PROGRAMA DE AUDITORÍA/CONSULTORÍA PARA LA VERIFICACIÓN Y ALINEACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN CON LOS OBJETIVOS DE TECNOLOGÍA PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Presentado por:
HELENA PATRICIA MORENO DURAN
ROSA PATRICIA GARCIA POLO
LUIS FERNANDO PLAZAS TUTTLE

ASESOR TEMÁTICO:
ING. WILMAR JAIMES FERNÁNDEZ

UNIVERSIDAD POLITÉCNICO GRAN COLOMBIANO
MAYO 2018

DEDICATORIA

Dedicamos este trabajo de grado a Dios por estar en cada paso dado, ya quien fue el que ilumino nuestras mentes en cada actividad de esta especialización, por permitir encontrarnos y mostrar nuestras fortalezas, a todos aquellos que se esfuerzan día a día en hacer lo mejor, progresar, crecer personal y profesionalmente.

A pesar de mantener vidas ocupadas, familia, amigos, trabajo, dedican el esfuerzo, horas de sueño, a ser mejor y a retarse para aprender cosas nuevas todos los días.

TABLA DE CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

1 ABSTRACT

We decide to make a program (Consulting/audit) for small and medium companies, aligning COBIT (Control Objectives for Information and related Technology) and ISO27001 (Information security management), because as a result of our investigation about this kind of software or program, did not match the objective we are looking for, the type of tool and instruments we are giving to accompany and help small a medium business to create, modify or implement a Security Information System with the necessary alignment with the technology department, and low resource cost.

When we applied the HEPALU Consulting & Software in a pilot company, the result was excellent, because the result was accepted, understood and they were thankful for the support we gave them. We were happy that the methodology applied worked as we hope:

- ✓ We found a company that need to implement an information security model
- ✓ The company did not spend so much resource on us, only the time needed for the more accurate results
- ✓ We applied the software and consulting tool, with no problem at all
- ✓ The software was easy to understand and apply
- ✓ The result was great with the conclusion and recommendation of the standards we selected

2 RESUMEN

Se pretende contribuir a pequeñas y medianas empresas que no cuenten o han dispuesto con los recursos, estructura y habilidades, para desarrollar un Sistema de Gestión de Seguridad de la Información SGSI alineado con activos de información y procesos tecnológicos, para lo cual se elaboró una herramienta (programa de auditoría/consultoría), que brinda los controles generales y estado de madurez en el que se encuentra o proyecta estar la entidad, recomendando o dando oportunidades que mejoren o establezca el modelo y las competencias necesarias para el desarrollo del mismo.

Esta herramienta establecerá el diseño y el funcionamiento de los controles mínimos requeridos y las revisiones necesarias, alineados con los marcos internaciones elegidos para poder ser ejecutado por personas de cualquier gentilicio que cuenten con el perfil necesario; obteniendo como resultado actividades, procesos, controles y responsabilidades que la organización debe tomar para la protección y seguridad de la información.

Para las organizaciones (1) actualmente la situación afectante ha sido la de adquirir o desarrollar proyectos que beneficiarían a la entidad en la creación, fortalecimiento y establecimiento de la cultura para la protección del activo más importante "**la información**", al no contar con un sistema de gestión de seguridad de la información y protección de datos alineado a una metodología, proceso interno, mejores prácticas o estándares reconocidos, para cumplir con la normatividad del estado o la del sector que se encuentra la empresa y salvaguarda este activo.

En la encuesta nacional de seguridad de información del 2017 realizada por ACIS "Asociación Colombiana de ingenieros de Sistemas", con una muestra aleatoria de 128 empresas de todo tipo y diferentes sectores, se evidencio el 29% de las empresas encuestadas, manifiesta no saber si la organización gestiona sus incidentes o cómo les da tratamiento; y un porcentaje significativamente superior 71%, está relacionado con la presencia de incidentes de seguridad de información dentro de las mismas(1).

