de las entidades en las Tecnologías de la Información (TI) es cada vez más sobresaliente a causa del modelo te economía actual que se basa en la continua generación o reinvención de conocimientos,[32] el uso de las tecnologías de la información y comunicación consiste en transmitir, administra y desarrollar activos de carácter intangible, es decir la información y el conocimiento, ellos son fundamentales para las estrategias corporativas y de negocio, así como los usuarios, clientes, empleados, colaboradores y demás personas o entidades que tengan acceso, manipulación o creación de datos deben poder acceder o denegársele, en primer medida el acceso a la información en caso tener su debida autorización o prohibirla en caso contrario.

Acorde al principio de confidencialidad: "Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la ley 1266 y en los términos de la misma"[33].

Este proyecto y la Arquitectura planteada fue diseñada para a ser beneficiosa desde las perspectivas costo-efectiva y robustez de la seguridad informática y en función del uso para la seguridad de la información, al utilizar en su totalidad código fuente de uso libre, parametrizado con las mejores prácticas de infraestructura informática y de los servicios de telecomunicaciones que reposaran en hardware tipo ARM: Es conocida como arquitectura RISC (Ordenador con Conjunto Reducido de Instrucciones), opera en 32 bits y 64 bits (requiere V8-A), es de bajo consumo de energía eléctrica, también llamada tecnología verde.

También utilizaremos las llamadas redes de computadoras o sistemas informáticos que están conectados en sí de manera física, inalámbrica y lógica con la finalidad compartir información en paquetes de datos y/o transmitirlos mediante impulsos eléctricos, radio frecuencia o haces de luz; Particularmente la redes cableadas serán de gran utilidad a la hora de implantar el hardware y garantizar la

---

[32] PETERSON, R. Integration Strategies and Tactics for Information Technology Governance. En W. VAN GREMBERGEN, Strategies for Information Technology Governance (p. 37-80). IDEA Group Publishing. 2004. p. 3. Disponible en línea: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=87306&lang=es&site=eds-live&scope=site

[33] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

comunicación hacia “las Nubes” al tener los datos de la organización en el sistema de gestión documental, estos datos podrán ser sincronizados a la “nube” finalizando ese proceso podemos decir que tenemos un DRP o Plan de Recuperación de Desastres aceptable faltándole su componente de forma o el conjunto de procedimientos a ejecutar de manera secuencial para reactivar lo más pronto posible la operación de misión crítica para una organización, en este caso todo el SGSI y sus documentos, así como los datos más críticos de la entidad pueden ser accedidos o restaurados ante cualquier eventualidad, en el caso de los servicios sobre la internet encontramos principalmente los tipo web, sitios o aplicaciones.

El sector económico y las empresas Colombianas una vez se formalizan están obligadas a crear un Registro Mercantil, el cual dicta que toda compañía que cumpla con la condición de ser de origen colombiano y que desarrollar directamente su actividad, comercial, económica, financiera o prestación de servicios a través de su sitio web,[34] está en la obligación de registrar la página web en su Cámara de Comercio, partiendo del punto que las empresas constantemente generan información, datos, ficheros que necesitan ser controlados y debe ser medible el uso que le den sus funcionarios internamente o lo que se publique a la Internet para los usuarios en general o los clientes de las empresas.

Y así generaran más tracción comercial al destacarse frente a sus competidores directos, o indirectos, puesto que han aplicado una guía de buenas prácticas sobre seguridad informática y en la guía están contenidas las recomendaciones para el tratamiento de la data en toda la “cadena de custodia”, cada acción o movimiento sobre un dato informático o un sistema, debe dejar un registro de auditoría, aún sin que dicha acción sea un delito informático es importante poder tener huellas de auditoría a la mano apoyándose el principio de No Irrefutabilidad.

En este caso la normatividad ISO IEC 27001, es la encargada de dictar los lineamientos para la implementación de los procesos que ayudan a que una organización ejecute servicios o productos de forma confiable, en términos de ciberseguridad y acorde a las especificaciones internacionales

Utilizaremos el conjunto de estándares definidos y/o en fase de mejora continua por la ISO (Organización Internacional de Estándares) y la IEC (Comisión Internacional Electrotécnica), ISO IEC 27001, actualmente su versión oficial es la 2013, el estándar propone un marco de gestión de la seguridad de la información usable por cualquier tipo de entidad, sin importar si está es catalogada como grande, pequeña, de carácter privado o sin ánimo de lucro e incluso si es de tipo estatal, será necesario contemplar de manera genérica para lograr la administración del riesgo

---

[34] MORENO GÓMEZ, G. A. (2017). El Estatuto Del Consumidor Como Forma De Corregir La Asimetría De La Información en La Adquisición De Productos O Servicios en Páginas Web en Colombia. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 17, 1–35. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=126901313&lang=es&site=eds-live&scope=site

como parte fundamental de los lineamientos de la normatividad ISO 27001, teniendo en cuenta los siguientes parámetros del SGSI y MAGERIT:

El **SGSI** requiere el uso de al menos una metodología de gestión e identificación de riesgos, se pretende usar una combinación genérica que permitirá ajustarse a cualquier organización y su aplicación de manera modular o por fases de manera sistemática.

Siendo **Magerit**: una de las metodologías más aceptadas por la comunidad y utilizadas cuando se requiere hacer gestión de riesgos, cuenta con un alcance bastante robusto, tanto en el análisis como en la gestión de los riesgos, de igual manera que permite realizar un análisis de amenazas en los activos informáticos ya sea de tipo cualitativo o cuantitativo, es muy reconocida a nivel mundial.

Magerit permite realizar el análisis de riesgos Informáticos como conjunto de procesos metodológicos para determinar el riesgo al que está expuesta la organización y sus activos de información, Magerit se encarga de establecer procedimientos estandarizados, tales como:

- Identificar cuáles son los activos más importantes, como se correlacionan y cuál es su valor monetario.
- Determinar cuáles amenazas son más factibles de materializarse en los activos de información.
- Estimar el impacto o daño que puedan afectar a los activos por nivel de criticidad.
- Estimar cual es el riesgo, ponderado de acuerdo con la probabilidad de que se materialice una o varias amenaza.

La administración del riesgo ayuda a mitigar el riesgo identificado, al aplicar las medidas necesarias y recomendadas de seguridad informática, enfocándose en.

- Amenazas.
- Vulnerabilidades.
- La cuantificación monetaria de los activos de información catalogados.

Con la identificación del riesgo se logra:

- Conocer los riesgos.
- Evaluar los posibles daños y su cuantificación.
- Justificación para la autorización y despliegue de las medidas recomendadas de seguridad de la información a proponer.
- Mitigar, eliminar o transferir las vulnerabilidades identificadas.

Posterior a la identificación del riesgo, acentuamos objetivos de análisis sobre los activos informáticos y su riesgo.

- Discernir cual es el impacto al materializarse las amenazas por nivel de criticidad e importancia para la organización.
- Establecer y estimar el valor o costo monetario en caso de pérdidas económicas en el negocio debido a que se manifestó un riesgo latente o no.
- Identificar y catalogar los riesgos.
- El valor intrínseco que ayuda justificar el despliegue de seguridad y control.

Las características típicas para tener en cuenta durante el análisis de riesgos son.

- Considerar cual es el costo y nivel de afectación de los activos informáticos, teniendo en cuenta el impacto que cause la pérdida, modificación o secuestro de la información.
- Entregar un mecanismo que facilita la comparación de las vulnerabilidades de forma separara y catalogada.
- Crear requerimientos de seguridad informática a implementar.
- Evaluar
- Cuáles son las amenazas latentes, al igual que vulnerabilidades identificadas.

El análisis de riesgos como parte de una metodología utilizada en el framework es una herramienta que nos entrega una arquitectura que logra reducir el nivel del riesgo latente y permite entender las vulnerabilidades asociadas a los activos de la información en una entidad.

Gestión de riesgo: Cada vez que se identifique un riesgo se puede optar por:

- "Aceptarlo.
- Transferirlo.
- Mitigarlo, con la implementación de políticas de seguridad.
- Evitarlo"[35].

[35] Sarria Cuellar, M. (2015). Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londo?o mediante la norma ISO/IEC 27001:2013. [Consultado 20 mayo 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ir00913a&AN=unad.10596.3631&lang=es&site=eds-live&scope=site

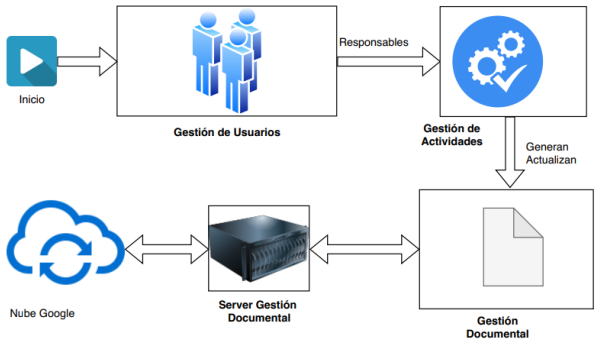
3.2 MARCO CONCEPTUAL

Uno de los referentes en cuanto a Framework de un SGSI es ISO Tools, si bien gran parte del material como plantillas, formatos, etc, es de carácter público existen costos sustancialmente grandes como el de la consultoría y todo lo que conlleva el trazado de una ruta a seguir, así como la resolución de posibles dudas o conflictos al interior de la organización, al plantear las mejores opciones de resolución u adopción de la ISO IEC 27000 y sus familias de normas, esto es muy bueno por que servirá como referente y base para establecer un marco genérico enfocado a solventar el planteamiento de los requisitos mínimos de la fase uno (1) de SGSI, se pretende llegar a ser un referente de la aplicabilidad y facilidad en la adopción del estándar a nivel local en las organizaciones Colombianas, también se espera que sea un medio para alcanzar, mantener y mejorar el SGSI.

Los controles por desplegar se presentan, generalmente como procedimientos e implementación técnica (por ejemplo equipos y software) y en políticas. Sin embargo, en muchos casos, las entidades ya tienen todo el software y hardware operando en sus instalaciones o las nubes públicas y privadas, pero los utilizan de una forma no segura en algunas o todas las ocasiones; de tal manera que, la mayor parte del despliegue de ISO 27001 estará enfocada en identificar los activos informáticos, determinar las políticas de seguridad de la información; estas deben estar enfocadas en proteger el Core del negocio, sus activos tecnológicos más preciados, establecer los mecanismos para evaluar, catalogar y reducción del riesgo.

En la figura 6, se plantea el esquema del framework del SGSI diseñado para el proyecto, este permitirá redactar documentos o formatos necesarios para prevenir violaciones o infracciones en la seguridad informática, “es por ello por lo que la seguridad de la información no se limita a lo relacionado con las TI (Tecnologías de la Información) únicamente, adicionalmente va de la mano con la gestión de los recursos humanos, de procesos, la protección física, la protección jurídica, etc. Sin dejar de lado los documentos y usuarios finales que de una u otra manera interactuara con los datos.

Figura 6: Modelo planteado del Framework de gestión documental del SGSI



Fuente: Propiedad del autor.

La Figura 6, presenta tres pasos básicos dentro del modelo planteado, hasta llegar al servidor de gestión documental, denominados como: Asignar encargados, Realización de la actividad y Control documental, a continuación, describen sus propósitos primordiales como son:

Asignar encargado(s): Gestión de roles o responsables de generar o actualizar los documentos requeridos.

Realización de la actividad: Los responsables llevan a cabo las actividades y publican el documento que las sustentan en su versión inicial o continuada.

Control documental: Ciclos continuos de la documentación (versiones) siguiendo el ciclo Deming o PHVA, finalmente se da resolución a las recomendaciones solicitadas o incidencias detectadas, como parte del proceso de mejora continua del SGSI.

Es imprescindible, que los responsables de los sistemas de información reconozcan la existencia de riesgos, así como la necesidad latente de mitigarlos continuamente y a tiempo, al igual que el escoger la Metodología de gestión de riesgos que utilizara la organización para analizar sistemática y repetidamente los riesgos identificados. De forma reiterativa se deben planificar las medidas a tomar oportunamente en aras de mantener los riesgos bajo control, es decir en su mínima expresión posible cada vez que se repita el ciclo Deming o de mejora continua. Dicho esto, es plausible "Que la organización se prepare para los procesos de evaluación, auditoría, certificación o acreditación"[36] de la norma y se convierta en un hábito el aplicar las mejores prácticas y recomendaciones entregadas como parte de la normatividad ISO IEC 27001:2013.

---

36 Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129–134. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=108732548&lang=es&site=eds-live&scope=site

La gestión documental debe asegurar el correcto resguardo de la información, gestión de los roles y usuarios que acceden a la información, de igual manera debe proveer mecanismos de recuperación o restauración de los datos, como forma de restauración avanzada incluir la posibilidad de restaurar deferentes versiones de cada archivo, sin importar que fuera editado en línea, desde un PC, desde un Smartphone o por otro usuario que esté debidamente autenticado y autorizado para realizar acciones sobre el documento u objeto en general.

La gestión documental y gobernanza en los modelos tic: prioriza la visibilidad y presencia de la normativa internacional enfocada al modelo de referencia COBIT framework (spanish). La gestión de servicios y gobernanza de sistemas de información disponiendo de múltiples normas que agrupan las mejores prácticas desarrolladas por empresas e instituciones. La recopilación de esas experiencias se ha venido presentando como marcos de referencia que estipulan procesos, indicadores y objetivos a utilizar como guías que ayudan a establecer procesos internos o externos, finalmente permite la comparación de su ejecución con otras entidades que ya están ejecutando las buenas prácticas de la industria. Uno de ellos que sobresale es el modelo COBIT que ha sido desarrollado por Information Systems Audit and Control Association (ISACA) y la norma internacional ISO/IEC 38500, dedicada a la gobernanza de las TIC.[37]

Definición de un marco general de referencia de y para la ciberseguridad en las entidades basado en adm-togaf. (spanish). Plantea un conjunto de pasos y actividades que son necesarios para el despliegue de un marco de referencia de ciberseguridad corporativo, por lo cual, hemos tomado al Método de Descripción Arquitectónica ADM-TOGAF y su integración con SABSA metodología de seguridad empresarial como referencia, estos definen las fases iterativas adaptadas con las normas de ciberseguridad definidas en los marcos COBIT 5 y NIST, y en los estándares ISO 27001 e ISO 27032 en conjunto. Adicionalmente, se presentaron resultados obtenidos tras la aplicación dirigida del marco de referencia al contexto empresarial local[38]

---

[37] Eito-Brun, R., & Aliaga, C. C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. (Spanish). Revista Española de Documentación Científica, 43(3), 1–14. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=146457387&lang=es&site=eds-live&scope=site

[38] Jaramillo H., D., Cabrera S., A., Abad E., M., Torres V., A., & Carrillo erdúm, J. (2015). Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1, 562. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=114061117&lang=es&site=eds-live&scope=site

3.3 ANTECEDENTES

La creciente de manda y uso de las tecnologías de la información gracias a la democratización de la Internet ha permitido que las empresas abran sus vitrinas al mundo para ofrecer sus productos o servicios, volviéndose imperativo el poder ofrecer transacciones electrónicas (pagos o compras), toda organización que quiera prestar los servicios de E-commerce para sus clientes debe aplicar las mejores políticas de seguridad de la información a sus activos, procesos de la mano del recurso humano, en pro de garantizar un marco adecuado y seguro en las transacciones, dado lo anterior y por normatividades resulta imprescindible y debe ser parte del horizonte alcanzable de estas compañías, Facilitar la implantación de un Sistema de Gestión de Seguridad de la Información – SGSI, "en el mundo hay 31.910 entidades certificadas en la Norma ISO IEC 27001:2013"[39] es decir tienen implantado el SGSI; estas consideraciones fundamentan mi propuesta de proyecto aplicado para la Implementación de un sistema de Gestión de Seguridad de la información ISO IEC 27001:2013 soportado en software de gestión documental con licenciamiento GPLv3 o Framework del Sistema de Gestión de la Seguridad Informática y su gestión documental sobre arquitectura ARM en pro de la democratización en el Valle y quizá a nivel nacional para entidades de cualquier sector que quiera reforzar sus mecanismos o capas adicionales de seguridad informática y de la información.

(Sarria 2015) aborda las dimensiones de la seguridad de la información desde: "diseñando el modelo del sistema de gestión de seguridad de la información, proporcionamos herramientas útiles para la toma de decisiones del área administrativa y las medidas adecuadas sobre la administración de recursos informáticos y las normatividades tecnológicas, posibilitando mejores tiempos de respuesta y logrando mitigar las amenazas existentes".

Conocer y valorar el activo que es afectado, con la metodología Magerit y las dimensiones de seguridad como la Integridad de los datos, Autenticidad, Trazabilidad, Disponibilidad y Confidencialidad de la información[40].

Estas dimensiones como pilares del SGSI aplicables a los activos informáticos de las entidades deben ser el foco continuo de las organizaciones y son parte integral de las pretensiones de este proyecto.

---

39 ISOTools. Excellence. ISO publica la encuesta 2018 de certificaciones de estándares. España. 2019. [Consultado 20 junio 2020]. Disponible en: https://www.isotools.org/2019/09/24/iso-publica-la-encuesta-2018-de-certificaciones-de-estandares

40 Sarria Cuellar, M. (2015). Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. [Consultado 20 mayo 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ir00913a&AN=unad.10596.3631&lang=es&site=eds-live&scope=site

En la Figura 7 vemos la BotNet Mariposa y su afectación al top 10 de esos Países, compuesta por más de 13 millones de direcciones IP (identificador 'único' de cada dispositivo en red) infectadas y a su vez distribuidas en 190 países al rededor del mundo. Donde Colombia ocupó el quinto puesto entre los países más afectados por la red zombie[41]

Figura 7: Países afectados por la BotNet Mariposa en 2010

No.	PAÍS	%
1	INDIA	19.14
2	MÉXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	COLOMBIA	4.94
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55

Fuente. CONPES 3701

La Universidad Piloto de Colombia (UPC) y su Facultad de Ingenierías, desde el posgrado. Especialización en Seguridad Informática, con documento tipo Tesis: Lineamientos de política para ciberseguridad y ciberdefensa, documento CONPES 3701, en su resumen menciona: Análisis sobre los ataques cibernéticos como uno de los principales riesgos a los que se enfrenta la sociedad globalizada de hoy, y las iniciativas generadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información en entidades públicas como privadas de la nación.[42]

Al ser conscientes de la importancia que tienen los ciclos PHVA o mejora continua en las empresas de hoy en día deben adaptar todos sus procesos institucionales y sus estrategias de negocios primando las directrices de seguridad de la información, considerando que sus recursos informáticos pueden sufrir diversos daños que son ocasionados desde exterior o interior de la entidad.

---

41 Conpes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. p. 2. [Consultado: 23 diciembre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

42 Fula Perilla, P. A. (2016). Lineamientos de política para ciberseguridad y ciberdefensa, documento CONPES 3701. Instname:Universidad Piloto de Colombia ; Reponame:Repositorio Institucional RE-Pilo. [Consultado 28 diciembre 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.D0819909&lang=es&site=eds-live&scope=site

Por ejemplo: Robo de información, uso no autorizado, destrucción, ataque de denegación de servicio , acceso indebido a los sistemas informáticos, entre muchos otros que pueden llegar a afectar la imagen corporativa, hasta perder parte o la totalidad del mercado frente a su competencia, quienes, si tengan estándares, directrices de ciberseguridad desplegadas y controlados con los ciclos de mejora continua. El no tener lineamientos claros, apoyo de los directivos en cuanto al cumplimiento de las normatividades vigentes, adoptadas y tareas asignadas a los colaboradores de la entidad, y que sean en aplicables en términos de ciberseguridad, puede afectar operación normal de cualquier organización[43].

Moreno 2017) precisa que el desarrollo de herramientas informáticas en el mercado, la apertura de datos, la globalización de la economía, las tendencias de apertura de la información y los servicios al ciudadano ido obligado a las entidades a replantear sus marcos estratégicos en materia de las tecnologías; debido al gran aumento de los riesgos, por ello el diagnosticar la plataforma tecnológica, las redes, el software y sus posibles vulnerabilidades son algunas de las actividades importantes los especialistas del área en armonía con los sistemas para disminuir y mitigar los riesgos informáticos garantizando la continuidad de la operación[44].

El identificar todos los activos informáticos y catalogarlos nos llevara a finalmente establecer políticas y controles de seguridad requeridos en el sistema en aras de la disminución de riesgos en las tecnologías de la información y comunicación o las permeadas por el comercio electrónico o prestación de servicios e incluso las experiencias de los clientes al utilizar plataformas tecnológicas, para así aunar esfuerzos que se verán reflejados al interior de la organización y la prestación de un servicio de primera y de calidad[45] al exterior de la organización y para los usuarios finales al contar con los parámetros aceptables de seguridad informática aceptados mundialmente.

La figura 8, permite ver el crecimiento de las entidades certificadas en la ISO IEC 27001 en América Latina, para el año 2017 en Colombia había 148 compañías certificadas en la norma. Tristemente son pocas las entidades que tienen musculo financiero y deciden embarcase en los procesos de adopción de la normatividad quizá por restarle importancia a la ciberseguridad de sus activos informáticos

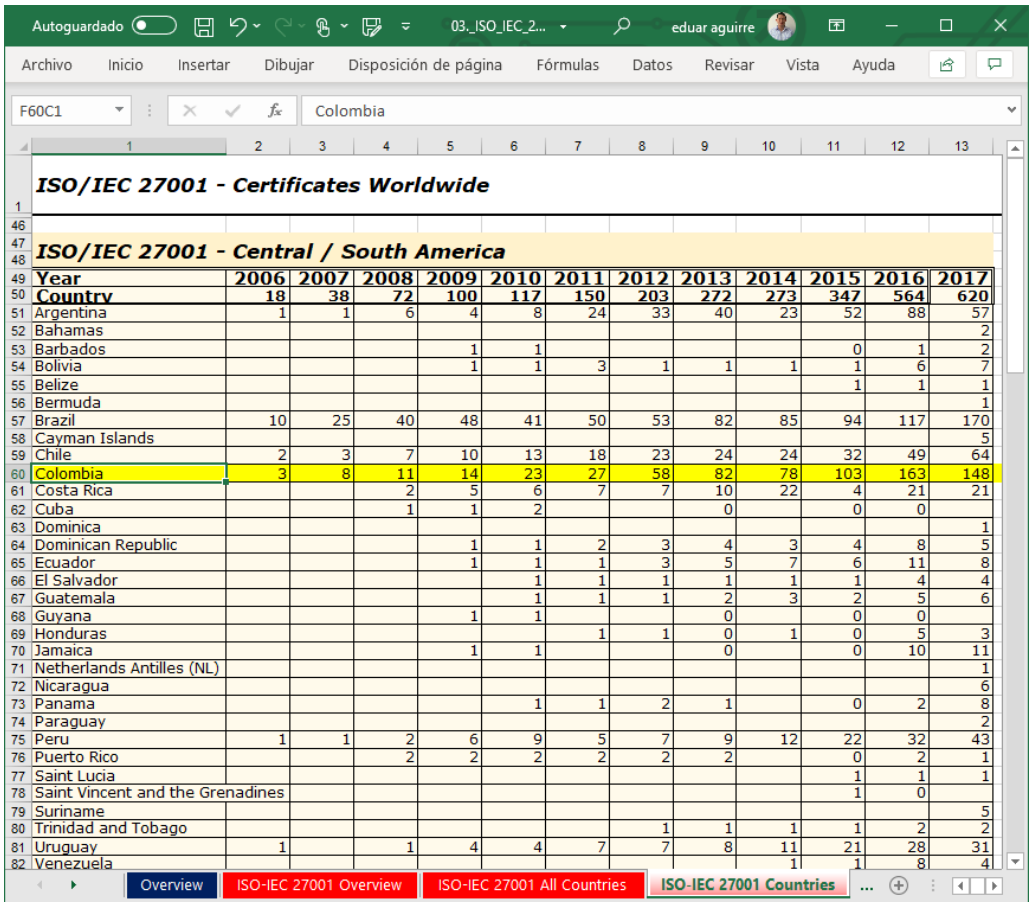
Figura 8: Países certificados: Sur América ISO IEC 2017:2013 entre 2006-2017

---

43 Sarria Cuellar, M. (2015). Diseñoo de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. [Consultado 20 mayo 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ir00913a&AN=unad.10596.3631&lang=es&site=eds-live&scope=site

44 Moreno F. C. E. (2017). Diseño de un Sistema de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías territorial Nariño.- p 13. [Consultado 15 mayo 2020]. Disponible en: *https://repository.unad.edu.co/handle/10596/11876*

45 Ibid. p. 13.



ISO/IEC 27001 - Certificates Worldwide

ISO/IEC 27001 - Central / South America

Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Country	18	38	72	100	117	150	203	272	273	347	564	620
Argentina	1	1	6	4	8	24	33	40	23	52	88	57
Bahamas												2
Barbados				1	1					0	1	2
Bolivia				1	1	3	1	1	1	1	6	7
Belize										1	1	1
Bermuda												1
Brazil	10	25	40	48	41	50	53	82	85	94	117	170
Cayman Islands												5
Chile	2	3	7	10	13	18	23	24	24	32	49	64
Colombia	3	8	11	14	23	27	58	82	78	103	163	148
Costa Rica			2	5	6	7	7	10	22	4	21	21
Cuba			1	1	2			0		0	0	
Dominica												1
Dominican Republic				1	1	2	3	4	3	4	8	5
Ecuador				1	1	1	3	5	7	6	11	8
El Salvador					1	1	1	1	1	1	4	4
Guatemala					1	1	1	2	3	2	5	6
Guyana				1	1			0		0	0	
Honduras						1	1	0	1	0	5	3
Jamaica				1	1			0		0	10	11
Netherlands Antilles (NL)												1
Nicaragua												6
Panama					1	1	2	1		0	2	8
Paraguay												2
Peru	1	1	2	6	9	5	7	9	12	22	32	43
Puerto Rico			2	2	2	2	2	2		0	2	1
Saint Lucia										1	1	1
Saint Vincent and the Grenadines										1	0	
Suriname												5
Trinidad and Tobago							1	1	1	1	2	2
Uruguay	1		1	4	4	7	7	8	11	21	28	31
Venezuela									1	1	8	4

Fuente: THE ISO SURVEY. Disponible desde: https://isotc.iso.org/livelink

Revisando propuestas especializadas como e-PULPO, siendo una plataforma que integra un módulo SGSI y facilita la planificación la primera fase del mismo, permitiendo la documentación, gestión de incidencias, manejo de activos, indicadores, formación y auditorías establecidas por la norma ISO IEC 27001:2013, adicionalmente el despliegue de controles basados en la normatividad ISO 27002; e-PULPO se centraliza en la revisión, administración, control y la gestión documental de ésta, de tal toma que su interfaz gráfica y componentes distribuidos de del módulo gestión documental, tienen facilidad e interactividad, permitiéndole ser una plataforma eficaz, eficiente y con funciones reguladas en el cumplimiento. (Ingenia, 2010)[46]. Sabemos la importancia de que las organizaciones tengan ciber-resiliencia que apoye la continuidad del negocio y sus operaciones como parte del DRP es de vital importancia.

[46] MARTELO, R. J., MADERA, J. E., & Betín (2017), Software para Gestión Documental un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI), 26(2), 129–134. DIsponible en: https://bibliotecavirtual.unad.edu.co

3.4 MARCO LEGAL

3.4.1 Ley 1273 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”[47].

3.4.2 Ley estatutaria 1266 de 2008

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”[48].

3.4.3 Código de Comercio, art. 86, art 515

“De los comerciantes y de los asuntos de comercio”[49].

3.4.4 Circular Externa 007 de 2018 - SIF

“Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad”[50].

3.4.5 Circular Externa 008 de 2018 - SIF

“Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad”[51].

---

47 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. Bogotá. (Mayo 10 de 2015). Diario Oficial No. 47.223 de 5 de enero de 2009, 2015). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

48 COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008., 2008). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

49 COLOMBIA, CONGRESO DE LA REPUBLICA. DECRETO 410 DE 1971. Bogotá. (diciembre 31 de 1971). Artículo 515. Diario Oficial No. 33.339 del 16 de junio de 1971, 1971). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio_pr002.html

50 Super Intendencia Financiera de Colombia, Circular Externa 007 de 2018, Bogotá. [Consultado 18 octubre 2020]. Disponible en: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc:

51 Super Intendencia Financiera de Colombia, Circular Externa 008 de 2018, Bogotá, 2018. [Consultado 18 octubre 2020]. Disponible en: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce008_18.doc

3.4.6 Ley 1341 de 2009

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"[52].

3.4.7 CONPES 3701 de 2011

"Lineamientos de política para la Ciberseguridad y Ciberdefensa"[53].

3.4.8 Ley 527 de 1999

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"[54].

3.4.9 CRT. Resolución 2058 del 2009

"Por la cual se establecen los criterios y las condiciones para determinar mercados relevantes y para la existencia de posición dominante en dichos mercados y se dictan otras disposiciones"[55].

3.4.10 Ley 1266 de 2008

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[56].

---

52 Comisión de Regulación de Comunicaciones, República de Colombia. 2015. p 77., 2018. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

53 Conpes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. p. 2. [Consultado: 23 diciembre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

54 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 de 1999. Bogotá. (Agosto 21 de 1999). Diario Oficial 43.673. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

55 Comisión de Regulación de Comunicaciones, República de Colombia. Resolución 2058 del 2009., 2009. [Consultado 18 octubre 2020]. Disponible en: https://www.crcom.gov.co/resoluciones/00002058.pdf

56 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 de 2008. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

3.4.11 Ley 1581 de 2012

“Por la cual se dictan disposiciones generales para la protección de datos personales”[57].

3.4.12 Decreto y 1377 de 2013

“Por el cual se reglamenta parcialmente la Ley 1581 de 2012"[58].

---

57 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012. Bogotá. (Octubre 18 de 2012). Diario Oficial 48.587. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

58 MIN TIC. Documentos para HABEAS DATA: Regulación y Reglamentación. Bogotá 2013. [Consultado 18 octubre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

4. REQUISITOS MÍNIMOS PARA EL DISEÑO DE UN FRAMEWORK ALINEADO A LA NORMA ISO/IEC 27001

La norma ISO IEC 27001:2013, exige que la seguridad informática se fundamente en la preservación de los tres pilares básicos: Integridad, disponibilidad y confidencialidad, por lo tanto, es imprescindible velar y verificar el cumplimiento de cada uno de ellos auditando los procesos periódicamente.

"Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta estratégica como soporte a las organizaciones para implementar políticas de seguridad informática, controles y procedimientos alineados con los objetivos del negocio, medibles y de esta forma obtener un panorama general sobre el estado de los riesgos, socializarlos y gestionarlos por la organización; De forma organizada, es decir, estructurada, sistemática y adaptada a los cambios de la organización, todo lo anterior debe ser debidamente documentado" [59] utilizando el framework como reposo y gestión de la información.

"En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático. Este proceso es el que constituye un SGSI". Como ruta base se presenta la figura 8.

Figura 9: Ruta base – ISO 27001

Fuente: Propiedad del autor

[59] ISO 27001. (2005). ¿Qué es un SGSI? El portal de ISO 27001 en español. [citado en 25 de abril de 2016]. Disponible en linea: http://www.iso27000.es

La normatividad contempla 10 dominios o fases a ejecutar como parte de su proceso de adopción, en este proyecto se han definido 5 fases para la aplicación de la norma ISO IEC 27001:2013, en la figura 9 presentamos los elementos o características claves a obtener por cualquier organización que despliegue el Sistema de Gestión de Seguridad de la Información.

Figura 10: Beneficios de la ISO 27001

Fuente: Propiedad del autor

4.1 DISEÑO DEL FRAMEWORK DEL SGSI

Resulta necesario escoger una metodología para la evaluación de riesgos informáticos que puedan impactar o no los activos informáticos de la organización causando una vulneración a los sistemas e imposibilitando el acceso a ellos o a su información, repercutiendo en pérdidas económicas para los dueños de negocio y desfavoreciendo la imagen corporativa.

Utilizando el modelo de seguridad en profundidad planteamos abstraer los mecanismos del SGSI aplicables al framework de gestión documental desde la capa externa hacia los bienes de misión crítica, es decir los elementos sobre los cuales tenemos control en un E-commerce o en los documentos de misión crítica y de carácter privado de la entidad, en la figura 10, precisamos cuales son esos mecanismos para utilizar del modelo de seguridad en profundidad adaptado desde SS360 para el Framework de Seguridad de la Información que cuenta con un agente instalado de la solución Sophos Central Intercept X con EDR, dicha solución se ha especializado y es líder en el cuadrante de Gardner.

Es imperativo contar con protección perimetral, Prevención de Intrusos, Detección de anomalías en la red, Control de navegación de los usuarios internos, Detección de redes BotNet (redes de computadoras comprometidas), Honeypots (servicios y/o servidores señuelos, “fáciles de vulnerar”), Detección de código malicioso y conocer el estado de salud de los dispositivos de la red como computadoras, celulares, servidores o cualquier otro host (equipo que tenga una dirección de red/IP).

En seguridad informática hay un principio que dicta, “Lo que no se conoce, no se puede proteger”, por lo tanto, la entidad debe identificar todos y cada uno de sus activos informáticos utilizando una metodología, después de elaborar la tabla 4, se escogió una, como apoyo en la labor de identificación de riesgos y su correcta gestión aplicada a los activos informáticos, de igual manera que se encuentra alineada con el uso de software o plataformas de bajo coste consideradas como potentes.

La metodología seleccionada es Magerit (ver tabla 1) por sus ventajas y versatilidad que permitirán eficiencia una vez tengamos identificados los activos haciendo uso de una matriz entregada por el Ingeniero Fernando Zambrano de la Universidad Nacional Abierta y a Distancia, durante la trayectoria final de la especialización en seguridad informática en el curso Riesgos y Control Informáticos, está matriz ha sido mejorada por diversos estudiantes y mi persona a lo largo del tiempo.

4.1.1 Ventajas y desventajas en metodologías de gestión de riesgos

Tabla 1. Metodologías de gestión de riesgos, ventajas y desventajas

Metodologías de gestión de riesgos	Ventajas	Desventajas
Magerit	Describe los pasos para realizar un correcto análisis del riesgo y sus estados en los activos informáticos de la organización y cómo gestionar su mitigación. Se dice que tiene un alcance completo para el análisis de riesgos y su correcta gestión Matriz madurara bajo el liderazgo del curso Riesgo y Control Informático. Facilita el desarrollo estrategias de seguridad y sus planes. Establece responsables de los activos informáticos.	La gestión de riesgos de seguridad de la información es genérica. Su traducción incompleta demanda sobre costos. Su inventariado de las políticas de seguridad de la información está incompleto.
Mehari	Las auditorías detectan vulnerabilidades al analizar situaciones de riesgo Su modelo es cuantitativo y cualitativo frente al análisis de riesgos.	Falencia en el No repudio al enfocarse en la confidencialidad, disponibilidad, e integridad de la información
Cramm (CCTA Risk Analysis and Management Method)	Realiza evaluación mixta al definir los objetivos de seguridad en función del respectivo análisis de riesgos y la selección de salvaguardas. Identifica y clasifica los activos de TI, al igual que evalúa el impacto empresarial.	No puede analizar procesos o los recursos. Es aplicable a organizaciones públicas y privadas solamente.
Octave	Se construyen los perfiles de las amenazas en función de los activos de información.	Solo aplica para PYMEs (pequeñas y medianas empresas).

Metodologías de gestión de riesgos	Ventajas	Desventajas
	Facilita el desarrollo de estrategias de seguridad y planes. Facilita la identificación de vulnerabilidades y su infraestructura. Es la metodología más completa debido a que involucra en operación el análisis de los procesos de negocio, dependencias, recursos, vulnerabilidades, activos y amenazas que se deben salvaguardar	No es compatible con los estándares.
ISO/IEC 27005	Es parte integral del SGSI a nivel de su aplicación o mejora continua. Aborda los riesgos de forma eficaz, cada vez que sea necesario. Facilita la identificación de los requisitos de seguridad de la información en función de las necesidades en la organización.	No define o recomienda o especifica una metodología en particular, por lo cual se deben tener en cuenta diversos factores como el alcance dado en el SGSI o el sector comercial de la entidad.

Fuente: Propiedad del autor

4.1.2 Listado con los requisitos de la norma ISO/IEC 27001:2013.

La norma que ISO/IEC 27001:2013ISO/IEC 27001:2013, describe un conjunto de herramientas corporativas y metodológicas que permiten definir un plan de acción a seguir en busca de la solución de problemas de seguridad informática, tanto a nivel técnico, como organizativo y también de tipo legislativo en una organización constituida; La versión 2013 de la norma ISO IEC 27001: incluye en su documentación catorce controles principales, desde el dominio A5, hasta el A18.

- Dominio A5. Políticas de la seguridad de la información.
- Dominio A6. Organización de la seguridad de la información.
- Dominio A7. Seguridad de los recursos humanos.
- Dominio A8. Gestión de activos.
- Dominio A9. Control de acceso.
- Dominio A10. Criptografía.
- Dominio A11. Seguridad física y del entorno.
- Dominio A12. Seguridad de las operaciones.
- Dominio A13. Seguridad de las comunicaciones.
- Dominio A14. Adquisición, desarrollo y mantenimiento de sistemas.
- Dominio A15. Relaciones con los proveedores.
- Dominio A16. Gestión de incidentes de seguridad de la información.
- Dominio A17. Aspectos de seguridad de la información de la gestión de Continuidad de negocio.
- Dominio A18. Cumplimiento[60].

Los 14 dominios se engloban en 10 pasos (ver tabla 1) y se mantienen utilizando el ciclo Deming, en el proyecto se utilizará el modelo de seguridad adaptativa como mejora complementaria del SGSI de la norma ISO IEC 27001:2013, sin perder su esencia y resaltando los apartados significativos identificados durante la especialización de seguridad informática.

---

[60] Morán, C. E. (2017). Diseño de un Sistema de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías territorial Nariño.. P. 128. [Consultado 14 marzo 2020]. Disponible en: https://repository.unad.edu.co/handle/10596/11876

Tabla 2. Requisitos norma ISO 27001: 2013

Requisitos	**Descripción**
Objeto y campo de aplicación	Es el primer apartado de la norma que establece las directrices, principios generales y orientaciones necesarias para la aplicación y uso de la norma en la organización mediante un catálogo de buenas prácticas. Los controles y objetivos de control de la norma son una guía para la aplicación de pautas de seguridad efectivas en la organización en función del análisis de riesgos a realizar y de los requisitos de seguridad identificados, así como la correcta gestión de los recursos disponibles en la organización.
Referencias normativas:	En este punto se indica que es importante e imperativo el recurrir a los documentos asociados términos de seguridad de la información.
Términos y Definiciones:	En esta cláusula queda descrito la terminología/glosario que se utiliza a lo largo y ancho de la normatividad vigente asociada a la seguridad de la información, al igual que la versión actual de la rige, como, por ejemplo: Activo, Disponibilidad, Confidencialidad, Integridad, Seguridad de la información, Evento en la Seguridad de la información y sus controles, Incidente de seguridad de la información, SGSI, Riesgo residual, Riesgo latente, Aceptación del riesgo, Análisis / Evaluación / Estimación / Gestión / Tratamiento / Mitigación de riesgos, Documentación de los procesos y controles que son relevantes para el SGSI al igual que su aplicabilidad en la organización.
Contexto de la Organización	Es un apartado muy importante, permite que las organizaciones identifique su contexto en el cual desarrollan sus actividades de negocio, tanto en clientes externos como internos, de este modo pueden conocer qué necesitan mejorar para 'satisfacer' a sus clientes de manera adecuada y adoptar las medidas mínimas necesarias para cubrir dichas necesidades, que les permitirán proponer opciones y facilitan la toma de decisiones al identificar los riesgos, lo cual permitirá trazar los objetivos, controles y políticas a implementar teniendo en cuenta los activos de la organización.

Requisitos	Descripción
Liderazgo:	La alta dirección, a través del liderazgo su compromiso constante en pro de la concienciación del recurso humano que estará involucrado y tendrá la obligación/responsabilidad acorde a sus roles en el proceso del Sistema de Gestión de Seguridad de la Información, así como garantizar los recursos financieros para desplegar/implementar la norma ISO IEC 27001:2013. Garantizando que sea un ciclo de mejora continua, gracias a su participación en la puesta en marcha, monitorización, revisión y mantenimiento del SGSI, generando una cultura empresarial de la mejora continúa mediante auditorías y el velar por que se apliquen las mejoras preventivas o correctivas.
Planificación:	En este apartado se ve reflejada la importancia de la identificación y catalogación de los riesgos sobre los activos de información a la hora de realizar una planificación del SGSI, así como los objetivos y la manera de aplicar los controles, apoyándose en las políticas de seguridad de la información.
Soporte:	Destaca que para que un Sistema de Gestión de Seguridad de la Información funcione con éxito, es preciso que se destinen los recursos adecuados como son: el talento humano, los financieros o materiales, además de que el personal involucrado en los procesos debe las habilidades requeridas, información y comunicación adecuada desde la alta gerencia. Con lo anterior podrán aplicar los controles de seguridad, para dar cumplimiento a las políticas de la información al igual que garantizan el poder identificar todo tipo de riesgos y su cuantificación como parte del proceso de mejora continua.
Operación:	El cumplimiento de los requisitos de un SGSI se obtiene al planificar su implementación y ejercer los controles adecuados a los procesos organizacionales, llevando a cabo una valoración de los riesgos a los que

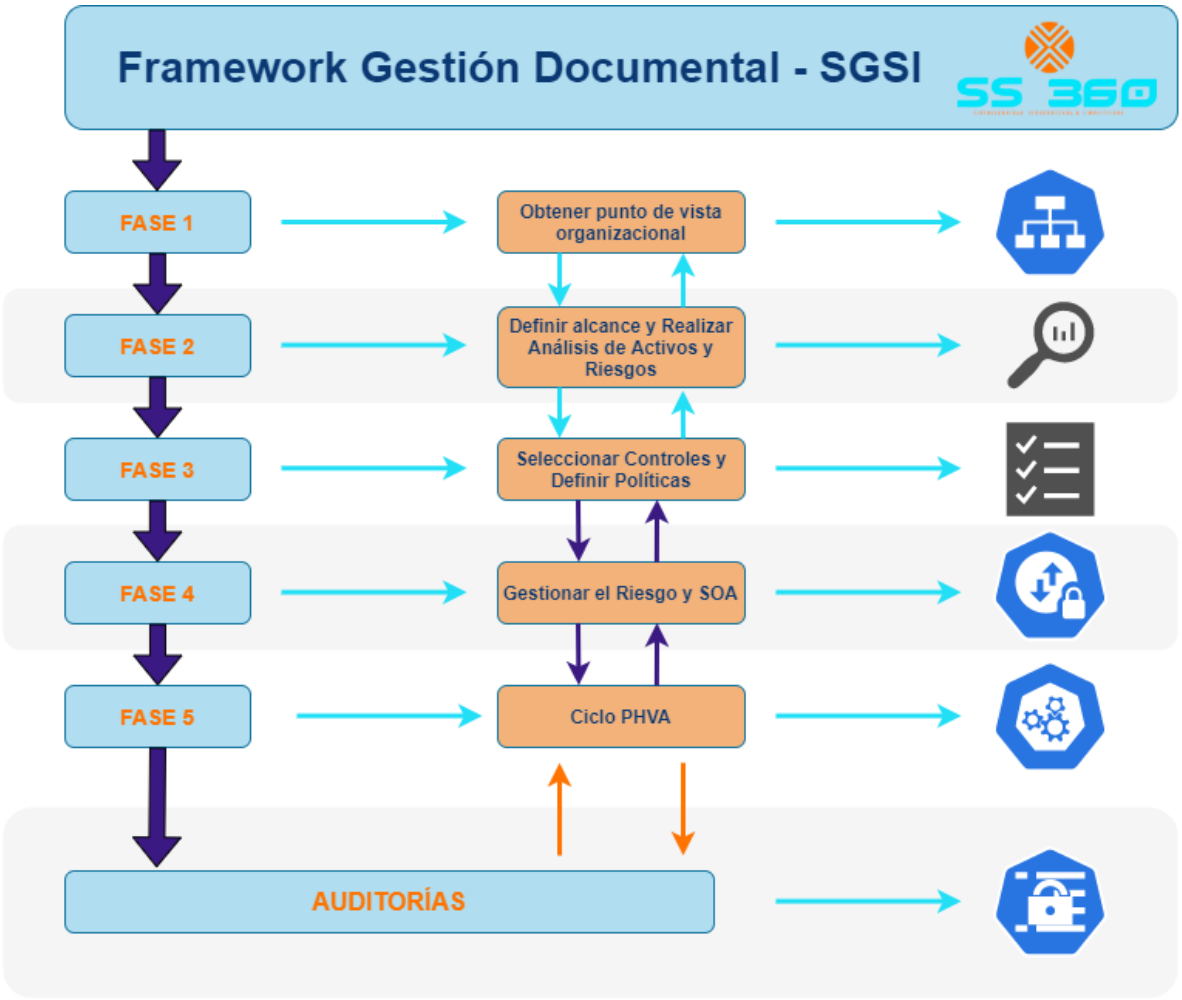
Requisitos	Descripción
	está expuesta la organización y por supuesto, el posterior tratamiento de estos gracias al apoyo y directrices que comunica la alta gerencia.
Evaluación del desempeño:	Necesidad continua de hacer un seguimiento adecuado de los controles de seguridad de la información aplicados en la organización, así como su respectiva medición, análisis, evaluación, auditoría interna, así como la revisión de la alta gerencia y los líderes del SGSI que velaran por el cumplimiento de la planificación realizada, controles de seguridad adoptados que deben ser alineados con los objetivos corporativos para tener un nivel mínimo aceptable de seguridad de la información.
Mejora:	Último apartado que requiere del aporto de los Directivos y en él queda establecida la necesidad de que todos los colaboradores involucrados en el proceso trabajen reiterativamente por conseguir la mejora continua, al ser un ciclo repetitivo, donde existe una cultura por empresarial Es decir, deben ser capaces de aplicar los correctivos necesarios para ponerle solución de fondo o mitigar el riesgo al presentarse las No Conformidades, y así, mejorar continuamente el Sistema de Gestión de Seguridad de la Información, gracias a las auditorías internas o externas.