La herramienta que se desarrolló alineando ISO 27001 y COBIT, estableciendo un modelo de madurez con los principales objetivos relacionados en estos marcos, a las áreas de tecnología con seguridad de la información, que según en nuestra investigación este tipo de programas se ha aplicado por separado y a nivel teórico, se implementara en la compañía C&C CORPORACIÓN, en donde su portafolio presenta un servicio de pruebas periciales que sean solicitadas como prueba anticipada o dentro de los procesos de responsabilidad médica, tanto en las áreas del derecho administrativo, civil y penal.

La información de procesos, pruebas e historias clínicas es catalogada como sensible y debe ser protegida y custodiada como lo exige la normatividad Ley 1266 de 2008 HABEAS DATA y Ley estatutaria 1581 (Protección datos Personales de Colombia), la cual se convierte en el pilar de la compañía con los principios de confidencialidad, integridad y disponibilidad de esta información, que puede afectar los niveles de rentabilidad, competitividad e imagen, los cuales son necesarios para lograr los objetivos y beneficios económicos.

3 INTRODUCCIÓN

Debido a la falta de interés y entendimiento de la protección de datos y seguridad de la información por parte de la alta gerencia en las organizaciones, se puede estar incurriendo en incumplimientos normativos exigidos como: Ley estatutaria 1581 (Protección datos Personales de Colombia), o no conocer el tratamiento, mecanismo o actividades para dar solución o controlar los incidentes de seguridad, al no contar con directrices sobre los temas tratados.

La herramienta no impone restricciones que sean contrarias a la cultura, confianza e integridad establecida dentro de la compañía, si no que proporciona recomendaciones, oportunidad de mejora y establece el modelo de madurez actual, para proteger los activos, funcionarios, aliados y socios.

Es importante entender que cada compañía es un mundo diferente con necesidades distintas, por esta razón cada una tiene diferentes controles, políticas, procedimientos, procesos, estructuras organizativas, pero si todas pueden utilizar nuestra metodología que se acomoda a los objetivos de los estándares internacionales alineando los objetivos del área de tecnología con los objetivos del negocio bajo un modelo de seguridad de la información.

4 GENERALIDADES

4.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente las compañías se encuentran en una constante organización y protección de su activo más importante "**la información"**; teniendo la necesidad de implementar un Sistema de Gestión de Seguridad de la Información SGSI, metodologías, actividades (2), ayudando a estructurar de una manera efectiva la seguridad de la información evitando incurrir en inversiones costosas, innecesarias y/o complicadas, las cuales no cubren las amenazas halladas en su entorno.

El problema inicia con las pequeñas y medianas empresas que no han establecido actividades para el manejo y la gestión de seguridad de la información, además áreas críticas como tecnología, trabajando como islas independientes, imposibilitando reconocer los riesgos e incidentes de seguridad de la información en conjunto, para poder gestionar y así validar si estos son transferidos o mitigados por las compañías, de una manera organizada, estructurada, sistémica y documentada.

4.2 OBJETIVOS

4.2.1 OBJETIVO GENERAL

Diseñar una herramienta (auditoría / consultoría) que permita medir el estado de madurez del Sistema de Gestión de Seguridad de la Información actual de las empresas, alineados con los objetivos de control de COBIT, y dar recomendaciones u oportunidades de mejora para alcanzar la madurez deseada, referenciados en COBIT y de la NORMA TÉCNICA NTC-ISO-IEC 27001.

4.2.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar los controles o elementos mínimos requeridos para el desarrollo de un adecuado Sistema de Gestión de Seguridad de la Información SGSI alineados con los objetivos de control de COBIT, en las pequeñas y mediana empresas.
- ✓ Establecer un check list con las diferentes evidencias o entregables que debe solicitar el auditor o programa como insumo para validar o establecer el estado de madurez actual del Sistema de Gestión de Seguridad de la Información SGSI, de la empresa a la que se está aplicando.
- ✓ Referenciar los controles de la norma ISO 27001 y COBIT, que se adapten a las necesidades de la empresa.
- ✓ Seleccionar de los 34 procesos desarrollados por COBIT, los que apoyan las actividades y los criterios en el funcionamiento de un Sistema de Gestión de Seguridad de la Información SGSI, en las pequeñas y mediana empresas.
- ✓ Realizar pruebas y validación de la herramienta en la empresa piloto