Fuente: Propiedad del autor

4.2 FASES DEL FRAMEWORK ALINEADO CON LA SGSI DE LA NORMA ISO 27001:2013

La figura 12 muestra un resumen de las fases adaptadas y propuestas para implementar un SGSI de la norma ISO 27001:2013 dentro del marco del Framework de Gestión Documental del SGSI.

Figura 11: Resumen SGSI propuesto



Fuente: Propiedad del autor

4.2.1 Fase 1: Obtener punto de vista organizacional

La identificación de la razón social, estructura organizacional o jerárquica (organigrama), quienes son los líderes de cada proceso de negocio, cual es el Core del negocio, cuáles son sus objetivos y metas organizacionales entre otros.

4.2.2 Fase 2: Definir alcance y Realizar Análisis de Activos y Riesgos

Comprende acotar la actividad comercial de la entidad, cuáles son los activos informáticos involucrados y que serán objeto del estudio de análisis riesgos de acuerdo con la nomenclatura de la metodología Magerit.

Tabla 3: Definición del alcance

OBJETIVO	Realizar análisis, identificación, evaluación de los activos informáticos y riesgos de seguridad de la información.
ALCANCE	Aplica para los activos
Nombre de la Empresa:	**SS360 S.A.S.**
Sitio web:	
CONTEXTO LEGAL	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	Se tratarán los riesgos cuyos niveles sean:
	NIVEL POR TRATAR: ACEPTABLE
	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	Niveles de aceptación del riesgo **Aceptable (A): "**entre 1 y 5", **Moderado (M): "**entre 6 y 15", **Inaceptable (I):** entre "16 y 26"
	Aplicar los controles es igual a aceptar un riesgo de residual en niveles APRECIABLE o **IMPORTANTE**
	Criticidad residual de: **Despreciable (d)** 1 a 4 **Baja (b)** 5 a 9 **Apreciable (a)** 10 a 15 **Importante (i)**16 a 20 **Crítico (c)** 21 a 25

Fuente: Propiedad del autor

Clasificación e Identificación de activos según Magerit:

[D] DATOS

[K] CLAVES CRIPTOGRAFICAS

[S] SERVICIOS

[SW] SOFTWARE

[HW] EQUIPAMENTO INFORMÁTICO

[COM] REDES DE COMUNICACIONES

[Media] SOPORTE DE INFORMACIÓN

[AUX] EQUIPAMENTO AUXILIAR

[L] INSTALACIONES

[P] PERSONAL.

En la figura 12 presentamos un ejemplo de inventario de activos, aplicando la clasificación del activo e identificación sugerida por la metodología de tratamiento de riesgos: Magerit. Para más información de la figura 12 puede consultarse el anexo B.

Figura 12: Inventario de activos

SALAS DE SISTEMAS

Sala N° 1 – Sala de sistemas con 20 equipos de computo

Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico	Activo	Tipo de activo
Switch 24 puertos	Dispositivo de comunicación de equipos.	Departamento de sistemas	Físico	Sala de sistemas	Si	[COM]	Redes de comunicaciones
Teléfono IP	Permite la comunicación en diferentes dependencias.	Departamento de sistemas	Físico	Sala de sistemas	Si	[COM]	Redes de comunicaciones
PC	Equipo informático	Departamento de sistemas	Físico	Sala de sistemas	Si	[HW]	Equipamiento informático

Fuente: Propiedad del autor.

Valoración del riesgo

Amparados en el uso de la Matriz de Análisis de Riesgo que nos permite identificar, cuantificar y valorar los riesgos de los activos de información de la organización, presentados por la metodología de Magerit y considerando el impacto que podría generar la ocurrencia de algún evento en la entidad o sus sistemas de información.

La figura 13 presenta la matriz de probabilidad de ocurrencia del riesgo, creada a partir de la tabla de valoración de riesgo y teniendo en cuenta las diferentes dimensiones de seguridad de la información, como son Disponibilidad, Integridad y Confidencialidad, los riesgos clasificados como MB o Muy Bajos y ubicados en la Categoría de Despreciable tendrán un peso o una valoración de 1 a 4, y así sucesivamente hasta llegar a los riesgos Muy Altos, categorizados como críticos y con valoración de 21 a 25; tenemos:

Figura 13: Matriz de Riesgos

VALORACIÓN DEL RIESGO			
Valoración del riesgo	Nomenclatura	Categoría	Valoración
	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Propiedad del autor

4.2.3 Fase 3: Seleccionar controles y Definir Políticas

Es imprescindible establecer los controles de la ISO IEC 27001:2013 aplicables al entorno y aplicabilidad acorde al alcance que se define con la junta directiva o gerencia general de la compañía.

Los controles presentados por la ISO IEC 27001 pueden ser consultados en el anexo A.

4.2.4 Fase 4: Gestionar el Riesgo y SOA

NOMBRE	CARACTERÍSTICAS
MODELOS DE MADUREZ	• Identificación de los posibles problemas y priorizar las amenazas. • Enfocarse en los objetivos de control, para mejorar la toma de decisiones. • Enfocarse en los principios seguridad informática. • Alinearse con los objetivos del negocio, aun cuando se presenten ataques informáticos. • Tratar de mantener un nivel de riesgo aceptable alineándose con los objetivos de seguridad. • Redundancia/Contingencia para la infraestructura, componentes o sistemas críticos de la organización.
DECLARACIÓN DE APLICABILIDAD (SOA)	• Se aplica después de realizar la evaluación de riesgos, contiene las amenazas identificadas y analizadas durante la evaluación de riesgos (histórico de los activos). • Mantener un control y registro de las medidas de seguridad aplicadas o por aplicar y las que no se tuvieron en cuenta (Objetivos de controles y control seleccionados). • Facilitar un análisis de brechas - GAP (amenazas internas y externas) • Es la materia prima para el PTR.
PLAN DE TRATAMIENTO DE RIESGOS (PTR)	• Se alinea con los objetivos estratégicos de la empresa, definiendo el alcance, obligaciones y buenas prácticas de seguridad a cumplir por terceros y directos de la organización • Reducir a niveles aceptables los riesgos a los que está expuesta la organización partiendo del análisis de la situación inicial • Plan de recuperación ante desastres • Plan de continuidad del negocio

NOMBRE	CARACTERÍSTICAS
PLAN DE TRATAMIENTO DE RIESGOS (PTR)	• Gestión de copias de seguridad • Definir e implantar las políticas de seguridad de la información

Fuente: Propiedad del autor

4.2.5 Fase 5: Ciclo PHVA

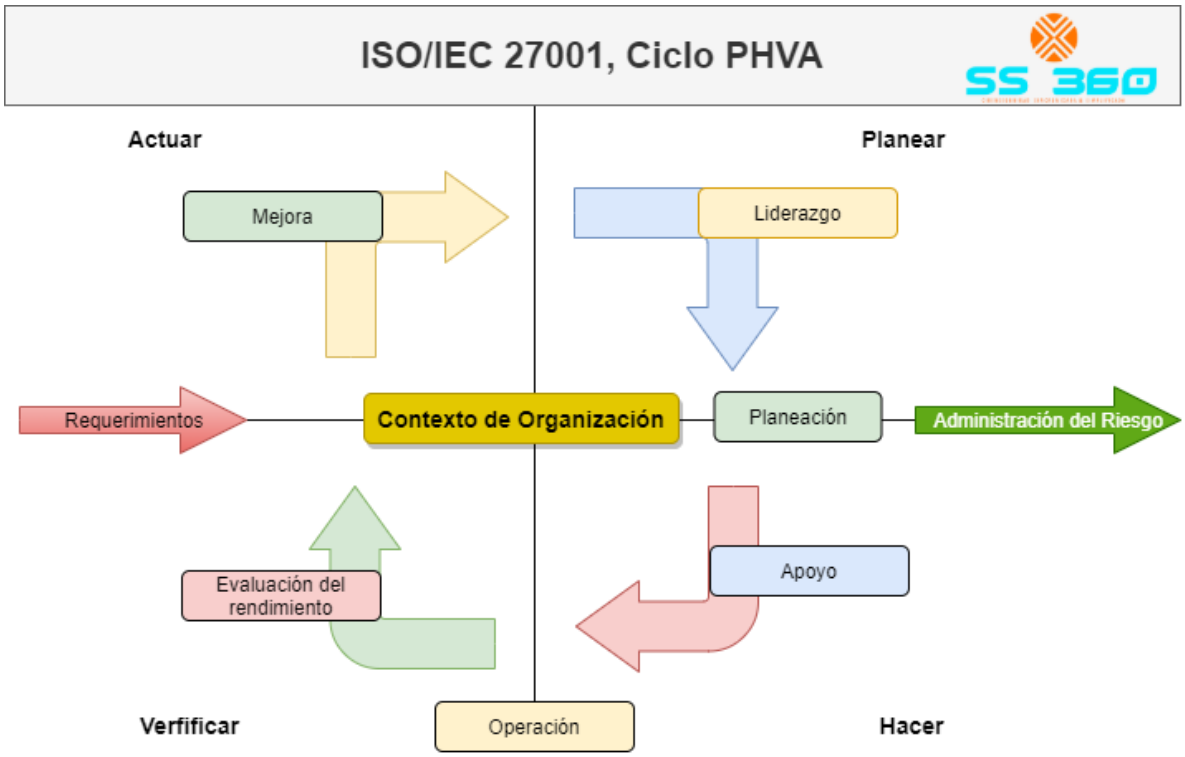
Mediante el ciclo **Deming** o PHVA (Planear, Hacer, Verificar, Actuar) en función del contexto base de cualquier organización teniendo como elemento principal sus documentos de tipo Ofimáticos (Word, Excel, Power Point, etc) se va alimentando el sistema de gestión documental del SGSI, quedando alineado con el modelo de negocios de la organización, estos documentos residirán en el sistema de gestión documental, siendo un complemento donde se gestionarán los documentos, plantillas, esquemas, y demás ficheros que permitan tener un registro del estado actual, avances, mejoras aplicadas y detectadas como parte del ciclo PHVA y controlara los soportes generados por cada proceso de la compañía mediante la estructura jerárquica de almacenamiento.

En la figura 14, presentamos el diagrama de cada una de las fases del ciclo PHVA, cada una tiene un objetivo específico pactico y puntual dentro del sistema de Gestión de Seguridad de la Información, como son:

- "Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.7-
- Act (actuar): mantener y mejorar el SGSI"[61]

[61] Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. [Citado 16 diciembre 2020]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/

Figura 14: Ciclo Deming o PHVA.



Fuente: Propiedad del autor

Planear

- Dejar a la suerte o azar los quehaceres primordiales significa abrir o mantener brechas de seguridad que aprovecharan los delincuentes informáticos, planear es sinónimo de pensar a futuro dentro del contexto que hemos venido definiendo.
- Se planea con base a objetivos definidos por la junta directiva, las demandas del mercado y en pro de lo que se desea como compañía, su prestigio o también llamado renombre.

Hacer

- El No ejecutar el plan de acción definido previamente significa que hemos perdido el tiempo y/o no estamos dándole la prioridad necesaria por tener otras premuras a nivel corporativo, lo cual es sinónimo de una alta gerencia poco comprometida con la seguridad informática de su organización, empleados, clientes y proveedores quedarán desprotegidos o en lo que he denominado el limbo informático.
- Los lineamientos definidos por la auditoría y controles a establecer según la fase de planeación deben ejecutarse, de manera sistemática y enfocada en

la consecución de los objetivos planteados durante el inicio del despliegue del SGSI.

Verificar

- Llegando al paso donde se realiza la respectiva evaluación o reevaluación de los pasos anteriores como parte de un ciclo continuo, se debe medir el desempeño del proceso, los objetivos de seguridad y cumplimiento de las políticas de seguridad, así como el debido reporte a la dirección de la entidad.
- Asegurarse que los mecanismos definidos en la fase de planeación y ejecutados en la fase de hacer fueran ejecutados de la mano de las mejores prácticas y se esté dejando documentación actualizada de los nuevos cambios, que sirven como insumo en las siguientes fases del ciclo Deming.

Actuar

- Una vez se ha planeado, se ejecutó y verifico la planeación, es necesario determinar el porcentaje de objetivos cumplidos acorde las directrices entregadas por la Alta Gerencia.
- Llevar a cabo cada uno de los objetivos, establecer y dar seguimiento a los controles de seguridad de la información definidos en el SOA y afianzando el PTR para reducir los riesgos en los activos informáticos que fueron identificados y catalogados mediante la metodología Magerit.

Esta metodología garantiza la integridad, confidencialidad y disponibilidad de los activos de un negocio. Las pequeñas empresas, al contrario de las grandes entidades, carecen de recursos humanos, económicos y técnicos para atender el mantenimiento de los sistemas de información y la ciberseguridad, por lo tanto, necesitan una herramienta práctica y de bajo costo que permita gestionar oportunamente los riesgos latentes o existentes.

La adopción de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO IEC 27001 de 2013, es una alternativa eficaz y enfocada para que la entidad defina una serie de actividades para sintetizar, ordenar y simplificar de manera reiterativa los esfuerzo conjuntos que ya se ejecutan -o se deberían ejecutar en seguridad informática y de la información.

4.3 AUDITORÍA INTERNA

Los procesos internos o externos de auditoria permiten garantizar una buena relación entre el auditor informático o equipo auditor y la organización o empresa, con el objeto de evitar improvisaciones o una anarquía en el funcionamiento del auditor, los procesos se mantienen en relación directa con la empresa y consta de varias fases como parte de la metodología de trabajo planteada.

Proceso cuyo contenido emite una opinión de condición profesional, que se justifica en el seguimiento de una serie de procedimientos que serán objeto de análisis a partir de la información obtenida de determinados soportes recolectados en la organización; cuya finalidad es determinar si la información representada refleja fielmente la realidad, o si responde a las expectativas que le son atribuidas.

Requiere de al menos un profesional con la formación adecuada y experiencia en auditoría e informática, debe tener conocimiento en la legislación, normas, reglamentos o cualquier otro elemento necesario a la hora de cumplir con su labora de auditor, también debe entender las directrices dadas por los directivos de la organización o el alcance que se le dio al sistema informático.

Los auditores evalúan los controles existentes en la organización, recomiendan la implantación de nuevos controles, al igual que refuerzan aquellos que lo necesiten y, en muy raras ocasiones, recomienda su supresión o eliminación, en cualquier caso, las recomendaciones generales son:

- Realizar entrevistas iniciales, evitando que usuario este prevenido frente al auditor.
- Cuidar la veracidad de los datos suministrados por los usuarios (corroborarlos).
- Los usuarios deben retro alimentar sobre los errores que identificaron de forma anónima o no y mediante cualquier mecanismo.
- Asegurarse de la adecuada Gestión de Controles y apoyo de los líderes de procesos, con el de informática.

5. FRAMEWORK BAJO LA ARQUITECTURA ARM Y SOFTWARE GPLV3 CON SINCRONIZACIÓN A LA NUBE, PARA LA EMPRESA SEGURIDAD SINCRONIZADA 360 (SS360)

El sistema de gestión documental requiere de unos componentes tipo hardware y software que funcionarán en perfecta sincronía y armonía de la mano de las configuraciones especializadas que ha diseñado SS360 para cada componente.

La placa de hardware a utilizar soportará al menos unos 10 usuarios en simultaneo que podrán acceder ya sea desde la interfaz web o desde las aplicaciones que se instalan en el PC en los celulares Desde cualquiera de esas interfaces de conexión dos usuarios pertenecerán a una estructura jerárquica donde heredara no conservarán dos permisos y a su vez pueden generar permisos de orden jerárquico hacia abajo en sus carpetas dentro de su propia estructura.

Instalar una App de computadora o smartphone permite el acceso al sistema de gestión documental, sin embargo, si desean utilizar el navegador web desde un equipo de uso temporal, también funciona.

En la figura 16 presentamos el diagrama que muestra cómo interactúan los compontes del FDG-SGSI, desde su diseño a nivel de arquitectura fue pensado para obtener la mejor relación costo beneficio para las entidades de cualquier sector de la economía de la República de Colombia, el Framework puede ayudar a reformar y mejorar la seguridad de los recursos tecnológicos que posea la entidad como parte de sus procesos de transformación digital.

El Framework del Sistema de Gestión Documental del SGSI o FGD-SGSI, fue diseñado como parte de una idea de negocio ya materializada hoy, bajo propiedad del autor y la empresa Seguridad Sincroniza S.A.S. o SS360 S.A.S, registrada en la cámara de comercio de Cali, Valle del Cauca, Colombia.

Figura 154: Componentes Framework de Gestión Documental del SGSI

Fuente: Propiedad del autor.

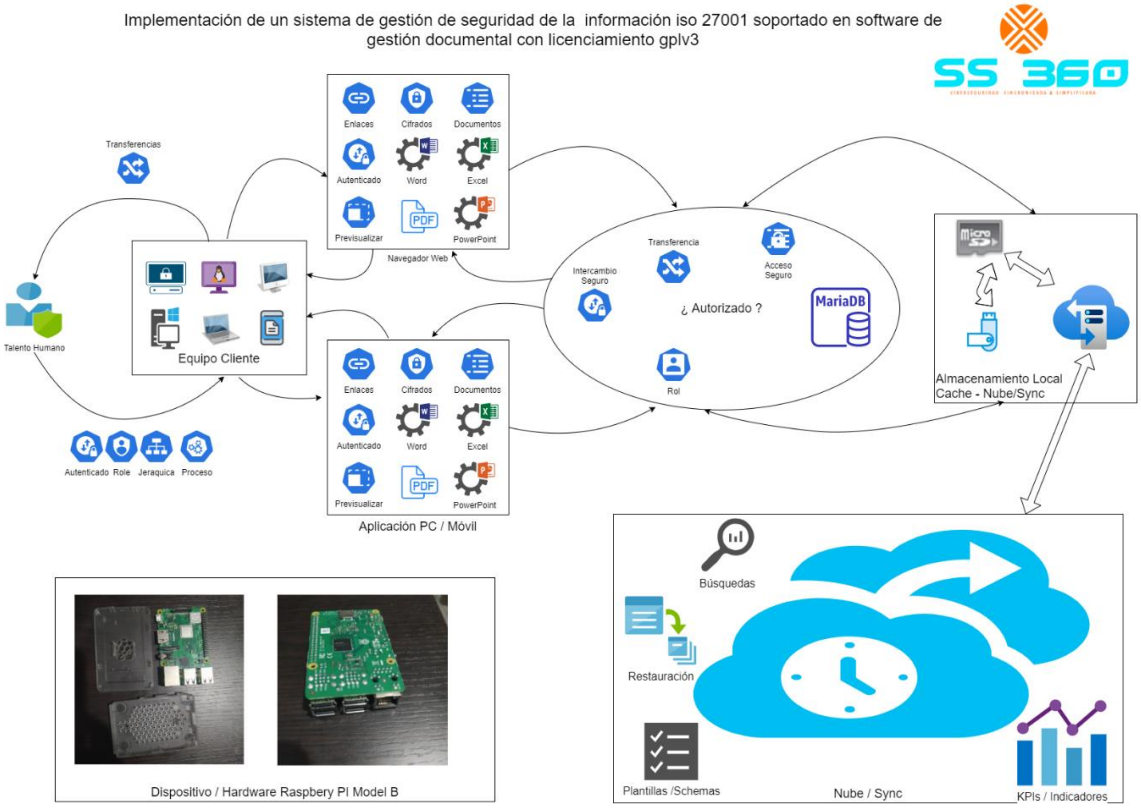
La figura 14, exhibe los componentes clave del sistemas de Gestión Documental del SGSI desarrollado por SS360, su hardware de bajo consumo energético, catalogado como energía verde, al consumir 5 voltios y 2 amperios, conocido como Raspberry Pi, puntalmente el modelo 3B, cuenta con un sistema operativo, su cache y almacenamiento base se alojan en una memoria MicroSD de 16GB, que es también utilizada para el intercambio de datos de usuarios de la red LAN y la sincronización a la nube a seleccionar, adicional se utiliza una memoria USB de 16 GB que utiliza un almacenamiento tipo Linux Ext4 por sus capacidades de verificación de errores o generar instantáneas de volúmenes lógicos que permiten la recuperación de los datos.

Al utilizar el almacenamiento Ext4 es imperativo que el sistema operativo es de tipo Linux y derivado de Debian, como parte de los mecanismos de Hardening aplicados al hardware en los componentes de la Raspberry PI 3B, se deshabilito la irradiación WIFI y Bluetooth incluidos en la placa base.

El talento humano una vez tenga instalada su app de computadora, smartphone o tenga su juego de credenciales para acceder al entorno web y cree, modifique, elimine, lea o comparta cualquier fichero o carpeta en el Framework de Gestión Documental del Sistema de Gestión de Seguridad de la Información; dejará una huella de informática que incluso registra las descargas realizadas de la información por medio del enlace de compartir archivos.

Desde su diseño a nivel de arquitectura el proyecto y empresarial fue pensado para obtener la mejor relación costo beneficio para diferentes entidades, siendo estás de cualquier sector de la economía teniendo en cuenta que en tiempos de pandemia a causa del COVID-19 todas las entidades debieron o están en procesos de implementación, despliegue o actualización de la denominada transformación digital en Colombia por el ministerio de las TIC y empresas de todos los sectores de la economía nacional.

Figura 16: Modelado Framework de Gestión Documental del SGSI



Fuente: Propiedad del autor

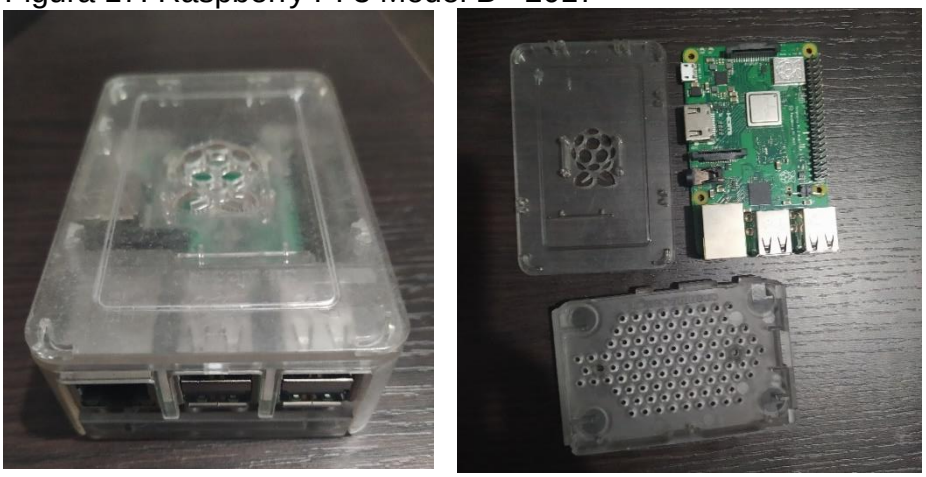
La Figura 16, detalla el diseño de arquitectura y comunicación de los componentes del Framework de Gestión Documental del SGSI, creado como unidad de negocio de la empresa SS360 S.A.S. hacer parte de este proyecto y es propiedad exclusiva del autor.

5.1 COMPONENTES

5.1.1 Hardware

Los dispositivos Raspberry PI, son una placa todo en uno de circuito integrado, ampliamente utilizadas por las comunidades estudiantiles, aficionados tecnológicos o gigantes como Amazon Web Services, su arquitectura ARM o RISC combinada en aglomeraciones de estos dispositivos que operan de forma sincronizada permiten darles vida a contenedores orquestados por Kubernets.

Figura 17: Raspberry PI 3 Model B+ 2017



Fuente: Propiedad del autor

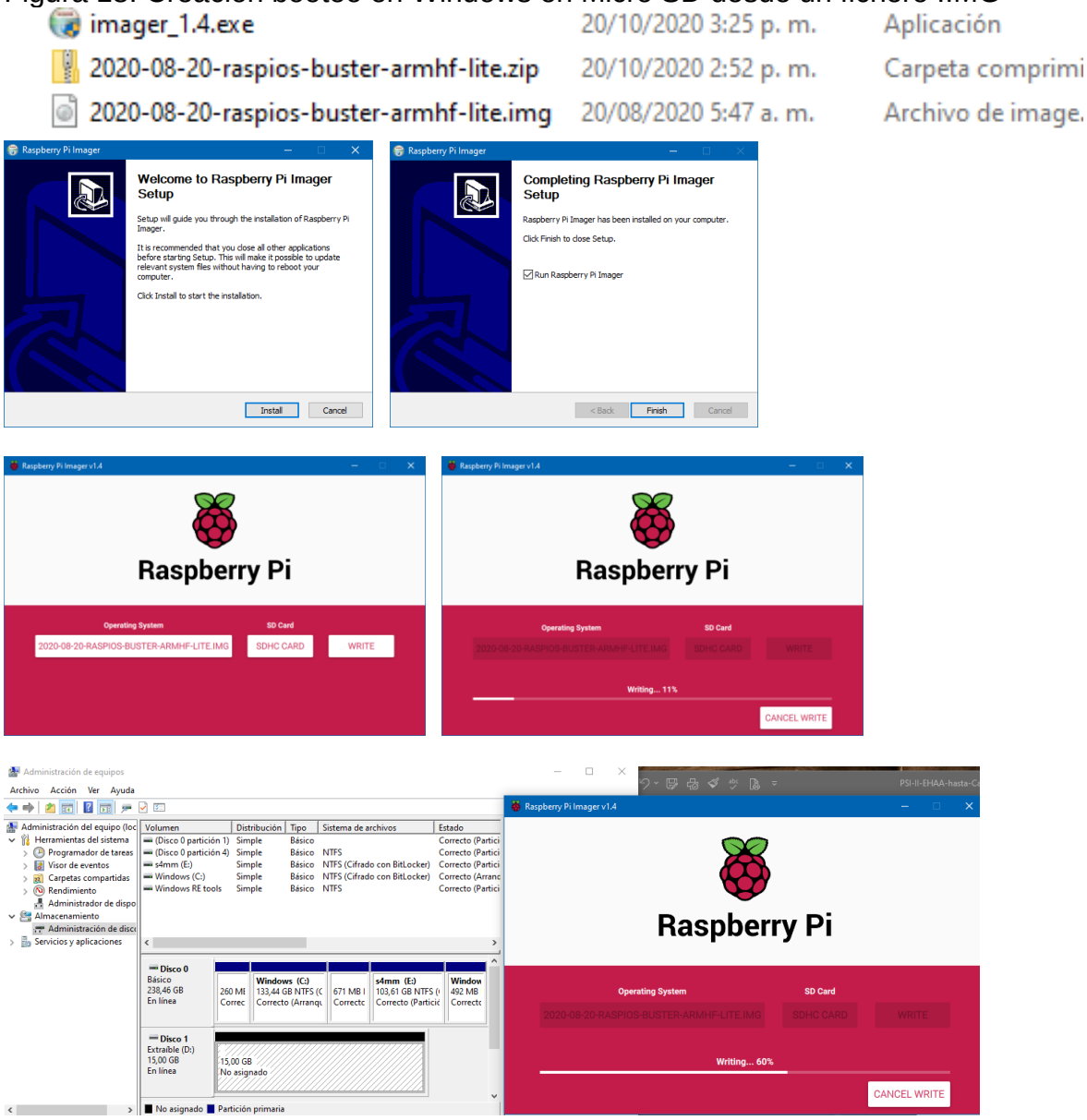
Sus buses/puertos componentes /Chips, necesarios e incluidos en el dispositivo son:

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1GB RAM
- Chip Wireless BCM43438 y Bluetooth de baja energía (BLE)
- Puerto Ethernet 100 Base T
- 4 puertos USB 2.0
- HDMI
- Puerto Micro SD
- Switch de energía Micro USB de 2.5 Amperios

5.1.2 Middleware o Sistema Operativo

Código fuente que interactúa con el hardware del dispositivo, almacenado en una memoria MicroSD, permite que el sistema Operativo basado en Debian y a su vez en Ubuntu, Raspbian GNU/Linux 10, versión lite con paquetería mínima, para interactuar con los buses o puertos de entrada y salida de información o el procesamiento de los datos.

Figura 18: Creación booteo en Windows en Micro SD desde un fichero .IMG

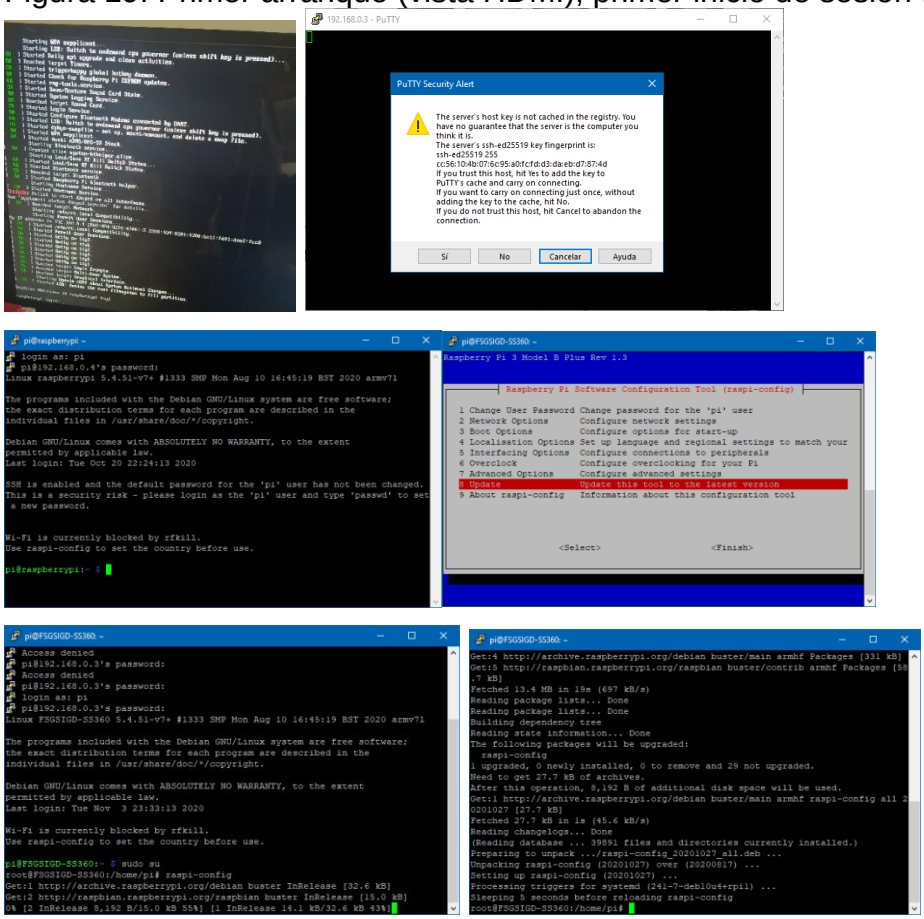


Fuente: Propiedad del autor

5.1.3 Software Fase 1

Cargue de paquetes y componentes base, durante el primer inicio el sistema automáticamente redimensiona y ajusta sus sistema de archivos, realiza un reinicio automático. una vez se han establecido los parámetros de red y servicio SSH utilizando un teclado USB y una pantalla con puerto HDMI con el comando ***Rasp-config,*** posterior podemos acceder por SSH (Conexión remota segura de consola).

Figura 19: Primer arranque (vista HDMI), primer inicio de sesión (SSH)



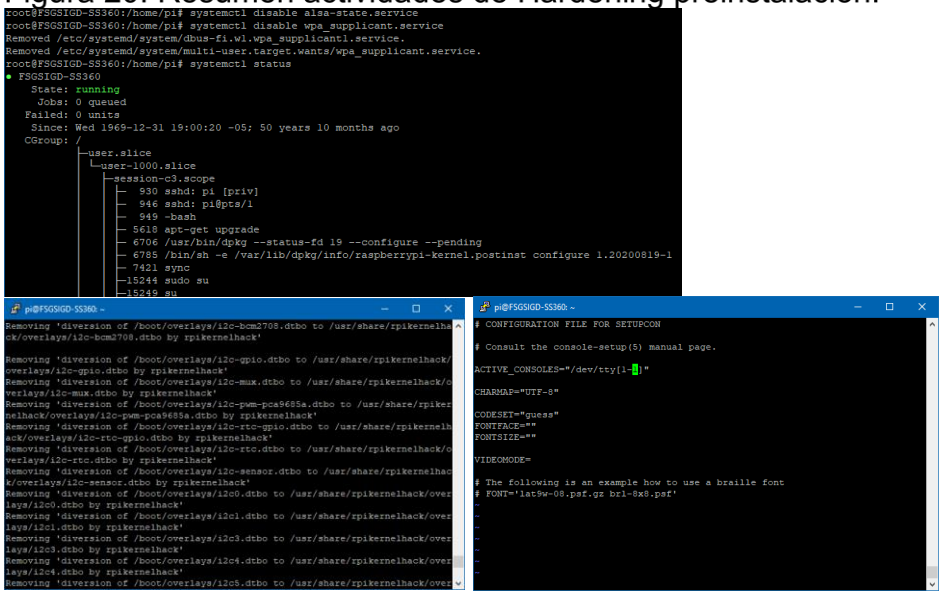
Fuente: Propiedad del autor

El usuario por defecto es pi, su contraseña es: raspberry, se procede con el cambio de credenciales y aplicación de técnicas de Hardening al Sistema Operativo y las aplicaciones por defecto.

5.1.4 Actividades de Hardening preinstalación software base FGD

- Cambio de contraseña de inicio de sesión, nombre del dispositivo en la red y puerto SSH por defecto.
- Acceso remoto por SSH (conexión segura y encriptada de administración remota)
- Configurar Locales para establecer la Zona horaria y distribución del teclado.
- Deshabilita TTY (acceso 'físico' innecesario – CTRL + ALT + [F1 - F7])[62]
- Actualización del sistema operativo y paquetería instalada por defecto.
- Realizar un reinicio del sistema para aplicar cambios.
- Contraseña en el GRUB (Gestor de arranque)[63]
- Cifrado del almacenamiento en MicroSD: Raíz '/' & directorio de usuarios '/home'[64]
- Deshabilitar servicios innecesarios del arranque: Bluethootd, DHCPD, SNMP v1, etc

Figura 20: Resumen actividades de Hardening preinstalación.



Fuente: Propiedad del autor

---

62 Deshabilitar Virtual de las Consolas tty[1-6]. [Consultado 20 noviembre 2020]. Disponible en línea: https://www.enmimaquinafunciona.com/pregunta/54032/deshabilitar-virtual-de-las-consolas-tty1-6

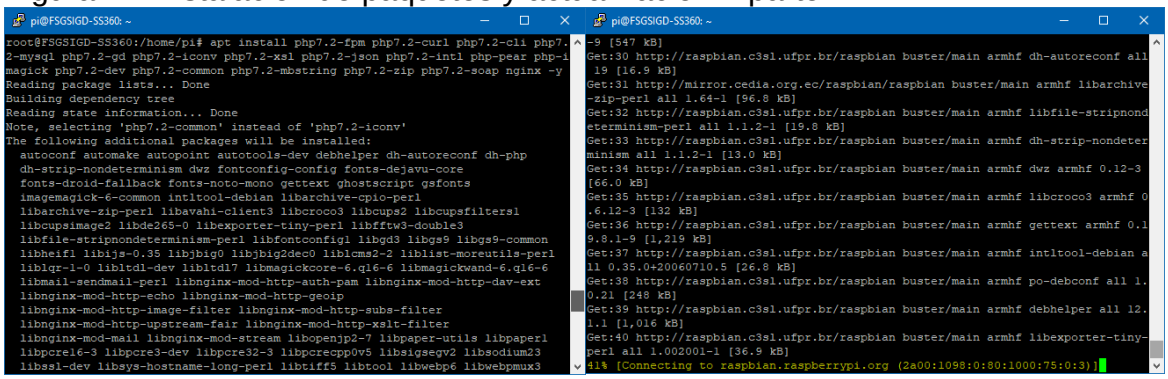
63 Jhon Carles, 2015 Proteger el Grub con Contraseña. [Consultado 20 noviembre 2020]. Disponible en línea en: https://geekland.eu/proteger-el-grub-con-contrasena/

64 Carlo Hamalainen,2017. Raspbian with full disk encryption. [Consultado 20 noviembre 2020]. Disponible en línea: https://carlo-hamalainen.net/2017/03/12/raspbian-with-full-disk-encryption/

5.1.5 Software Fase 2

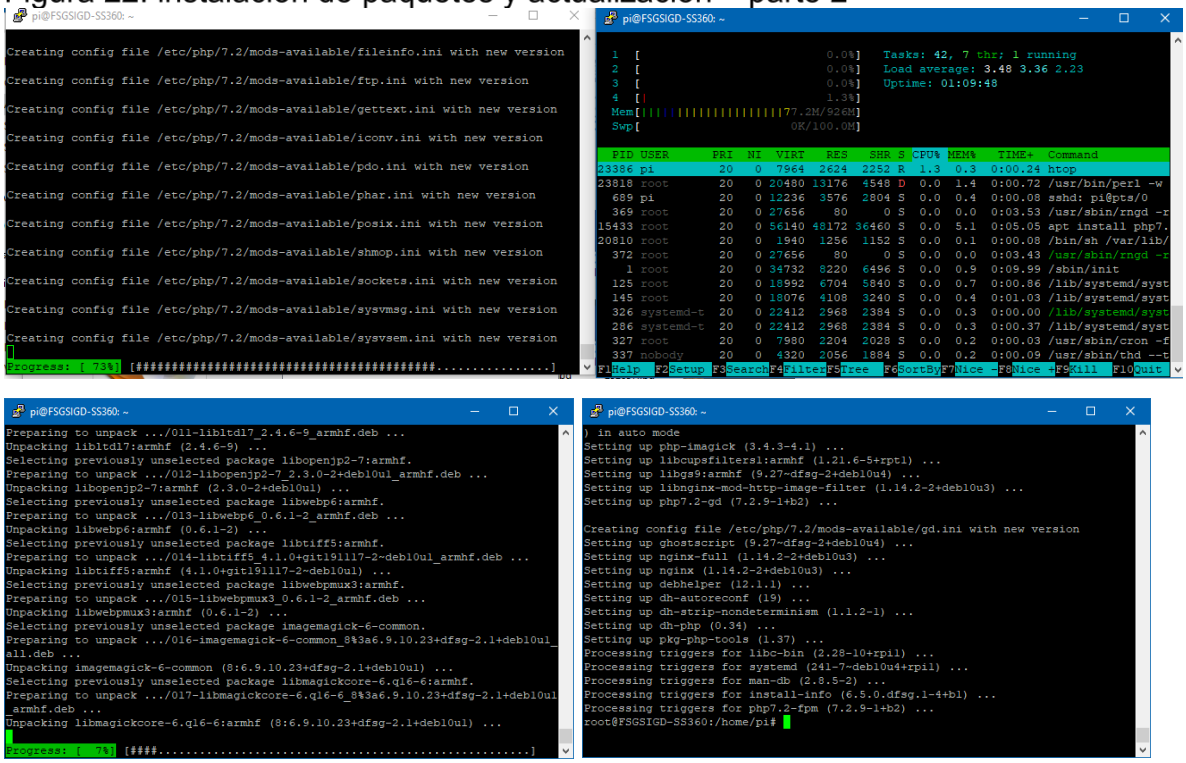
Instalar paquetería necesaria para crear sistema de gestión documental, interfaz web y app para pc Windows o Linux o móviles tipo Smartphone:

Figura 21: instalación de paquetes y actualización – parte 1



Fuente: Propiedad del autor.

Figura 22: instalación de paquetes y actualización – parte 2



Fuente: Propiedad del autor.

Los comandos utilizados para ayudar en la edición de archivos, actualizar la base de datos de los repositorios, instalar, arrancar y habilitar en el inicio el servicio Nginx, son:

echo "alias 'vim=vim.tiny'" >> /root/.bashrc

echo "alias 'vim=vim.tiny'" >> /home/pi/.bashrc

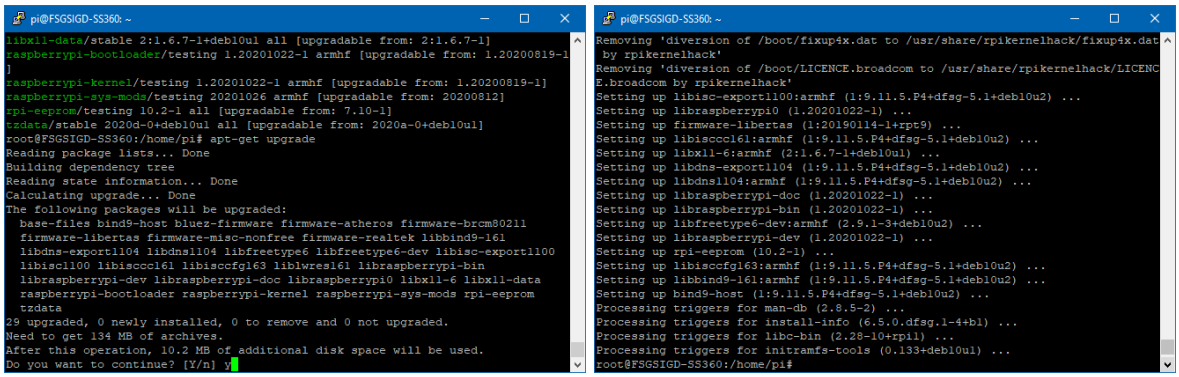
sudo apt update

sudo apt install nginx -y

sudo systemctl start nginx

sudo systemctl enable nginx

Figura 23: Actualización del Sistema Operativo.