4.3 ALCANCE

El proyecto estará enfocado en empresas pequeñas y medianas, que deseen conocer el estado de madurez de su Sistema de Gestión de Seguridad de la Información SGSI o la construcción del mismo. La empresa quien se implementara para prueba de este diseño es C&C CORPORACIÓN

4.4 JUSTIFICACIÓN

Al contar con el programa de auditoría/consultoría que pueda ser aplicable a cualquier empresa o empresas particulares diferentes, se podrá lograr una dirección corporativa o particular sobre los controles que se deben establecer, para poder lograr conocer el nivel de madurez de la gestión de seguridad de la información y protección de datos, además de conocer el grado de alineación y dedicación de las empresas.

Adicionalmente, los controles estarán alineados con los procesos de COBIT 4.1, 5, controles de la ISO27001 y marcos de referencia que puedan ser útiles con el fin de permitir que las empresas puedan implementar políticas, procesos, controles y actividades que están respaldas y son utilizadas como mejores prácticas.

Áreas como auditoria interna, seguridad de la información, contraloría, seguridad física, entre otras, tendrán una guía para probar los controles y estar alineados a mejores estándares. Este entregable podrá servir a cualquier empresa que necesite conocer su estado actual o crear el modelo de Sistema de Gestion de Seguridad de la información alineado con COBIT.

4.5 METODOLOGÍA IMPLEMENTADA EN EL PROYECTO.

Actualmente es importante para toda empresa la implementación de un Sistema de Gestión de Seguridad de la información SGSI, para custodiar al activo más importante de la compañía, se utilizó el fundamento del ciclo PHVA.

PLANIFICAR	Establecer la metodología a trabajar en las empresas a partir de los estándares existentes en ISO 27001 y COBIT alineado con los objetivos de la compañía.
HACER	Crear una adecuada implementación de los controles seleccionados, y generar una estructura organizada con los controles y evidencias a manejar en un Sistema de Gestión de Seguridad de la información SGSI.
VERIFICAR	Evaluar y verificar el desempeño de la herramienta en C&C CORPORACIÓN
ACTUAR	Iniciar las acciones preventivas y correctivas al diseño de la herramienta basadas en los resultados de la auditoria y la evaluación realizada por dirección.

Tabla 1: Ciclo PHVA En El Proyecto

4.6 EMPRESA PILOTO

El principal criterio para la selección de esta empresa C&C CORPORACIÓN es su necesidad de tener un correcto SGSI, al manejar información confidencial y tener una ventaja competitiva frente a otras compañías del mismo sector y tamaño de empresa.

C&C CORPORACIÓN dentro de su portafolio presenta un servicio de pruebas periciales que sean solicitadas como prueba anticipada o dentro de los procesos de responsabilidad médica, tanto en las áreas del Derecho Administrativo, Civil y Penal.

Es una entidad sin ánimo de lucro, que cuenta con personal adscrito, médicos especializados en todas las áreas de la medicina e idóneos, con experticia comprobada, para emitir conceptos o dictámenes técnicos-científicos como prueba pericial frente a la responsabilidad médica, dentro los procesos judiciales o como prueba anticipada a estos.

- Dictámenes Periciales (Peritajes médicos- científicos) a nivel Nacional
- Todas las Especialidades Médicas
- Auditoria Médica (Pre procesal y Procesal)
- Auditoria Jurídica (Pre procesal y Procesal)

Busca asesorar en asuntos judiciales con trasparencia y responsabilidad, reconociendo el conocimiento científico, respaldando el pago de honorarios según la especialidad y complejidad.