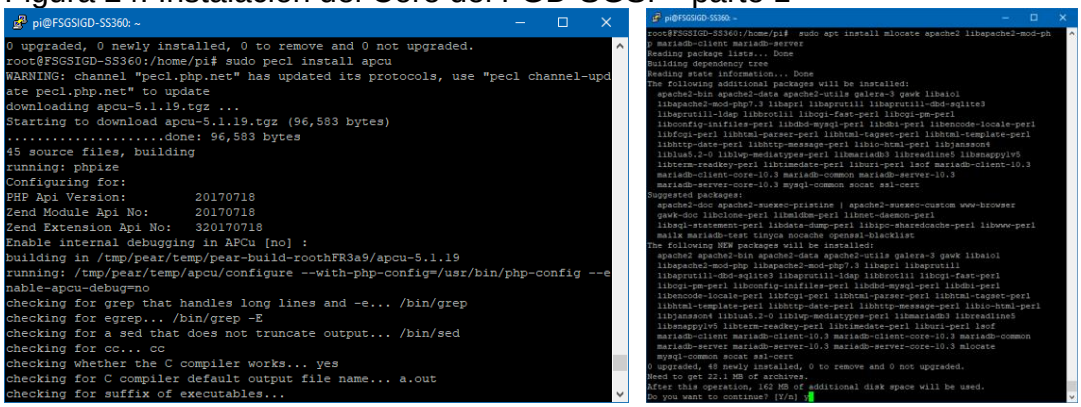


Fuente: Propiedad del autor.

5.1.6 Instalación GD

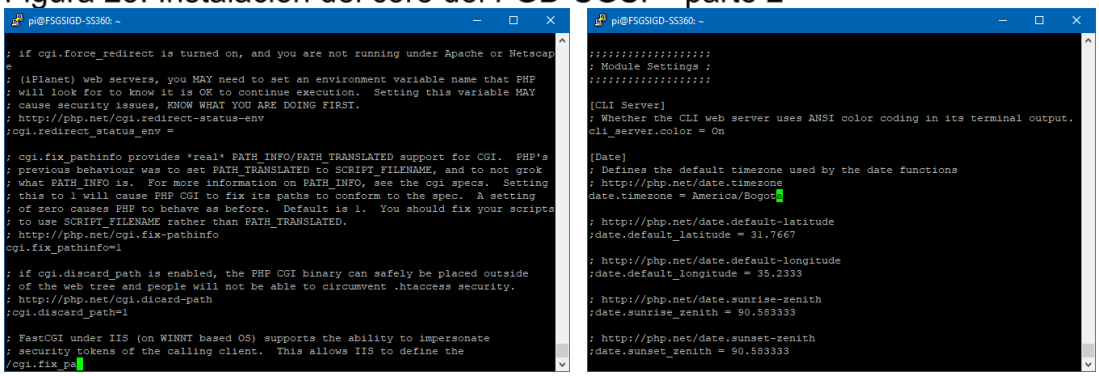
Una vez el sistema Operativo y sus aplicativos base estén correctamente actualizados, procedemos con el inicio de la instalación de los servicios NGINX y PHP, los cuales se encargarán de mostrar la interfaz web a los usuarios. Posterior se deben tunear los ficheros base del PHP, para agregar optimización y compatibilidad con el Sistema de Gestión Documental - GD. Lo anterior podemos observarlo en las figuras 25 y 26

Figura 24: Instalación del Core del FGD-SGSI – parte 1



Fuente: Propiedad del autor

Figura 25: Instalación del core del FGD-SGSI – parte 2



Fuente: Propiedad del autor

La edición del fichero www.conf de PHP, mediante el comando vim, en la ruta: 7.2/fpm/pool.d/www.conf, se realiza des comentamos todas las siguientes líneas (Casi al final del fichero):

env[HOSTNAME] = $HOSTNAME

env[PATH] = /usr/local/bin:/usr/bin:/bin

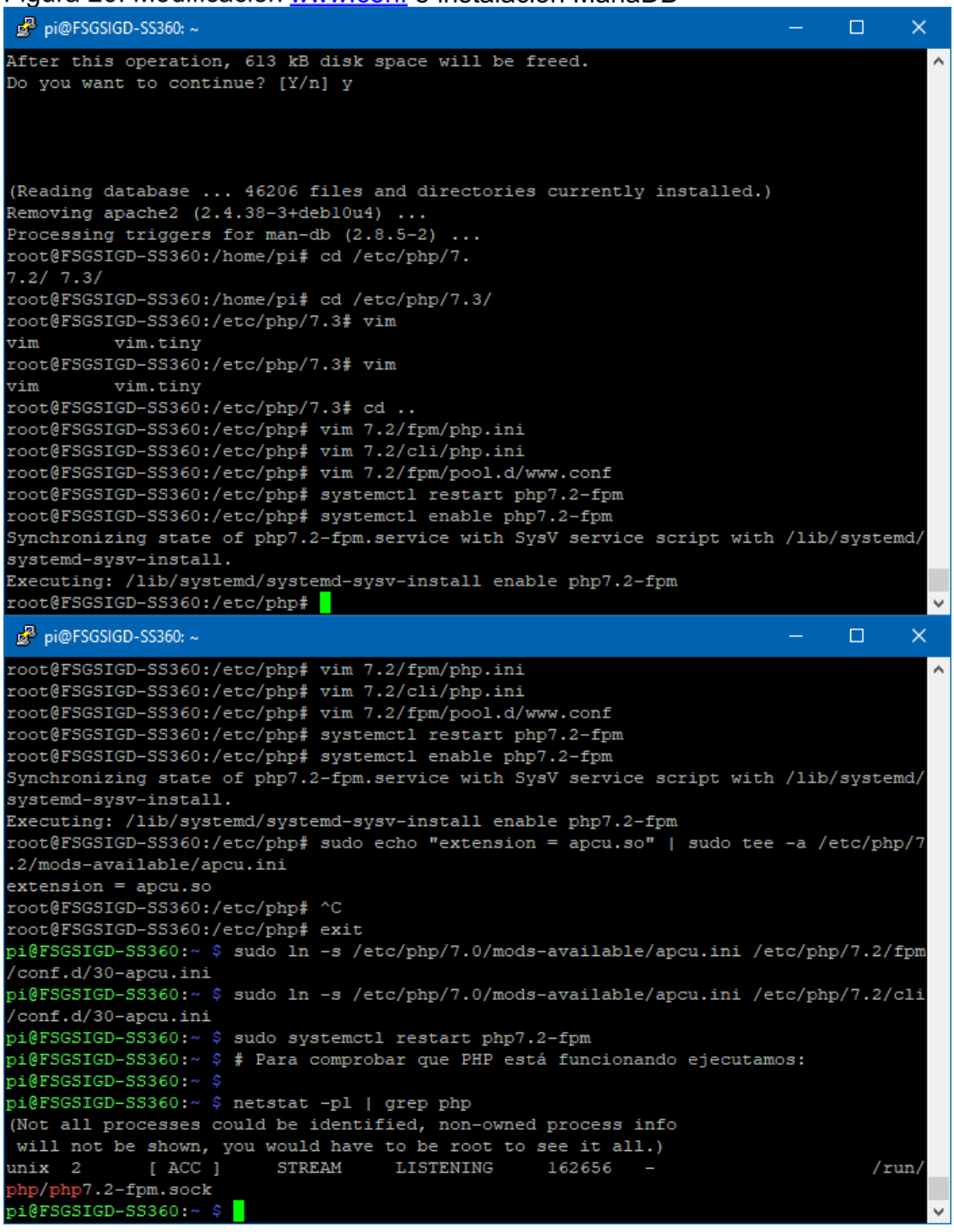
env[TMP] = /tmp

env[TMPDIR] = /tmp

env[TEMP] = /tmp

Una vez guardados los cambios realizados en el fichero se vuelve necesario realizar un reinicio del servicio PHP y su activación, como lo presenta la figura 26, donde posteriormente se realizará el proceso de instalación del server de base de datos escogido, para este proyecto en particular se utiliza María DB por ser liviano en cuanto al consumo de recursos y es recomendado por el equipo desarrollador del componente principal de software a utilizar por el FGD-SGSI.

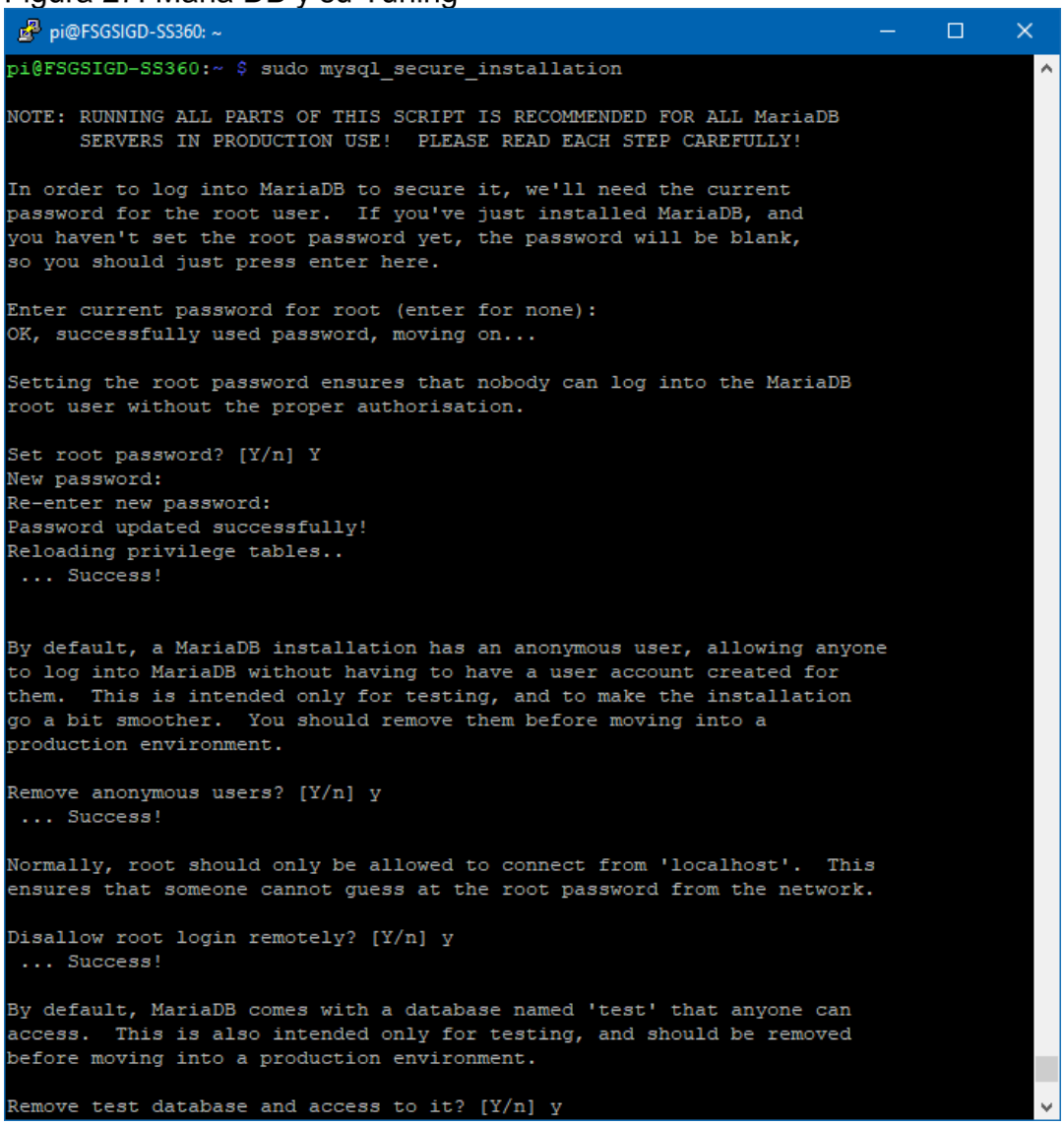
Figura 26: Modificación www.conf e instalación MariaDB



Fuente: Propiedad del autor

En la instalación y aseguramiento básico de Maria DB, hemos establecido inicialmente la contraseña del ROOT, posterior se elimina el login de usuarios anónimos, continuando con el bloqueo de acceso remoto del ROOT, por último, se remueve el acceso a la Base de datos “test”, la cual puede ser utilizada con otros fines a las contempladas por los desarrolladores.

Figura 27: Maria DB y su Tuning



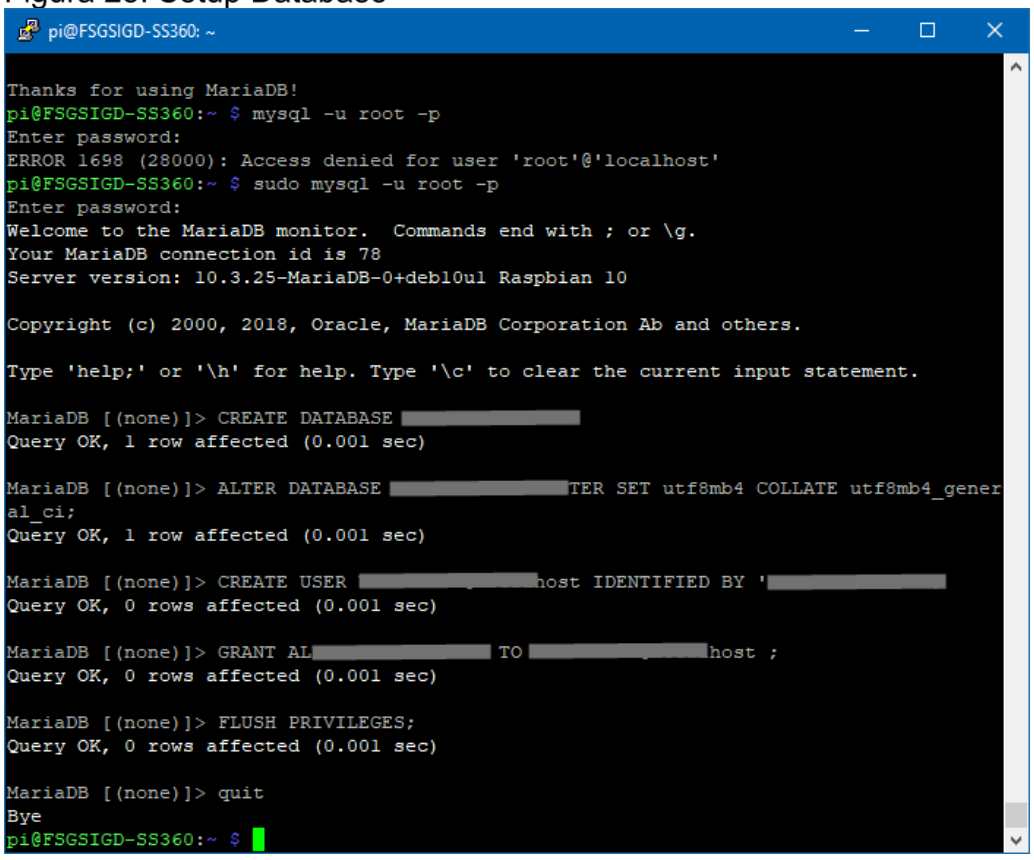
Fuente: Propiedad del autor

Trabajando con María DB, en la creación de tablas, usuario y asignación de privilegios, por ejemplo:

Colocamos la contraseña que le pusimos a root en MariaDB y una vez dentro ejecutamos lo siguiente:

CREATE DATABASE *********;
ALTER DATABASE c0labor4 CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE USER *********@localhost IDENTIFIED BY '*********';
GRANT ALL on *********.* TO *********@localhost ;
FLUSH PRIVILEGES;

Figura 28: Setup Database



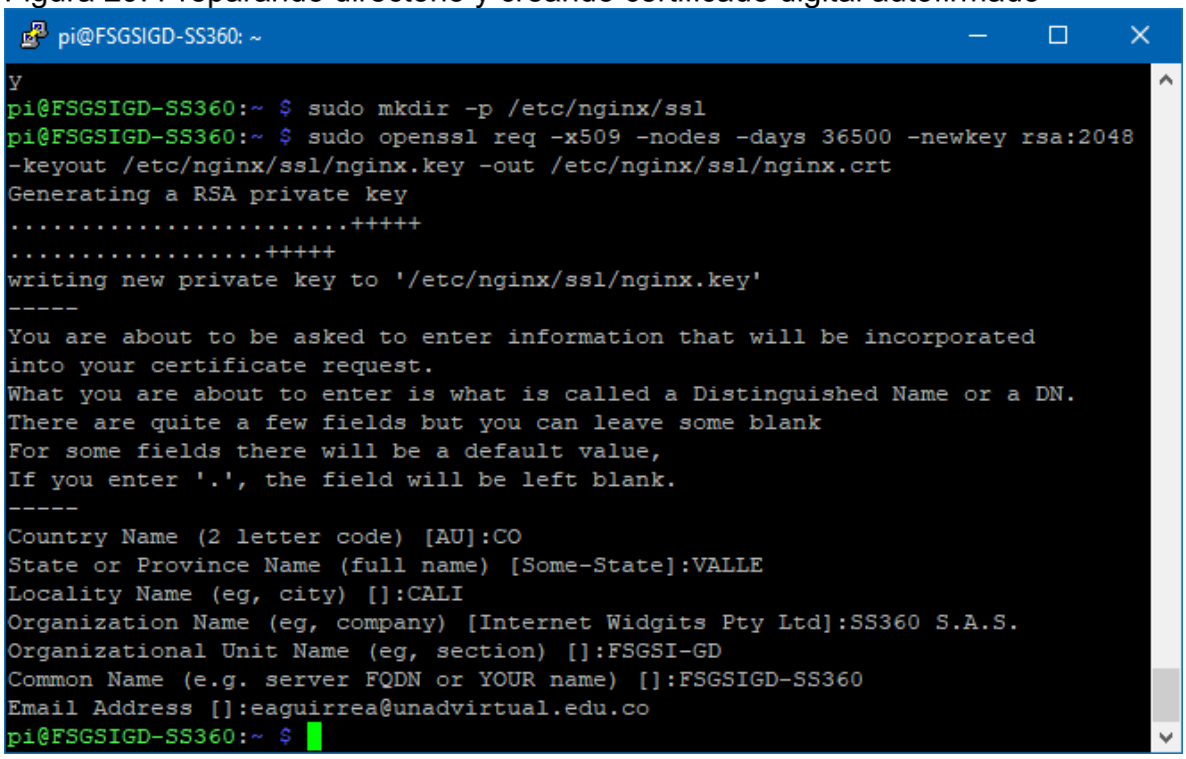
Fuente: Propiedad del autor

Posterior debemos detener el servicio web de Nginx, con el comando:

$ sudo systemctl stop nginx

Y luego ejecutamos los siguientes comandos junto a los parámetros adecuados:

Figura 29: Preparando directorio y creando certificado digital autofirmado



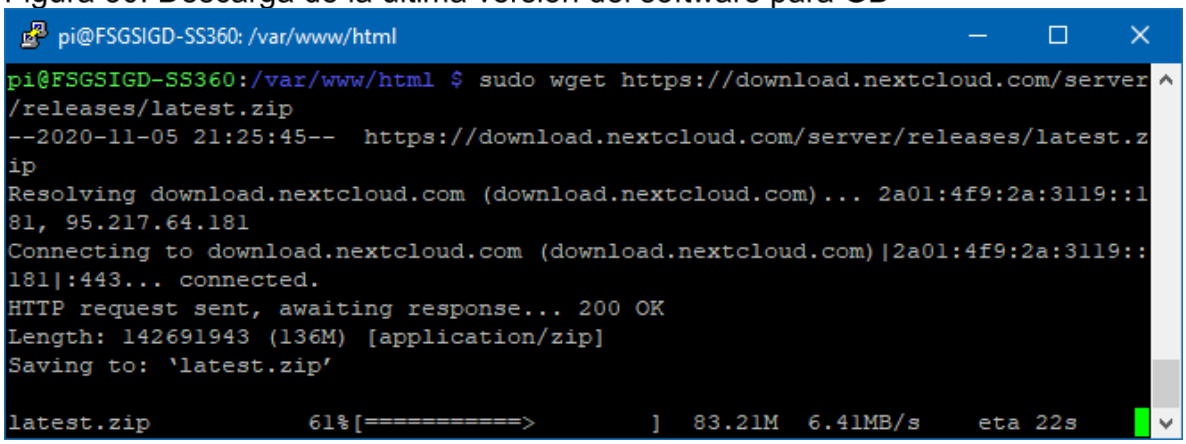
Fuente: Propiedad del autor

En la figura 29 notamos el proceso de creación de un certificado digital auto firmado con una vigencia de 36.500 días, clave RSA (algoritmo/forma de cifrado) de 2048 bites, La llave nginx.key y su verificador nginx.crt se almacenarán en la ruta previamente creada '/etc/nginx/ssl/'

Vamos a instalar Nextcloud, como software de Gestión Documental, pero primero un par de utilidades necesarias ejecutando el comando:

$ sudo apt install wget unzip zip -y

Figura 30: Descarga de la última versión del software para GD



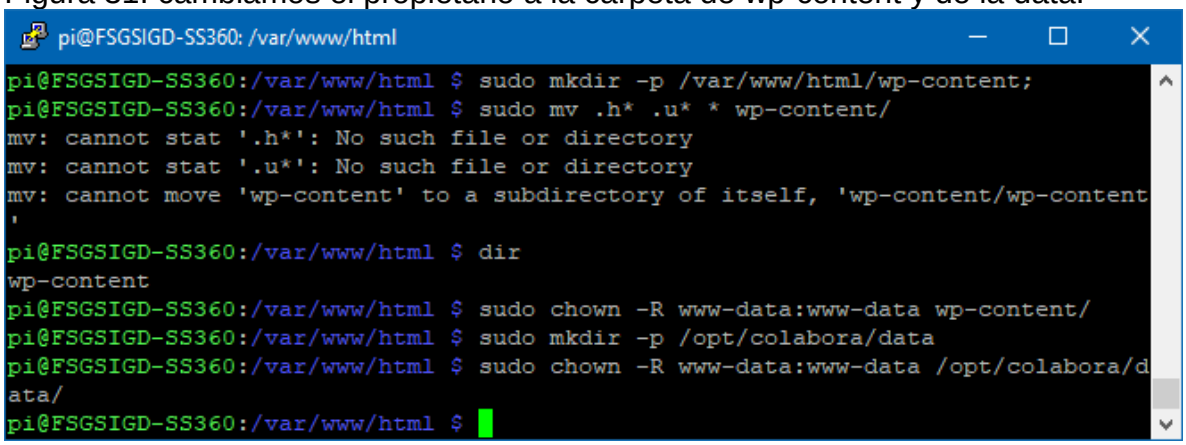
Fuente: Propiedad del autor

Lo descomprimimos y creamos la carpeta data donde irán nuestros ficheros, con los comandos:

$ sudo unzip latest.zip

$ sudo rm latest.zip

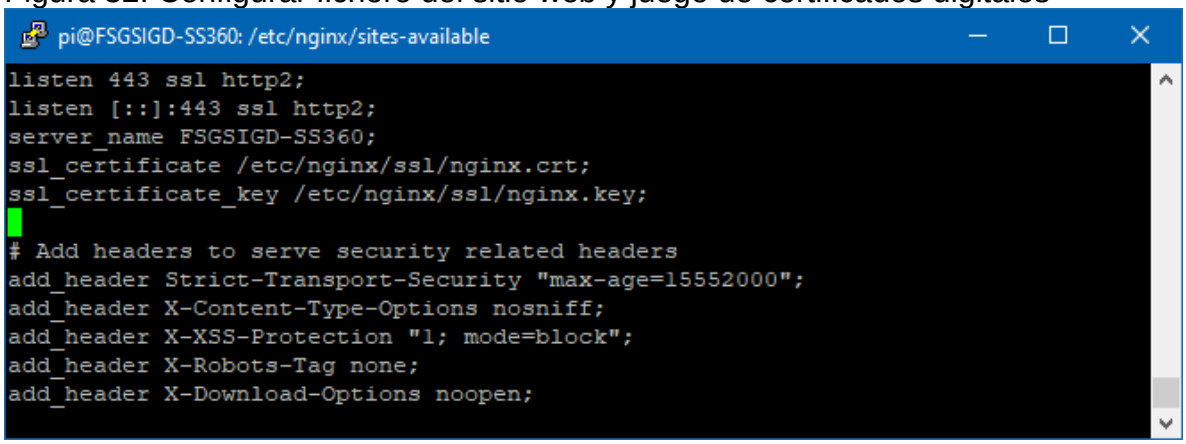
Figura 31: cambiamos el propietario a la carpeta de wp-content y de la data:



Fuente: Propiedad del autor

Configuración server nginx, resulta necesario cerrar el acceso por el puerto 80 comúnmente asociado al protocolo inseguro HTTP y dejar habilitado únicamente el puerto 443 asociado al protocolo web de comunicación segura HTTPS, donde utilizamos el certificado digital generado y auto firmado para cifrar el enlace de conexión web entre el servidor y el navegador web del talento humano que se conecte, ese mismo certificado servirá para cifrar la comunicación desde la App PC o Móvil en cualquier caso.

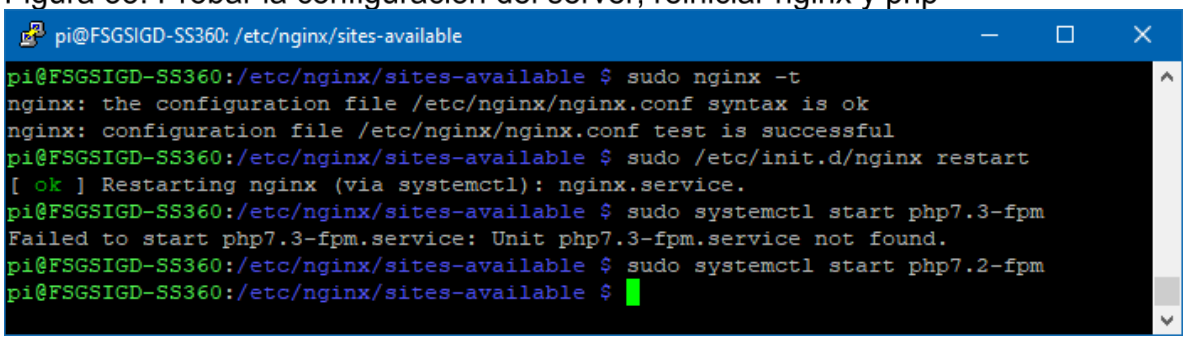
Figura 32: Configurar fichero del sitio web y juego de certificados digitales



Fuente: Propiedad del autor

En ocasiones quedan ‘basuritas’, ‘comas’ o caracteres no deseados en los ficheros de configuración d ellos servicios que evitan que nos funciones y se logran convertir en un dolor de cabeza, por lo cual ejecutaremos la utilidad ‘nginx -t’, en la figura 24 presentamos el proceso, validando que la configuración se correcta y las rutas de directorios o variables sea la adecuada.

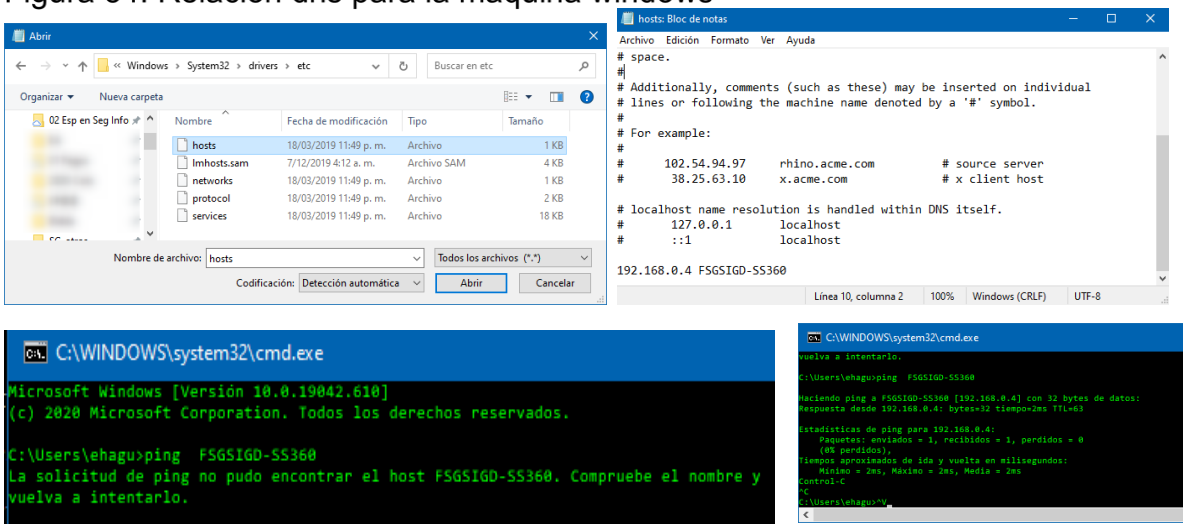
Figura 33: Probar la configuración del server, reiniciar nginx y php



Fuente: Propiedad del autor

En este punto ya podremos acceder al entorno web y realizar la configuración del servidor, comunicándolo con la base de datos; En el siguiente fichero: *C:\Windows\System32\drivers\etc\hosts,* del sistema operativo Windows* encontramos la relación entre nombres de dominio o Host y direcciones IP de forma manual, para forzar a que la computadora resuelva nuestro entorno de laboratorio. En la figura 25 presentamos la relación entre la dirección IP LAN y el nombre de dominio dado al proyecto.

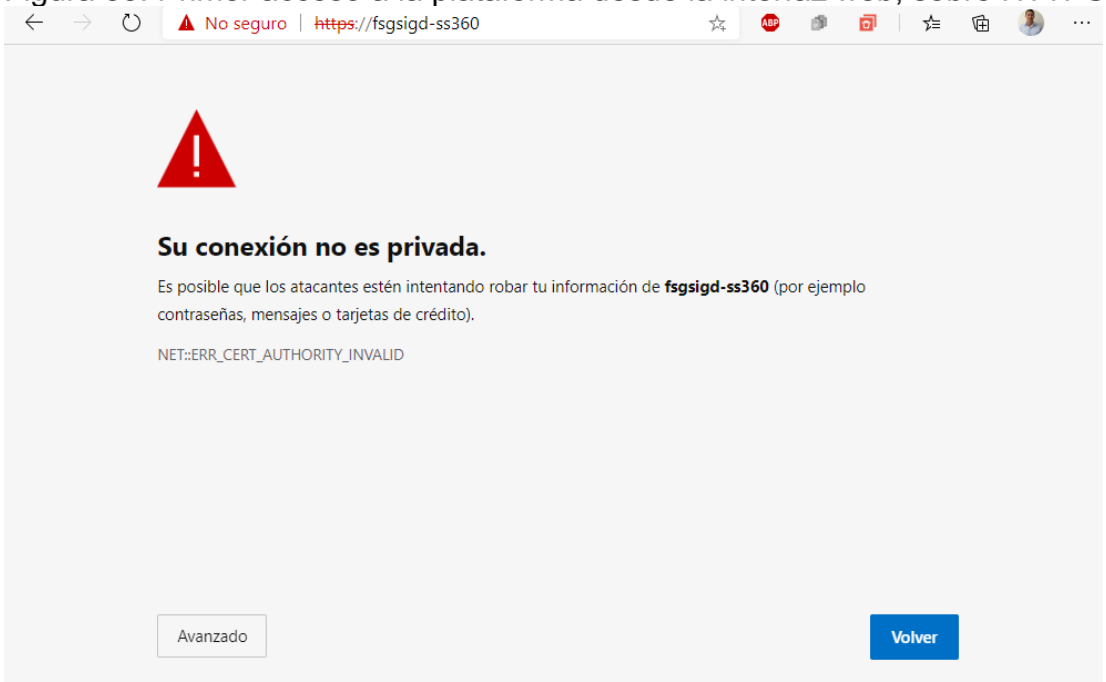
Figura 34: Relación dns para la maquina windows



Fuente: Propiedad del autor

Recientemente tuve un cambio de modem del proveedor de Internet, resultando en la pérdida del acceso a su administración y como tal a la posibilidad de hacer redirección al puerto 443 del dispositivo Raspberry PI 3, imposibilitando la habilitación de un certificado digital reconocido y aceptado por las entidades certificadoras raíz de confianza, por tal razón vemos en la figura 26 el mensaje de advertencia.

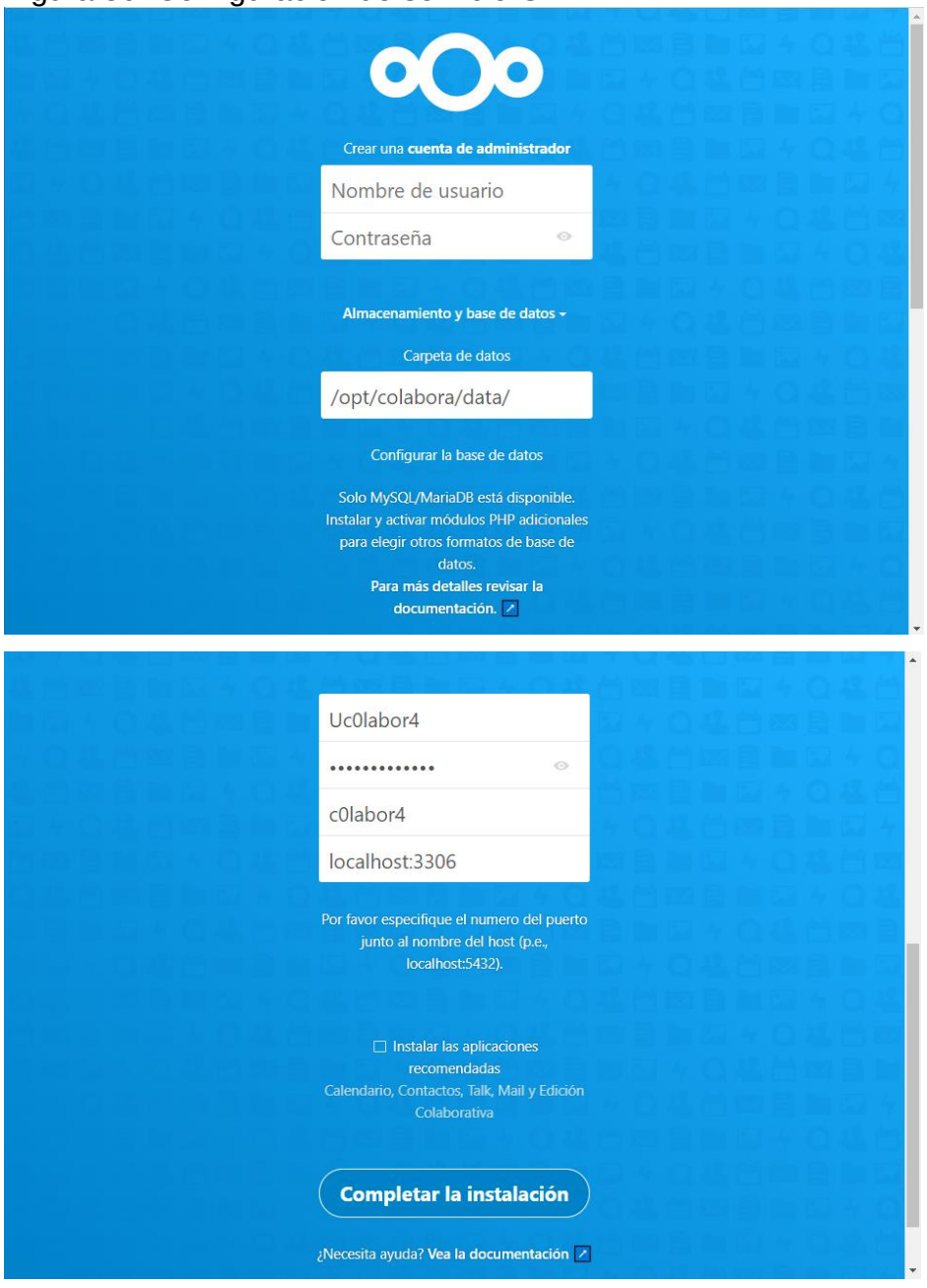
Figura 35: Primer acceso a la plataforma desde la interfaz web, sobre HTTPS.



Fuente: Propiedad del autor

Configuración de usuario administrador, directorio donde se almacenará la data del sistema de Gestión Documental, posterior se deben configurar los parámetros de acceso a la base de datos de Maria DB.

Figura 36: Configuración de servicio GD

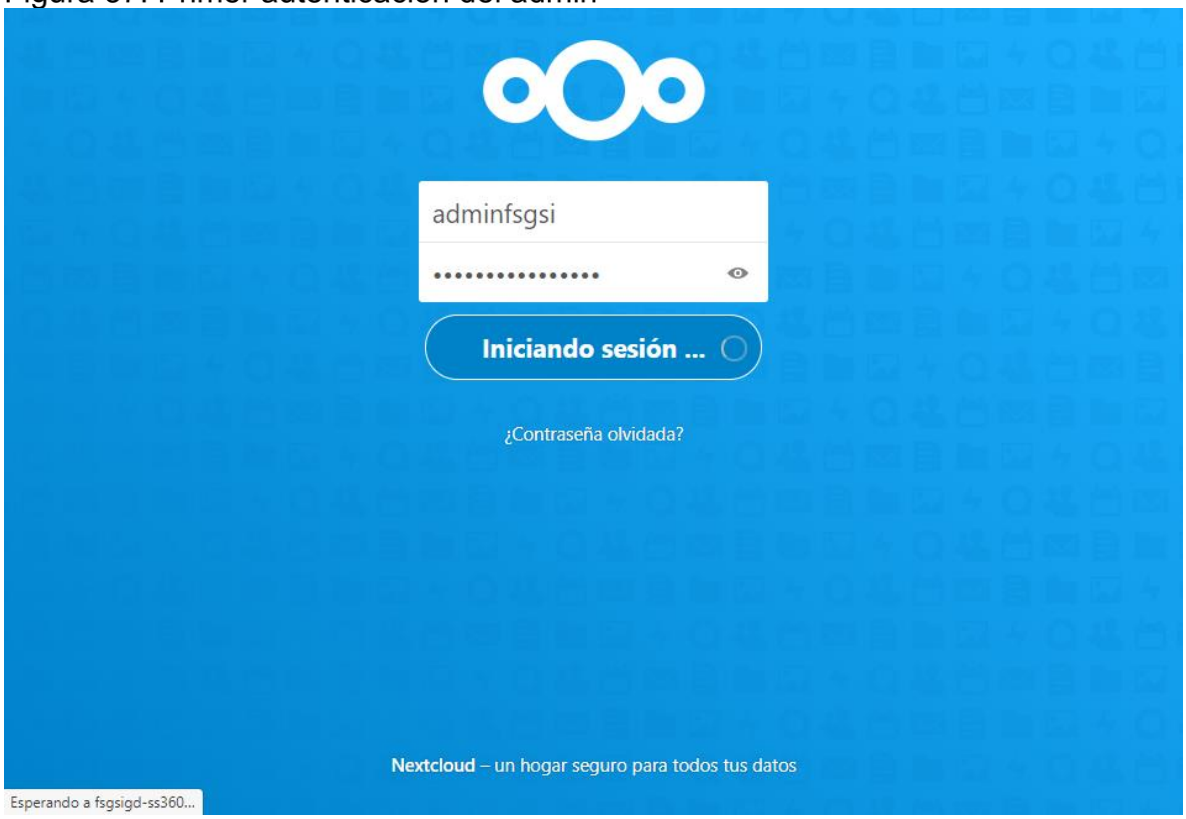


Fuente: Propiedad del autor

La figura 36 presenta la interfaz en su primera configuración, donde se asocia la ruta de almacenamiento de la información y conexión con la base de datos María DB, es importante fijar el puerto de escucha del servicio SQL.

El proceso de finalización de la primera configuración puede tardar unos 5 minutos aproximadamente, debido a que por detrás está realizando la creación de tablas y registros de la base de datos, al igual va preparando el entorno de trabajo para que el administrador del sistema pueda crear usuarios, definir roles, crear directorios base y asignar los respectivos permisos. La figura 37 muestra la interfaz de inicio de sesión para usuarios o administradores.

Figura 37: Primer autenticación del admin



Fuente: Propiedad del autor

5.1.7 Algunas técnicas de Hardening aplicadas

- Tuneo Base de Datos
- Habilitación de certificado SSL
- IPv6 Disable[65]
- Montaje se dispositivo USB en el arranque del sistema[66]

5.1.8 *Plantillas

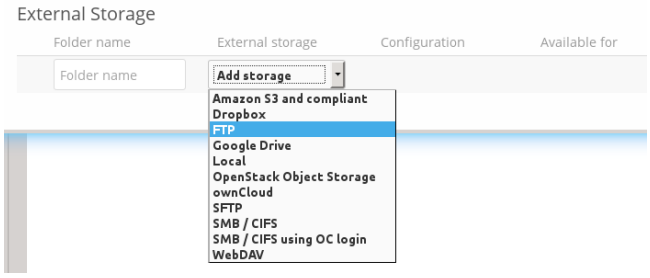
5.1.9 *Definir Roles y Creación de usuarios

5.2 SINCRONIZACIÓN A LA NUBE PÚBLICA O PRIVADA

Podemos afirmar que el trabajo colaborativo y la sincronización de la información han ido relegando a las copias de seguridad al estar estas inmersas en sobre los documentos que trabajamos en el día a día de tipo ofimáticos como, por ejemplo: Word, Excel, PowerPoint, entre otros.

Desde la perspectiva de un usuario final que ha guardado su información de trabajo en la carpeta vigilada por el agente que se instaló en su computadora o smartphone; este agente automáticamente sincroniza los datos hacia el framework de gestión documental del SGSI. Posterior se inicia sincronización hacia la o las nubes informáticas de almacenamiento externo que fueron habilitadas, mediante el montaje de servicios de almacenamiento externo, como, por ejemplo: Google Drive, Dropbox, Amazon S3, servidores de archivos tipo SMB / CIFS y servidores FTP en el Framework de gestión documental. El administrador del servidor puede controlar cuáles de estos están disponibles para el uso de las organizaciones, (ver figura 39).

Figura 38: Configuración almacenamiento externo.



Fuente: Propiedad del autor

---

65 ITSFOSS. Disable IPv6. [Consultado 20 noviembre 2020]. Disponible en línea: https://itsfoss.com/disable-ipv6-ubuntu-linux/

66 Linux Hint. mount_partition_uuid_label_linux. [Consultado 20 noviembre 2020]. Disponible en línea https://linuxhint.com/mount_partition_uuid_label_linux/

6. PLAN DE MEJORA CONTINUA PARA LA EMPRESA SEGURIDAD SINCRONIZADA 360 (SS360)

Tal como lo mencionamos introductoriamente en el capítulo 5 y figura 13, es necesario partir de las bases y firmeza que entrega el ciclo Deming, el cual ha sido ampliamente aceptado por la comunidad local, nacional e internacional de seguridad de la información, que utiliza o se basa en la norma ISO 27001:2013 o sus versiones anteriores. En este capítulo recalcaremos la importancia de sus 4 fases continuas, tipo bucle.

El ciclo PDCA (o PHVA en español) es la herramienta de mejora continua, diseñada y creada por el Dr. Walter Shewhart en el año 1920 y fue presentada por Edwards Deming desde el año 1950, está se compone de cuatro pasos que forman el ciclo (Díaz, 2010). Plan (planificar), Do (hacer), Check (verificar) y Act (actuar), estos se describen ligeramente y en pasos continuos conformando el ciclo de Deming (Aliaga, 2013).

La metodología ciclo Deming o PDCA, en un sistema de gestión de seguridad de la información o SGSI, facilita el descubrimiento de los puntos débiles o vulnerables de una entidad y generando valiosas herramientas que permiten diseñar procedimientos y procesos de seguridad cada vez más eficaces. [67], ampliando un poco más sus alcances, tenemos:

Planear

- Dejar a la suerte o azar los quehaceres primordiales significa abrir o mantener brechas de seguridad que aprovecharan los delincuentes informáticos, planear es sinónimo de pensar a futuro dentro del contexto que hemos venido definiendo.
- Se planea con base a objetivos definidos por la junta directiva, las demandas del mercado y en pro de lo que se desea como compañía, su prestigio o también llamado renombre.