Ilustración 1: Logo C&C Corporación Justicia para Todos

5 MARCO CONCEPTUAL - "ESTADO ARTE"

5.1 ANTECEDENTES

En los últimos años varios visionarios en los temas de gobiernos de seguridad han sugerido metodologías para integrar en un mismo ambiente el marco de referencia COBIT y la norma ISO 27001; estos trabajos en su mayoría se fundamentan solo en el aspecto teórico, proponiendo modelos como los alumnos de la 1Universidad Piloto de Colombia; en su artículo guiado por el ciclo PHVA. El objetivo es integra los controles de ISO 27001 ayudando a fortalecer y guiar la implementación del SGSI en beneficio de la información en las organizaciones. Requiere para su implementación tener una estructura ya creada de procesos e infraestructura de seguridad.

El modelo que proponemos a diferencia de lo anterior radica en que no requiere obligatoriamente una infraestructura ya creada o ser una empresa muy robusta para su implementación, por lo que nuestro nicho de acción son las pequeñas y medianas empresas. Nuestro modelo es flexible y se basa en el autodiagnóstico de manera que la compañía puede iniciar su SGSI desde cero e ir creciendo en la medida de sus posibilidades. Es aquí cuando el continuo seguimiento y retroalimentación de nuestro aplicativo con el acompañamiento y experticia de nuestros consultores juega un papel importante ya que se ajusta a las necesidades propias de la empresa y no a las necesidades del auditor (3).

Tenemos claro que la implementación del gobierno de seguridad de la información cobra su mayor auge por la necesidad y el cumplimiento de los requerimientos normativos, no podemos desconocer que este no es una camisa de fuerza para la organización que en vez de facilitar los procesos de la compañía genera sobrecarga en la operación por tediosas y complicadas tareas.

El ciclo PHVA muestra una propuesta de autodiagnóstico y seguimiento garantizando el compromiso de la empresa y los directivos, adicional a que les permite tener una consulta de resultados obtenidos de manera interactiva gracias al almacenamiento de los datos en el aplicativo.

2ISACA nos propone un programa de evaluación de COBIT para ayudar a las empresas a asegurar sus procesos; fundamentada en los procesos de calidad de sus resultados y la maximización de las inversiones en TI

5.2 NECESIDAD DE LAS PEQUEÑAS EMPRESAS TENER UN SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN.

Colombia es pionera en América Latina en seguridad de la información al incorporar las recomendaciones y las[3] mejores prácticas internacionales según la revista la republica LA, en su

[1] http://polux.unipiloto.edu.co:8080/00000825.pdf

[2] http://www.cioal.com/2011/12/26/isaca-presenta-un-programa-de-evaluacion-de-cobit-para-ayudar-a-las-empresas-a-asegurar-sus-procesos/

[2] http://acis.org.co/revista143/content

[3] https://www.larepublica.co/empresas/colombia-es-pionera-en-america-latina-en-seguridad-digital-2392666

publicación del jueves 23 del 2016 por Lina Orozco, teniendo muy claro que la gestión es la mejor herramienta de la prevención de la seguridad. El fortalecimiento y la defensa del recurso más susceptible de una compañía "**la información**", pero las grandes empresas reconocen el esfuerzo realizado y las batallas ganadas (5).

Las pequeñas y medianas empresas no se han concientizado de todos peligros que tiene su información, actualmente se ha venido incrementando los ataques, donde aprovechan las vulnerabilidades de las compañías permitiendo el plagio o robo de información valiosa.

En la tesis de grado Diseño Políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO, de la universidad San Buenaventura muestran que de 100 empresas que propusieron validar los niveles de seguridad en la compañía, solo 16 aceptaron el reto.

Resultado de Llamada	No. Empresas	%
Cambio constante de instalaciones- cambio de domicilio	16	16 %
No están interesados	47	47 %
No definen Visita	21	21 %
Aceptan Visita de análisis	16	16 %

*Tabla 2: Invitación análisis de información **(6)***

Fuente: Tesis de grado Diseño de políticas y controles para la seguridad de la información en pequeñas Empresas con redes SOHO en el sector transporte de Bogotá Universidad San Buenaventura[4].