Hacer

- El No ejecutar el plan de acción definido previamente significa que hemos perdido el tiempo y/o no estamos dándole la prioridad necesaria por tener otras premuras a nivel corporativo, lo cual es sinónimo de una alta gerencia poco comprometida con la seguridad informática de su organización,

[67] Bustamante Maldonado, G., & Osorio Cano, J. A. (2015). Metodología de la seguridad de la información como medida de protección en pequeñas empresas.. Disponible en línea: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.B067139B&lang=es&site=eds-live&scope=site

empleados, clientes y proveedores quedarán desprotegidos o en lo que he denominado el limbo informático.

- Los lineamientos definidos por la auditoría y controles a establecer según la fase de planeación deben ejecutarse, de manera sistemática y enfocada en la consecución de los objetivos planteados durante el inicio del despliegue del SGSI.

Verificar

- Llegando al paso donde se realiza la respectiva evaluación o reevaluación de los pasos anteriores como parte de un ciclo continuo, se debe medir el desempeño de los objetivos de seguridad, del proceso y el cumplimiento de las políticas de seguridad, así como el debido reporte a la dirección de la entidad.
- Asegurarse que los mecanismos definidos en la fase de planeación y ejecutados en la fase de hacer fueran ejecutados de la mano de las mejores prácticas y se esté dejando documentación actualizada de los nuevos cambios, que sirven como insumo en las siguientes fases del ciclo Deming.

Actuar

- Una vez se ha planeado, se ejecutó y verifico la planeación, es necesario determinar el porcentaje de objetivos cumplidos acorde las directrices entregadas por la Alta Gerencia.
- Llevar a cabo cada uno de los objetivos, establecer y dar seguimiento a los controles de seguridad de la información definidos en el SOA y afianzando el PTR para reducir los riesgos en los activos informáticos que fueron identificados y catalogados mediante la metodología Magerit.

6.1 CAPACITACIONES PROGRAMADAS A TODO EL PERSONAL

Si bien, hoy en día la gran mayoría de empresas del sector privado. Gubernamental o sin ánimo de lucro han ido tomando conciencia de los beneficios al tener personal técnico o que utilice e interactúe en su día a día con tecnologías de la información y comunicación, es decir desde la persona que utiliza un smartphone que se conecta a la red corporativo o de invitados de la organización debería conocer la gran mayoría de recomendaciones mínimas para acceder o utilizar algunas de las herramientas cotidianas como son:

6.1.1 Aplicaciones o tráfico esperado en una red en estos días

- Redes sociales (Facebook, Twitter, Instagram, WhatsApp, etc)
- Productividad empresarial: (Correo electrónico, Intranet corporativa, acceso por VPN, Escritorio Remoto
- Multimedia: (YouTube, Vimeo, Radio en línea, etc)

- Protocolos básicos de intercomunicación LAN o hacia Internet: (DNS, DHCP, HTTPS, similares)
- La programación de espacios de capacitación interna o por entidades expertas en la materia reduciría ampliamente la brecha existente que ha venido beneficiando a los delincuentes informáticos por el desconocimiento de los usuarios finales, por ejemplo, en técnicas de ataque de Phishing (robo de información “usuarios, contraseñas”, es decir correos electrónicos que simulan ser emitidos para entidad que están suplantando para crear portales de autenticación o solicitud de información falsa que es capturada por el delincuente informático quien tuvo mucho tiempo para establecer sus estrategias de ataque y recolección de información para avanzar a su siguiente fase que generalmente a punta a desplegar un ataque de Ransomware una vez han logrado acceder al sistema y conseguir elevar sus privilegios.
- En Seguridad informática el dicho que dicta, “La cadena se rompe por el eslabón más débil” siempre se ha ido comprobando, sabemos que los atacantes se aprovechan de los usuarios con poco conocimiento sobre cómo identificar o reaccionar ante un correo electrónico aparentemente legitimo o enviado por un remitente desconocido, por citar un ejemplo común sobre la importancia de estar en constante capacitación.

6.1.2 Recomendaciones básicas para usuarios finales

- No abrir correos electrónicos de remitentes desconocidos.
- No permitir la visualización de imágenes en los correos.
- No dar clic en los enlaces si no estamos seguros de la confiabilidad del remitente.
- No abrir o descargar archivos adjuntos de remitentes de dudosa reputación.
- No abrir, ni permitir habilitación de contenido o macros en archivos de Word, Excel, Power Point.
- El mantener actualizados sus aplicativos y dispositivos móviles, hacen parte de las responsabilidades compartidas entre el área de TI/Seguridad y los usuarios finales.
- No utilizar la misma contraseña en todas las Aplicativos, sitios web o plataformas tecnológicas

CONCLUSIONES

- Los pilares de la seguridad informática resultan de vital importancia y son fundamentales en el desarrollo de este proyecto, al englobar los criterios base para garantizar la gestión de roles y permisos sobre la información que se almacena en el framework.
- Las técnicas de hardening, doble factor de autenticación, cifrado de la información, acceso seguro. al final terminan siendo capas adicionales de seguridad que le agregamos al sistema para proteger la información embebidas dentro de la metodología de la Norma ISO 27001:2013.
- EL ciclo Deming o de mejora continua es parte de la columna vertebral del SGSI, al igual que los varios mecanismos, procesos o rutinas bases implementadas en el framework de gestión documental.
- El talento humano y su rol sobre la información o la forma en la que interactúa con ella deja siempre una huella de auditoria que fácilmente permite identificar qué pasó con un fichero en determinado momento, como parte de la No Irrefutabilidad.
- Mantener actualizados e identificados los activos informáticos facilitará la correcta gestión del riesgo y adopción del SGSI en la organización dentro del marco de Gestión Documental – GD
- Mediante las capacitaciones y simulacros se va fortaleciendo el nivel de conocimiento en general del talento humano de cualquier organización, logrando reducir la brecha de seguridad informática; Brecha que es brutalmente aprovechada por los delincuentes informáticos.
- Trabajar con versiones obsoletas puede generar agujeros de seguridad, de igual manera tampoco es recomendable trabajar con la última versión disponible, generalmente tienen bugs o fallos de programación no identificados por los desarrolladores.
- Los nuevos mecanismos de autenticación y seguridad desplegada en apache 2.4, son un impedimento para la autenticación o primer login del framework a fecha de hoy 1711/20, hace unos 9 meses funcionaba bien al seguir las múltiples guías que había desarrollado como unidad de negocio, al final despliegue una imagen de Docker que facilito todo el despliegue.

RECOMENDACIONES

- Establecer políticas de seguridad de la información para los usuarios de la entidad acorde a sus roles propendiendo por que se garanticen los pilares de la seguridad informática.
- Realizar auditorías internas o externas enfocadas en determinar si se están respetando y aplicando adecuadamente los controles establecidos para garantizar los pilares de la seguridad informática.
- Realizar seguimiento cada trimestre al avance de los procesos del SGSI de acuerdo con el plan estratégico de la organización.
- Actualizar cada 6 meses el inventario de activos y gestión del riesgo haciendo seguimiento al cumplimiento, resolución de las No conformidades indicadas por la auditoría.
- Toda la organización debe ser parte del proceso en mayor o menor medida al igual que el ciclo Deming es parte crucial para todos.
- Los procesos y programación de capacitaciones deben ser un habitó constante al menos 2 capacitaciones generales por trimestre.
- Se debe de revisar periódicamente las bases de datos públicas sobre vulnerabilidades que afectan el hardware o software.
- Se deben revisar o auditar al menos 1 vez cada 6 meses que se respeten y mantengan aplicados los roles y permisos adecuados en la estructura jerárquica de primero, segundo y tercer nivel.

BIBLIOGRAFÍA

Carlo Hamalainen,2017. Raspbian with full disk encryption. [Consultado 20 noviembre 2020]. Disponible en línea: https://carlo-hamalainen.net/2017/03/12/raspbian-with-full-disk-encryption/

Centro de estudios estratégicos y Marítimos. SISTEMA DE SEGURIDAD NACIONAL. p. 14. [Consultado: 23 diciembre 2020]. Disponible en: https://www.esup.edu.pe/descargas/dep_investigacion/SISTEMA CIBERSEGURIDAD NACIONAL 2014.pdf

Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. [Citado 16 diciembre 2020]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. Bogotá. (mayo 10 de 2015). Diario Oficial No. 47.223 de 5 de enero de 2009, 2015). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008., 2008). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

COLOMBIA, CONGRESO DE LA REPUBLICA. DECRETO 410 DE 1971. Bogotá. (Diciembre 31 de 1971). Artículo 515. Diario Oficial No. 33.339 del 16 de junio de 1971, 1971). [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio_pr002.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 de 1999. Bogotá. (Agosto 21 de 1999). Diario Oficial 43.673. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 de 2008. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012. Bogotá. (Octubre 18 de 2012). Diario Oficial 48.587. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Comisión de Regulación de Comunicaciones, República de Colombia. Resolución 2058 del 2009., 2009. [Consultado 18 octubre 2020]. Disponible en: https://www.crcom.gov.co/resoluciones/00002058.pdf

Comisión de Regulación de Comunicaciones, República de Colombia. 2015. p 77., 2018. [Consultado 18 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Comisión de Regulación de Comunicaciones, República de Colombia. 2015. p 77.) [Consultado 12 septiembre 2020]. Disponible en: https://www.crcom.gov.co/recursos_user/Documentos_CRC_2015/Actividades_regulatorias/Ciberseguridad/Doc_Ciberseguridad28_07_15.pdf

Confecámaras. INFORME DE DINÁMICA EMPRESARIAL EN COLOMBIA. Bogotá.2017. p. 2. Disponible en línea: https://incp.org.co/Site/publicaciones/info/archivos/Informe-de-Dinamica-Empresarial-2017-17012018.pdf

Conpes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. p. 2. [Consultado: 23 diciembre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

DEFINICIÓN DE MALWARE. [Consultado 22 noviembre 2019]. Disponible en: https://definicion.de/malware/

Deshabilitar Virtual de las Consolas tty[1-6]. [Consultado 20 noviembre 2020]. Disponible en línea: https://www.enmimaquinafunciona.com/pregunta/54032/deshabilitar-virtual-de-las-consolas-tty1-6

Eito-Brun, R., & Aliaga, C. C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. (Spanish). Revista Española de Documentación Científica, 43(3), 1–14. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=146457387&lang=es&site=eds-live&scope=site

GÓMEZ CASTRO SANTIAGO. E-Commerce, crecimiento y ecosistema digital en Colombia. Edición 1213. Bogotá 2019. p. 1. Disponible en: https://www.asobancaria.com/wp-content/uploads/1213.pdf

Information security architecture; an integrated approach to security in the organization, 2d ed. (2006). SciTech Book News. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.142887097&lang=es&site=eds-live&scope=site

ISO 27001. (2005). ¿Qué es un SGSI? El portal de ISO 27001 en español. [citado en 25 de abril de 2016]. Disponible en linea: http://www.iso27000.es

ISOTools. Excellence. ISO publica la encuesta 2018 de certificaciones de estándares. España. 2019. [Consultado 20 junio 2020]. Disponible en: https://www.isotools.org/2019/09/24/iso-publica-la-encuesta-2018-de-certificaciones-de-estandares

ITSFOSS. Disable IPv6. [Consultado 20 noviembre 2020]. Disponible en línea: https://itsfoss.com/disable-ipv6-ubuntu-linux/

Jaramillo H., D., Cabrera S., A., Abad E., M., Torres V., A., & Carrillo erdúm, J. (2015). Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferencia Ibérica de Sistemas e Tecnologías de Información) Proceedings, 1, 562. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=114061117&lang=es&site=eds-live&scope=site

Jhon Carles, 2015 Proteger el Grub con Contraseña. [Consultado 20 noviembre 2020]. Disponible en línea en: https://geekland.eu/proteger-el-grub-con-contrasena/

Linux Hint. mount_partition_uuid_label_linux. [Consultado 20 noviembre 2020]. Disponible en línea https://linuxhint.com/mount_partition_uuid_label_linux/

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129–134. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=108732548&lang=es&site=eds-live&scope=site

Michael E. Whitman, & Herbert J. Mattord. (2017). Principles of Information Security, Edition 6. Cengage Learning. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=2639438&lang=es&site=eds-live&scope=site

MIN TIC, Guía No 7. Guía de gestión de riesgos. Seguridad y Privacidad de la información. Bogotá 2016. p. 4. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MIN TIC. Documentos para HABEAS DATA: Regulación y Reglamentación. Bogotá 2013. [Consultado 18 octubre 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

MORENO GÓMEZ, G. A. (2017). El Estatuto Del Consumidor Como Forma De Corregir La Asimetría De La Información en La Adquisición De Productos O Servicios en Páginas Web en Colombia. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 17, 1–35. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=126901313&lang=es&site=eds-live&scope=site

Moreno F. C. E. (2017). Diseño de un Sistema de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías territorial Nariño.- p 13. [Consultado 15 mayo 2020]. Disponible en: https://repository.unad.edu.co/handle/10596/11876

Morán, C. E. (2017). Diseño de un Sistema de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías territorial Nariño.. P. 128. [Consultado 14 marzo 2020]. Disponible en: https://repository.unad.edu.co/handle/10596/11876

PETERSON, R. Integration Strategies and Tactics for Information Technology Governance. En W. VAN GREMBERGEN, Strategies for Information Technology Governance (p. 37-80). IDEA Group Publishing. 2004. p. 3. Disponible en línea: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=87306&lang=es&site=eds-live&scope=site

PWC. HAWKSWORTH JHON, AUDINO HANNAH.CLARRY ROB. El mundo en el 2050, Una mirada al futuro. ¿Cómo cambiará el orden económico mundial para el 2050?. 2017. p. 6. Disponible en: https://www.pwc.com/co/es/assets/document/el_mundo_en_2050.pdf

Red Hat. ¿Qué es Kubernetes?. [Consultado 20 diciembre 2020]. Disponible en: https://www.redhat.com/es/topics/containers/what-is-kubernetes

Red iris. DDoS: Un campo de batalla abierto en la seguridad de Internet. [Consultado: 23 diciembre 2020]. Disponible en: https://www.rediris.es/difusion/publicaciones/boletin/57/enfoque2.html

Sarria Cuellar, M. (2015). Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. [Consultado 20 mayo 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.as

px?direct=true&db=ir00913a&AN=unad.10596.3631&lang=es&site=eds-live&scope=site

Superintendencia Financiera de Colombia, Circular Externa 007 de 2018, Bogotá. Disponible en línea: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc

Superintendencia Financiera de Colombia, Circular Externa 008 de 2018, Bogotá. Disponible en línea: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031742/ce008_18.doc

SOPHOS Ltd. El rompecabezas imposible de la ciberseguridad. Reino Unido 2019. p. 8. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

Superintendencia Financiera de Colombia, Circular Externa 007 de 2018, Bogotá. [Consultado 18 octubre 2020]. Disponible en: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc

Superintendencia Financiera de Colombia, Circular Externa 008 de 2018, Bogotá, 2018. [Consultado 18 octubre 2020]. Disponible en: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce008_18.doc

TIPTON, 2006 Harold F. Tipton, Micki Krause (eds.), Information Security Management Handbook, 5th Ed., CRC Press, 2006. [Consultado 10 junio 2020]. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=115870&lang=es&site=eds-live&scope=site

Velasco Melo, A. H. (2008). El Derecho Informático Y La Gestión De La Seguridad De La Información Una Perspectiva Con Base en La Norma ISO 27 001. Revista de Derecho, P. 29, 333–366. Disponible en línea: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=34969402&lang=es&site=eds-live&scope=site

ANEXOS

ANEXO A: Dominios ISO 27001:2013

Núm.	Nombre	Descripción / Justificación
A.5	**Políticas de seguridad de la información**	
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	**Objetivo**: Garantizar el apoyo por parte de la dirección, en temas de seguridad de la información y en función los requisitos del negocio, teniendo en cuanta la legislación aplicable y la reglamentación adecuada
A.5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6	**Organización de la seguridad de la información**	
A.6.1	Organización interna	**Objetivo**: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

Núm.	Nombre	Descripción / Justificación
A.6.2	Dispositivos para movilidad y teletrabajo.	**Objetivo**: Establecer un marco de referencia de gestión para el uso y control de los dispositivos de movilidad y teletrabajo de la organización.
A.6.2.1		Control: Política de uso de dispositivos para movilidad.
A.6.2.2		Control: Teletrabajo
A.7	**Seguridad de los recursos humanos**	
A.7.1	Antes de la contratación	**Objetivo**: Establecer los lineamientos antes de la contratación en la organización.
A.7.1.1		Control: Investigación de antecedentes.
A.7.1.2		Control: Términos y condiciones de contratación.
A.7.2	Durante la contratación	**Objetivo**: Establecer los lineamientos durante la contratación en la organización.
A.7.2.1	Responsabilidades de la dirección	Control: La dirección exige y apoya a todos los colaboradores internos o externos en pro de la aplicación o despliegue de la seguridad de la información y su alineación con las políticas de cualquier índole, al igual que los procedimientos establecidos para la organización.
A.7.2.2	Toma de conciencia en educación continua y formación en la seguridad de la información	Control: Todos los colaboradores internos o externos, serán participes de la formación continua seguridad de la información, actualizaciones regulares sobre las políticas de seguridad de la información y los procesos pertinentes delegados a su cargo.
A.7.3	Cese o cambio de puesto de trabajo	**Objetivo**: Establecer los lineamientos durante el cese o cambio de puesto de trabajo en la organización.

Núm.	Nombre	Descripción / Justificación
A.7.3.1		Control: Cese o cambio de puesto de trabajo.
A.8	**Gestión de activos**	
A.8.1	Responsabilidad por los activos	**Objetivo**: Identificar los activos informáticos de la organización y definir cuáles son las responsabilidades aplicables que garanticen la protección adecuada
A.8.1.1	Inventario de activos	Control: Inventariar e identificar los activos informáticos y que están asociados con la información, así como el lugar o ubicación donde se procesa la información, Se crear un documento con el inventario de estos activos que debe actualizarse periódicamente.
A.8.1.2	Propiedad de los activos	Control: Cada activo de la organización debe tener un responsable a quien fue asignado.
A.8.1.3	Uso aceptable de los activos	Control: Debe existir un documento formal que dicte cuales son las buenas prácticas de uso aceptable para los activos informáticos cualquier entidad y los espacios de procesamiento de datos dispuestos
A.8.1.4	Devolución de activos	Control: Sin excepción todos y cada uno de los colaboradores, usuarios externos; deben regresar los activos de la organización que fueron entregados a su cargo, una vez se dé por terminado su contrato o acuerdo establecido.
A.8.2	Clasificación de la información	**Objetivo**: Acorde a los niveles de criticidad del activo, se deben ejecutar los mecanismos de protección adecuados para el mismo
A.8.2.1		Control: Teniendo en cuenta los requisitos legales, criticidad, valor y susceptibilidad a divulgación o la posibilidad de que la información modificada de manera

Núm.	Nombre	Descripción / Justificación
		no autorizada. se deben clasificar adecuadamente los activos
A.8.2.2	Etiquetado de la información	Control: Asociar el esquema de clasificación que utilice la organización al etiquetar la información y facilitando los procedimientos
A.8.2.3	Manejo de los activos	Control: Teniendo en cuenta el esquema de clasificación de la información es necesario implementar los procedimientos de manejo adecuado de los activos de información.
A.8.3	Manejo de los soportes de almacenamiento	**Objetivo**: Lineamiento para el uso y manejo de los soportes de almacenamiento
A.8.3.1		Control: Gestión de soportes extraíbles
A.8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requiera, utilizando procedimientos formales.
A.8.3.3		Control: Soportes físicos en tránsito
A.9	**Control de accesos**	
A.9.1	Requisitos del negocio para control de acceso	**Objetivo**: Delimitar y restringir el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	Control: En función de los requisitos del negocio y de seguridad de la información es necesario crear, documentar y aplicar una política de control de acceso
A.9.1.2	Política sobre el uso de los servicios de red	Control: únicamente los usuarios debidamente autorizados previamente deben tener acceso a la red y a los servicios tecnológicos en la red

Núm.	Nombre	Descripción / Justificación
A.9.2	Gestión de acceso de usuarios	**Objetivo**: Permitir solamente el acceso los usuarios autorizados al sistema o centros de procesamiento de datos y denegar el acceso no autorizado a los sistemas ubicaciones o servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Debe existir un documento formal que sea una bitácora donde reposen, se modifiquen o actualicen los registros del talento humano contratado o ajeno a la organización.
A.9.2.2	Suministro de acceso de usuarios	Control: Desplegar un proceso formal creación y asignación de privilegios a los usuarios o revocarlos, restringiendo los derechos de acceso a los sistemas, ubicaciones y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Debe existir un mecanismo que controlare y restrinja el proceso de asignación de privilegios o el uso de derechos de acceso no autorizados
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: Toda información clasificada como confidencial o sensible se debe controlar a través de un proceso debidamente formalizado
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los encargados de los activos continuamente deben revisar que los derechos de acceso de los usuarios sean los autorizados
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Cada vez que haya cambios de personal internos o externos y que interactúen con los datos o las locaciones de procesamiento de datos se debe dar de baja en los sistemas o modificar sus derechos de acceso.