La seguridad de la información es un carácter bidimensional no es solo de carácter técnico al tener la tecnología de punta la cual requiere un capital elevado, sino el uso adecuado de mecanismo de seguridad (Políticas, estándares, reglas, etc.) que se encuentra ligada a la interacción con los seres humanos. Es una cultura que debemos centralizar en las compañías [5]al crear un ejercicio de comportamientos del tratamiento de la información (7).

Sabemos que en las pequeñas empresas es más fácil realizar un análisis de riesgos o creación de políticas que cuando una compañía es grande, la cultura de la información es una forma de hacer negocios, al tener un respaldo ante nuestros clientes, proveedores y stakeholders, en el caso de C&C CORPORACIÓN reconoce que las historias clínicas son información confidencial que debe ser salvaguarda.

La implementación de un Sistema de Gestión de Seguridad de la Información SGSI, en las pequeñas y medianas compañías, nace como la necesidad de crear una metodología organizacional para salvaguardar los diferentes activos de estas. Los costos elevados de una herramienta (programa de auditoría/consultoría), que brinda los controles generales y estado de madurez del

[4] http://bibliotecadigital.usb.edu.co/handle/10819/2952

[5] http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/134-cultura-de-seguridad-de-la-informaci%C3%B3n

SGSI en el mercado, pone una barrera a los directivos de estas compañías al no contar con el capital requerido.

Al realizar la investigación de programas y consultorías que alineen los marcos de referencia COBIT e ISO27001, y puedan ser aplicados o usados por distintas compañías sin importar su tamaño ni gentilicio, no se encontraron ni identificaron metodologías que alineen los objetivos del negocio con tecnología COBIT, con el referentes internacional ISO 27001 en la práctica, pero existen varias empresas desarrolladoras de herramientas para análisis del estado de madurez del SGSI en la compañías, las cuales solo manejan NORMA TÉCNICA NTC-ISO-IEC 27001, o como la organización ISACA, que teóricamente te da como debe ser aplicado su marco COBIT. A continuación, se describen 2 de ellas.

La empresa IT 360 de origen español y su herramienta ISOCRUNCH, la cual es útil para implementar un SGSI con la normatividad vigente en ISO 27001, evidencia la madurez de este y da una calificación para la certificación de la compañía. Genera un scoring de la gestión de riesgo identificados y la evolución del tratamiento de los mismo en relación a las soluciones planteadas por la empresa contratante, esta herramienta es aplicada solo para en las compañías que contraten los servicios de consultoría, esto significa que, si no adquiere los servicios de auditoría con personal de IT360, no puede adquirir la herramienta. (10)

En los servicios a contraer son:

- Análisis Inicial
- Levantamiento de información
- Cantidad de especialistas asignados
- Capacitación de la herramienta
- Capacitación de auditores internos
- Plan de trabajo
- Auditoria interna
- Plan de mejora
- Acompañamiento en Certificación.

Los costos varían en esta herramienta del tamaño de la compañía auditada, y la madurez del SGSI que se maneje:

- Implementación de la herramienta: US$ 4.512, la cual tiene asignado un usuario administrador, 3 operativos y 5 de consulta. (**12,829,465.92 COP)**
- Costo anual varía dependiendo del tamaño de la empresa US $ 1.000 (**2,843,410.00 COP)**
- Costo mensual por auditor asignado: US$ 3.000 (**8,530,230.00 COP)**
- Costo Horas Soporte; US$ 100 (**284,341.00 COP)**
- Cloud mensual 10 G de US$ 185 (**526,030.85 COP)**
- **Valor $ 1 USD = $ 2,843.41 COP**

La empresa de software ISOTools Excellence con su herramienta ISOTools SGSI, esta empresa multinacional con representación en Colombia ha desarrollado una herramienta que ayuda a implementar, mantener y validar la madurez del SGSI actual, maneja los diferentes controles para el

tratamiento de la información dependiendo del país origen de la compañía contratante; este permite a la compañía guiarse en cada uno de los requisitos de ISO 27001.

Los costos se dan de acuerdo al tamaño de la compañía, los cuales son:

- Modulo Base € 1.000 **($ 3,421,547 COP)**
- Modulo Calidad: € 500 **($ 1,710,774 COP)**
- Módulo de Seguridad de la información € 400 **($ 1,368,619 COP)**
- Usuario Administrador € 500 **($ 1,710,774 COP)**
- Usuario Responsable € 500 **($ 1,710,774 COP)**
- Usuario Operativo € 100 Euros por cada usuario mínimo 5 usuarios € 500 **($ 1,710,774 COP)**
- El costo a pagar anual son solo usuarios.
- Costo de horas soporte o capacitación € 80 hora **($ 273.724 COP)**
- Cloud mensual de 10G € 150 **($ 513.232 COP)**
- **Valor € 1 = $ 3.422 COP**

Nuestro proyecto ofrece el alineamiento de dos marcos de referencia al implementar ISO 27001, apoyado por COBIT aplicando los controles en tecnología de información que asegure:

- La manera efectiva, directa y clara del uso de la información.
- Asignación de los recursos necesarios y adecuados
- Garantías que la información es confiable, se encuentra disponible e integra
- El desarrollo de una estrategia que evidencie las 4 etapas de COBIT.
    - ✓ Planeación y organización en el manejo de las TI
    - ✓ Adquisición e implementación de las TI
    - ✓ Entregar y soporte la ejecución positiva de TI garantizando siempre la seguridad de la información
    - ✓ Seguimiento y evaluación que la compañía cumpla con la normatividad vigente en Colombia direccionado con los objetivos del negocio.

Este proyecto de grado está dirigido a pequeñas y medianas empresas que tienen limitaciones ocupacionales y financieras, las cuales se encuentran en un crecimiento y dependientes de un mercado, es por esta razón presentan limitaciones en la utilización de tecnologías costosas como las mencionadas anteriormente.

Es donde nuestra herramienta HEPALU Consulting Software, apoyara su proceso de SGSI, al potenciar la adaptabilidad de estructura tecnología y seguridad de la información de las empresas pequeñas y medianas, al ofrecer no una carga operativa adicional, sino una nueva metodología en la busca continua de la seguridad de la información, al mantener tareas periódicas, con bajos costos. Desarrollamos en la estrategia 41 controles, con 16 objetivos, 10 evaluaciones y 87 evidencias.

A continuación, realizamos una comparación

CARACTERÍSTICA /EMPRESA	HEPALU	ISOCRUNCH	ISOTools SGSI
Adquisición de la Plataforma	Donación	$ 12,829,466	$ 10,264,642
Horas Soporte	200.000	$ 284,341.00	$ 273.724
Mantenimiento Anual	Donación	$ 2,843,410.00	$ 5,132,321
Auditoria Acompañamiento	2.500.000	$ 8,530,230.00 (mensual)	$ 10.000.000
Acompañamiento en el proceso de Creación SGSI	1.000.000	0	$10.000.000
Cloud	N/A	$ 526,030.85	$ 513.232
Alineamiento COBIT	SI	NO	NO
Apoyo en la Documentación	SI	SI	NO
Evidencias	SI	NO	NO
Hallazgos	SI	SI	SI
Revisión Documental	SI	SI	SI
Conclusiones de Auditoria	SI	NO	NO
Seguimiento de la auditoria	SI	NO	NO
Informe de Auditoría	SI	NO	NO

Tabla 3: Tabla Comparaciones HEPALU - ISOCRUNH - ISOTools SGSI

5.3 COBIT – ISO 27001

A continuación, relacionamos nuestro primer acercamiento en donde hemos extraído del marco de referencia COBIT y de la NORMA TÉCNICA NTC-ISO-IEC 27001 SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, los controles y objetivos mínimos y alineados requeridos para la gestión de seguridad de la información y el inicio de modelo del mismo, con la construcción de nuestra herramienta para pequeñas y medianas empresas (3) (4).