Núm.	Nombre	Descripción / Justificación
A.9.3	Responsabilidades de los usuarios	**Objetivo**: Cada usuario es responsable por asegurarse que su información se resguarde en el lugar provisto utilizando los mecanismos de autenticación dispuestos para ello.
A.9.3.1	Uso de la información de autenticación secreta	Control: Los usuarios deben cumplir las prácticas y políticas de seguridad de la información en cuanto al uso de información de autenticación que es de carácter meramente secreto
A.9.4	Control de acceso a sistemas y aplicaciones	**Objetivo**: Evitar, mitigar, restringir el acceso no autorizado a las aplicaciones o los sistemas de la compañía o de terceros.
A.9.4.1	Restricción de acceso Información	Control: Teniendo en cuenta la Política de control de acceso, es necesario restringir el acceso a las funciones de los sistemas de aplicaciones o, a la información como tal.
A.9.4.2	Procedimiento de ingreso seguro	Control: Todo acceso a los sistemas o aplicaciones deben ser controlados y asegurados acorde a la política de control de acceso
A.9.4.3	Sistema de gestión de las contraseñas	Control: La gestión de los sistemas de contraseñas deben ser interactivos, seguros y garantizar la robustez de las contraseñas.
A.9.4.4	Herramientas de administración	Control: Uso de herramientas de administración de sistemas.
A.9.4.5	Acceso al código fuente de programas	Control: Control de acceso al código fuente de los programas.
A.10	**Criptografía**	

Núm.	Nombre	Descripción / Justificación
A.10.1	Controles Criptográficos	**Objetivo**: Determinar las directrices mínimas de los controles criptográficos
A.10.1.1		Control: Política de uso de los controles criptográficos.
A.10.1.2		Control: Gestión de claves o Llaves
A.11	**Seguridad física y del entorno**	
A.11.1	Áreas seguras	**Objetivo**: Prevenir el acceso físico a las áreas restringidas, evitando el acceso no autorizado a la información o instalaciones o centros de datos, de igual manera que evite el daño o la interferencia con la información
A.11.1.1	Perímetro de seguridad física	Control: Se deben establecer perímetros de seguridad, destinados a proteger los sitios de manejo de información. de la información sensible o crítica,
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras o restringidas deben estar resguardadas mediante controles biométricos asegurando que únicamente, quien esté debidamente autorizado tenga el respectivo acceso.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se diseña, mejora o aplica la seguridad física en las instalaciones, oficinas, sedes, centros o recintos
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se diseña, mejora o aplica la protección física contra desastres naturales, incidentes, ataques informáticos maliciosos o posibles accidentes.
A.11.1.5		Control: El trabajo en áreas catalogadas como seguras
A.11.1.6		Control: Áreas de acceso público, carga y descarga

Núm.	Nombre	Descripción / Justificación
A.11.2	Equipos	**Objetivo**: Prevenir la interrupción de las operaciones de la organización, evitar el robo, daño o perdida de la data contenida y/o que los activos sean comprometidos
A.11.2.1	Ubicación y protección de los equipos	Control: Mitigar los peligros del entorno tecnológico, y las oportunidades que se presenten de accesos no autorizado, protegiendo los equipos y reduciendo los riesgos de que se materialicen las amenazas
A.11.2.2	Servicios de suministro	Control: Protección a los equipos contra fallas del suministro eléctrico que puedan causar interrupciones al sistema o la organización
A.11.2.3	Seguridad del cableado	Control: Se debe proteger el cableado que transporta las telecomunicaciones o servicios de información evitando que sea objeto de interceptación, obstrucción, ataques de hombre en medio físicos o daños.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos reciben mantenimientos preventivos y correctivos para asegurar su disponibilidad e integridad operativa.
A.11.2.5	Retiro de activos	Control: Cada vez que se requiera realizar un retiro de software o de equipos de información se debe presentar la autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Es recomendable aplicar diferentes medidas para robustecer la seguridad de los activos de información que se encuentren por fuera de las ubicaciones físicas de la entidad y contemplar los posibles riesgos a los que se exponen al trabajar fuera de las instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Control: Todos los equipos o medios de almacenamientos susceptibles a disposición o

Núm.	Nombre	Descripción / Justificación
		reutilización deben ser borrados de forma segura o sobre escribir su información.
A.11.2.8	Equipos de usuarios desatendidos	Control: cada usuario tiene que asegurarse y exigir que les brinden protección adecuada para los equipos considerados como desatendidos
A.11.2.9	Política de escritorio y pantalla limpios	Control: Es ampliamente recomendable que por medo de una política de seguridad de la información se exija tener el escritorio de trabajo informático limpio, al igual que se limpie periódicamente los dispositivos de almacenamiento removibles
A.12	**Seguridad de las operaciones**	
A.12.1	Procedimientos operacionales y responsabilidades	**Objetivo**: Los centros de datos y procesamiento de información deber ser seguros
A.12.1.1	Procedimientos de operación documentados	Control: Los conjuntos de procesos y procedimientos necesarios para la operación deben estar debidamente documentados y al alcance de los usuarios debidamente autorizados
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios dentro de la organización, documentos o procesos de negocio en todas las sedes y ubicaciones tenga presencia la entidad; al igual que en los sistemas informáticos que afectan o impacten directa o indirectamente la seguridad de los sistemas y de la información.
A.12.1.3	Gestión de capacidad	Control: Realizar monitoreo del uso de los recursos y el nivel de desempeño optimo del sistema que permita realizar los tunning o ajustes, al igual que permita y

Núm.	Nombre	Descripción / Justificación
		proyectar el crecimiento esperado de acuerdo con la dinámica del negocio capacidad que necesitara a futuro
A.12.1.4	Entornos de desarrollo, prueba y producción	Control: Separación y control de los entornos de desarrollo, pruebas y producción
A.12.2	Protección contra códigos maliciosos	**Objetivo**: garantizar que están habilitados los mecanismos mínimos de protección que reducirán el riesgo de vulneración por códigos maliciosos en los centros de datos o sistemas informáticos de la entidad
A.12.2.1	Controles contra códigos maliciosos	Control: Concienciación adecuada de los usuarios al ser el “eslabón más débil de la cadena”, al igual que se deben implementar controles de prevención, detección y recuperación, para proteger contra ataques ocasionados códigos maliciosos.
A.12.3	Copias de respaldo	**Objetivo**: Proteger contra la pérdida de datos.
A.12.3.1	Respaldo de información	Control: Se debe mantener un esquema de backups en el modelo abuelo, padre, hijo para garantizar el respaldo de la información, imágenes, vídeos, documentos, software de los sistemas, etc.; estás deben reposar en un lugar seguro, acorde a la política de copias de respaldo de la entidad.
A.12.4	Registro y seguimiento	**Objetivo**: Generar evidencia al registrar los eventos
A.12.4.1	Registro de eventos	Control: Se deben conservar y revisar regularmente los registros que generan los sistemas acerca de actividades del usuario en los mismos, así como las fallas, eventos de seguridad de la información o las excepciones.

Núm.	Nombre	Descripción / Justificación
A.12.4.2	Protección de la información de registro	Control: Blindar la información de registro evitando su acceso no autorizado o alteración lógica y física.
A.12.4.3	Registros del administrador y del operador	Control: Se deben almacenar y auditar periódicamente los registros que generan los sistemas acerca de actividades del administrador y operador, así como las fallas, eventos de seguridad de la información o las excepciones.
A.12.4.4	sincronización de relojes	Control: La hora de todos y cada uno de los sistemas informáticos de la organización se debe sincronizar con una o más fuentes confiables de tiempo.
A.12.5	Control de software operacional	**Objetivo**: Garantizar la integridad de los sistemas informáticos o la data que resida en ellos
A.12.5.1	Instalación de software en sistemas operativos	Control: Los procedimientos o procesos o para instalar software en los sistemas operativos solo deben ser ejecutados por el personal debidamente autorizado y de manera controlada
A.12.6	Gestión de la vulnerabilidad técnica	**Objetivo**: Mitigar, recudir la brecha y posibilidad de que se materialicen las vulnerabilidades técnicas sobre los sistemas de información.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe levantar información sobre las posibles vulnerabilidades a las que se exponen los activos informáticos de la organización, al igual mitigar el uso de técnicas de los sistemas de información que se usen para exponer a la organización a estas vulnerabilidades, es imperativos tomar medidas adecuadas en pro de reducir el riesgo asociado.

Núm.	Nombre	Descripción / Justificación
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las políticas sobre instalación de software por parte de los usuarios.
A.12.7	Consideraciones de las auditorías de los sistemas de información	**Objetivo**: Definir los lineamientos para realizar las auditorías a los sistemas de información
A.12.7.1	Información controles de auditoría de sistemas	Control: Es necesario planear y conseguir autorización para minimizar las posibles interrupciones de servicios que pueda afectar los procesos de la entidad y sus objetivos de negocio o del sistema operativo.
A.13	**Seguridad de las comunicaciones**	
A.13.1	Gestión de la seguridad de las redes	**Objetivo**: Garantizar que las redes informáticas de la entidad cuentan con la protección adecuada en su centro de datos y las ubicaciones físicas.
A.13.1.1	Controles de redes	Control: Protección de los sistemas de información, sus redes o aplicaciones de la mano de las mejores prácticas de gestión
A.13.1.2	Seguridad de los servicios de red	Control: Los requisitos de gestión y los niveles de servicio de todos los servicios de red, deben ser de conocimiento interno o externo si fuera requerido y deben reposar en los acuerdos de servicios de red
A.13.1.3	Separación en las redes	Control: Segmentación o división de las redes acorde a los departamentos, áreas o procesos de la entidad.
A.13.2	Transferencia de información	**Objetivo**: Garantizar el nivel de seguridad mínimo aceptables a la hora de transmitir información al interior de la organización o entidades externas a la misma.

Núm.	Nombre	Descripción / Justificación
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Los mecanismos de transferencia de información por cualquier canal de comunicaciones, deben estar debidamente documentados y deben existir políticas de seguridad de la información asociadas como tal.
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos contemplaran los mecanismos de transferencia segura dentro de la organización o con entidades externas.
A.13.2.3	Mensajería electrónica	Control: El contenido del mensaje debe estar debidamente protegido tanto en almacenamiento, como en transmisión
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se debe crear o actualizar el acuerdo de confidencialidad y documentar los requisitos mínimos para que se dé tal acuerdo, al igual que garantice su cumplimiento al mantener la confidencialidad y no divulgación de información de carácter sensible
A.14	**Adquisición, desarrollo y mantenimientos de sistemas**	
A.14.1	Requisitos de seguridad de los sistemas de información	**Objetivo**: Garantizar que los sistemas de información protegidos y la seguridad de la información, sean la constante durante todo el ciclo de vida, tanto en las redes privadas como de acceso público
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Las mejoras a tecnologías en uso o los nuevos sistemas de información, deben tener requisitos de seguridad de la información inmersos
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: garantizar que la información expuesta o disponible como parte de un servicio publicado este debidamente protegida, evitando su divulgación no autorizada.

Núm.	Nombre	Descripción / Justificación
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: Los datos transmitidos por servicios o aplicaciones deben estar debidamente protegidos en su medio de almacenamiento o de transmisión, así como desplegar mecanismos que eviten transmisiones incompletas, no autorizadas o sea alterada la información
A.14.2	Seguridad en los procesos de desarrollo	**Objetivo**: Definir las características mínimas que para garanticen la correcta ejecución de los procesos de desarrollo y de forma segura
A.14.2.1	Política de desarrollo seguro	Control: Todo desarrollo dentro de la organización debe tener reglas claras y enfocadas a mantener los mejores niveles de seguridad
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: la Gestión del cambio debe controlar los cambios como parte del ciclo de vida de desarrollo de software y deben quedar debidamente documentados dentro de los sistemas de información dispuestos.
A.14.2.3		Control: Efectuar pruebas de aceptación mínima tras realizar cambios en el sistema operativo en un entorno controlado.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se restringir los cambios o modificaciones nivel de paqueterías de software, limitando solo a los cambios estrictamente
A.14.2.5	Principios de construcción de sistemas seguros	Control: Garantizar que de desarrollan o construyen sistemas seguros, teniendo en cuenta las actividades de implementación, actualización y su respectiva documentación
A.14.2.6		Control: Seguridad en los ambientes de desarrollo
A.14.2.7		Control: Tercerización del desarrollo de software

Núm.	Nombre	Descripción / Justificación
A.14.2.8	Pruebas de seguridad de sistemas	Control: las pruebas de funcionalidad son una parte integral del durante el desarrollo de software o aplicaciones y en función de la seguridad informática
A.14.2.9	Prueba de aceptación de sistemas	Control: Establecimiento de los criterios mínimos de aceptación relacionados con nuevas versiones, actualizaciones a los sistemas de información
A.14.3	Datos de prueba	**Objetivo**: Los datos utilizados en los entornos de pruebas deben ser debidamente protegidos.
A.14.3.1	Protección de datos de prueba	Control: Los datos de ensayo y error deben ser protegidos y controlados cuidadosamente.
A.15	**Relación con los proveedores**	
A.15.1	Seguridad de la información en las relaciones con los proveedores	**Objetivo**: Garantizar la protección de activos información que son accedidos por proveedores o terceros ajenos a la entidad
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Se deben establecer acuerdos con los proveedores para mitigar los posibles riesgos de los activos de información y estar debidamente documentados
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben definir acuerdos con los proveedores para establecer los niveles de acceso, almacenamiento, sistemas o componentes de infraestructura de TI sobre los que tendrá acceso en pro de mitigar los posibles riesgos de los activos de información y dejarlos debidamente documentado
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores tienen que incluir objetivos para mitigar riesgos de seguridad de la información que pueden estar asociados a la cadena de

Núm.	Nombre	Descripción / Justificación
		suministro de servicios o productos de las tecnologías de la información y las telecomunicaciones.
A.15.2	Gestión de la prestación de servicios con los proveedores	**Objetivo**: Los acuerdos con los proveedores deben mantener el nivel de seguridad acordado y en función de os servicios prestado a la entidad
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Auditar los servicios prestados por los proveedores a la entidad deben ser una constante y susceptible a mejoras
A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deben controlar los cambios dentro de la organización o por proveedores, documentos o procesos de negocio en todas las sedes y ubicaciones donde tenga presencia la entidad; al igual que en los sistemas informáticos que afectan o impacten directa o indirectamente la seguridad de los sistemas y de la información.
A.16	**Gestión de incidentes de seguridad de la información**	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	**Objetivo**: Garantizar alineación coherente y efectiva frente a los incidentes gestión de seguridad de la información, incluyendo las comunicaciones, debilidades identificadas o sobre eventos de seguridad
A.16.1.1	Responsabilidad y procedimientos	Control: Asegurar una respuesta oportuna, rápida y eficiente, de manera ordenada frente a los incidentes de seguridad de la información definiendo los procedimientos y responsabilidades de gestión.
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Se deben informar todos los eventos de seguridad de la información utilizando los canales adecuados y que fueron dispuestos para ello, lo antes posible.

Núm.	Nombre	Descripción / Justificación
A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Es de carácter obligatorio que todos los colaboradores y contratistas informen cualquier debilidad o vulnerabilidad latente identificadas e incluso sospechosas al utilizar los servicios y sistemas de información de la entidad,
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Definir si los eventos de seguridad de la información identificados son catalogados como incidentes de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Utilizar los procedimientos y documentación de los incidentes de seguridad de la información detectados
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: Documentar debidamente los incidentes de seguridad de la información que fueron analizados y/o resueltos reduciendo el posible impacto de incidentes a futuro
A.16.1.7	Recolección de evidencia	Control: La entidad debe recolectar información que sirva como tras una afectación o vulneración detectada
A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**	
A.17.1	Continuidad de seguridad de la información	**Objetivo**: Debe ser parte de la política empresarial el dar continuidad de seguridad de la información a través de los sistemas gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: Durante una desastre o crisis, la organización debe establecer cuáles son los requisitos para mejorar la seguridad de la información y dar continuidad a la

Núm.	Nombre	Descripción / Justificación
		gestión de la seguridad de la información en situaciones ajenas o adversas
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La entidad debe definir, documentar, desplegar y mantener los procedimientos, controles o procesos que permitan asegurar un nivel adecuado de continuidad de seguridad de la información durante una situación no contemplada
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La entidad debe definir intervalos de verificación periódicos frente a los controles de continuidad de la seguridad de la información estipulados e implementarlos, con la finalidad de asegurar que son eficaces y válidos durante situaciones no contempladas o ajenas a su control.
A.17.2	Redundancias	**Objetivo**: garantizar la disponibilidad de los centros de datos o procesamiento de la información y las comunicaciones
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de datos o comunicaciones deberían desplegarse en redundancia, de tal forma que permitan cumplir con los requisitos mínimos de la disponibilidad.
A.18	**Cumplimiento**	
A.18.1	Cumplimiento de requisitos legales y contractuales	**Objetivo**: Las obligaciones legales, estatales, de complimiento o contractuales y asociadas con la seguridad de la información, se deben gestionar oportunamente para dar su debido cumplimiento
A.18.1.1	Identificación de la legislación aplicable y de	Control: Se deben documentar, actualizar e identificar estrictamente todos los requisitos estatales, de reglamentación pertinentes al igual que los

Núm.	Nombre	Descripción / Justificación
	los requisitos contractuales	contractuales en los sistemas de información y para la entidad, con enfoque de cumplirlos a cabalidad
A.18.1.2	Derechos de propiedad intelectual	Control: Se deben desplegar procedimientos adecuados que garanticen el cumplimiento de los requisitos de reglamentación, legislativos y contractuales asociados a los derechos uso de productos de software patentados y de propiedad intelectual.
A.18.1.3	Protección de registros	Control: Se debe garantizar que los registros o bitácoras estén debidamente protegidos contra falsificación, pérdida, acceso no autorizado, liberación no autorizada o destrucción de los mismos, en función de los requisitos legislativos, contractuales o del negocio.
A.18.1.4	Privacidad y protección de datos personales	Control: Cada vez que sea plausible, se deben asegurar los datos de carácter persona en función de la protección y la privacidad de la información, tal cual es exigido por la legislación vigente
A.18.1.5	Reglamentación de controles criptográficos	Control: Los controles criptográficos deben ser robustos en cumplimiento las normatividades vigentes y que permitan garantizar la confidencialidad, disponibilidad e integridad y de la información
A.18.2	Revisiones de seguridad de la información	**Objetivo**: Garantizar el despliegue y operación de la seguridad de la información conforme a las políticas corporativas y procesos del negocio
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque adecuado de la entidad para la implementación y gestión de la seguridad de la información debe ser: (es decir, los procedimientos, objetivos de control, los procesos las políticas y los controles para seguridad de la información) revisada

Núm.	Nombre	Descripción / Justificación
		independiente y puntualizada mente, de forma recurrente y con planificación o cuando se presenten cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con bastante regularidad el cumplimiento los procesos y procedimientos de información, acorde a su nivel de responsabilidad entregado por la alta gerencia, enfocándose en las normas y políticas de seguridad de la información adecuadas, así como tener presente, y otro eventual requisito necesario para satisfacer las normatividades
A.18.2.3	Revisión del cumplimiento técnico	Control: Para garantizar el cumplimiento de las políticas y normatividades adoptadas de seguridad de la información en la entidad, se deben revisar cíclicamente los sistemas de información y procedimientos dispuestos

Fuente: Morán, C. E. (2017). Diseño de un Sistema de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías territorial Nariño. Recuperado de: https://repository.unad.edu.co/handle/10596/11876.

ANEXO B: Levantamiento de activos informáticos.

Nombre del activo de información	Proceso propietario del activo	Responsable
[firewall] ASA0-5505	Departamento de Sistemas	Eduar Aguirre
[router] Internet 2811	Departamento de Sistemas	Eduar Aguirre
[s] Servidor PBX	Departamento de Sistemas	Eduar Aguirre
[s] Sistemas de Registro y Control	Departamento de Sistemas	Eduar Aguirre
[s] Servidor DHCP	Departamento de Sistemas	Eduar Aguirre
[switch] Switch-0	Departamento de Sistemas	Eduar Aguirre
[ipphone] Teléfono IP 115	Departamento de Sistemas	Eduar Aguirre
[ftp] Servidor FTP	Departamento Antiguo de Sistemas	Eduar Aguirre
[switch] Switch-3	Centro de estudio	Luz Marina Ayala
[ipphone] Teléfono IP 114	Centro de estudio	Luz Marina Ayala
[print] Printer 1	Centro de estudio	Luz Marina Ayala
[hw] PC0	Centro de estudio	Luz Marina Ayala
[hw] PC1	Centro de estudio	Luz Marina Ayala
[switch] Switch-2	Departamento de registro y control académico	Erika Liliana Silva
[ipphone] Teléfono IP 113	Departamento de registro y control académico	Erika Liliana Silva

Nombre del activo de información	Proceso propietario del activo	Responsable
[print] Printer 0	Departamento de registro y control académico	Erika Liliana Silva
[switch] Switch-Contabilidad	Departamento de Contabilidad	Rosa Melina Murillo
Teléfono IP 112	Departamento de Contabilidad	Rosa Melina Murillo
[hw] PC14	Departamento de Contabilidad	Rosa Melina Murillo
[hw] PC15	Departamento de Contabilidad	Rosa Melina Murillo
[hw] PC16	Departamento de Contabilidad	Rosa Melina Murillo
[switch] Switch-Sala-Sistemas	Departamento de Sistemas	Eduar Aguirre
[ipphone] Teléfono IP 112	Departamento de Sistemas	Eduar Aguirre
[hw] PC17	Departamento de Sistemas	Eduar Aguirre
[hw] PC18	Departamento de Sistemas	Eduar Aguirre
[switch] Switch-Sala-Internet	Centro de estudio - SI	Luz Marina Ayala
[ipphone] Teléfono IP 110	Centro de estudio - SI	Luz Marina Ayala
[hw] PC37	Centro de estudio - SI	Luz Marina Ayala
[hw] PC38	Centro de estudio - SI	Luz Marina Ayala
[hub] HUB-0	Campus Universitario	Eduar Aguirre
[hub] HUB-1	Campus Universitario	Eduar Aguirre

Nombre del activo de información	Proceso propietario del activo	Responsable
[hub] HUB-2	Campus Universitario	Eduar Aguirre
[hub] HUB-3	Campus Universitario	Eduar Aguirre
[wap] WRT300N-Campus1	Campus Universitario	Eduar Aguirre
[wap] WRT300N-Campus2	Campus Universitario	Eduar Aguirre
[L] Sala de internet	Departamento Académico	Luz Marina Ayala
[L] Sala de Tutores	Departamento de registro y control académico	Erika Liliana Silva
[L] Oficina de contabilidad	Departamento de Contabilidad	Rosa Melina Murillo

Fuente: Propiedad del autor