COBIT 4. 1 y 5 (3)	**ISO 27001** (4)
Objetivo de control COBIT: • P02 Definir la Arquitectura de la Información	**Anexo A:** • A5 Políticas de la seguridad de la información • A6 Organización de La Seguridad de La Información
Alineación: Se debe establecer, formalizar, o crear un modelo para el manejo de la información, para que todas las partes de la Entidad hablen un mismo idioma, con unas reglas básicas de sintaxis, controles para la protección de este activo. Además, la existencia dirección y el liderazgo.	
Objetivo de control COBIT: • P07 Administrar los Recursos Humanos de TI	**Anexo A:** • A7 Seguridad de los Recursos Humanos
Alineación: Contar con mecanismos idóneos para la contratación de personal, con competencias, principios y valores para poder ejecutar las funciones asignadas con eficacia y eficiencia.	
Objetivo de control COBIT: • DS5 Garantizar la Seguridad de los Sistemas	**Anexo A:** • A8 Gestión de Activos • A9 Control de Acceso

	• A11 Seguridad Física y Del Entorno
Alineación: Para mantener la integridad de la información y de proteger los activos de TI y la Entidad, se requiere de un proceso de administración de la seguridad, el cual cuente con identificación de activos, perfiles para el acceso, controles para las operaciones y uso. Además, contar con controles ambientales y lógicos para proteger el recurso humano y el activo físico dentro y fuera de los perímetros de la Entidad	
Objetivo de control COBIT: • DS13 Administración de Operaciones	**Anexo A:** • A12 Seguridad de las Operaciones
Alineación: Asegurar la correcta operación y la seguridad de las instalaciones de procesamiento de información, con el fin de preservar la integridad, disponibilidad y confidencialidad, de este activo importante "Información"	
Objetivo de control COBIT: • AI3 Adquirir y Mantener Infraestructura Tecnológica	**Anexo A:** • A14 Adquisición, desarrollo y mantenimiento de sistemas
Alineación: Se deben formalizar y ejecutar procesos para adquirir, Implementar y actualizar la infraestructura tecnológica, con el fi, que estos activos cumplan con los objetivos para los cuales fuere adquiridos y puedan prestar los servicios con los controles adecuados.	
Objetivo de control COBIT: • DS2 Administrar los Servicios de Terceros	**Anexo A:** • A15 Relaciones con los Proveedores
Alineación: Contar con controles y salvaguardas para la protección de los activos y servicios de la organización que sean accesibles a los proveedores, evitando daños, modificación, fugas o perdidas de estos.	
Objetivo de control COBIT: • DS8 Administrar la Mesa de Servicio y los Incidentes.	**Anexo A:** • A16 Gestión de Incidentes de Seguridad de la Información
Alineación: Contar con un proceso o enfoque coherente y eficaz para la gestión de problemas e incidentes de seguridad de la información, que incluya registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución.	
Objetivo de control COBIT: • DS4 Garantizar la Continuidad del Servicio	**Anexo A:** • A17 Aspectos de Seguridad de La Información de la Gestión de Continuidad de Negocio
Alineación: En caso de un evento adverso, poder retornar a la operación normal de la Entidad en todos sus procesos incluyendo Seguridad de la información (Resiliencia)	
Objetivo de control COBIT: • ME3 Garantizar el Cumplimiento con Requerimientos Externos	**Anexo A:** • A18 Cumplimiento
Alineación: Cumplir con los requerimientos legales y jurídicos donde opere la Entidad	

Tabla 4: COBIT – ISO 27001

6 DESARROLLO Y METODOLOGÍA

6.1 REGLAS DE SINTAXIS PARA EL FUNCIONAMIENTO DE LA HERRAMIENTA

Se definieron 5 fases para la aplicación de nuestra metodología HEPALU, en donde cada uno define los controles mínimos requeridos para empezar a estructurara un modelo de seguridad de la información alineados con los objetivos de tecnología, esto con el fin, de dar a cada empresa que adquiere los servicios con **HEPALU Consulting Software** una fácil y clara forma de entender las oportunidades de mejora u observaciones que den como resultado, para la construcción de su modelo a continuación se definen.

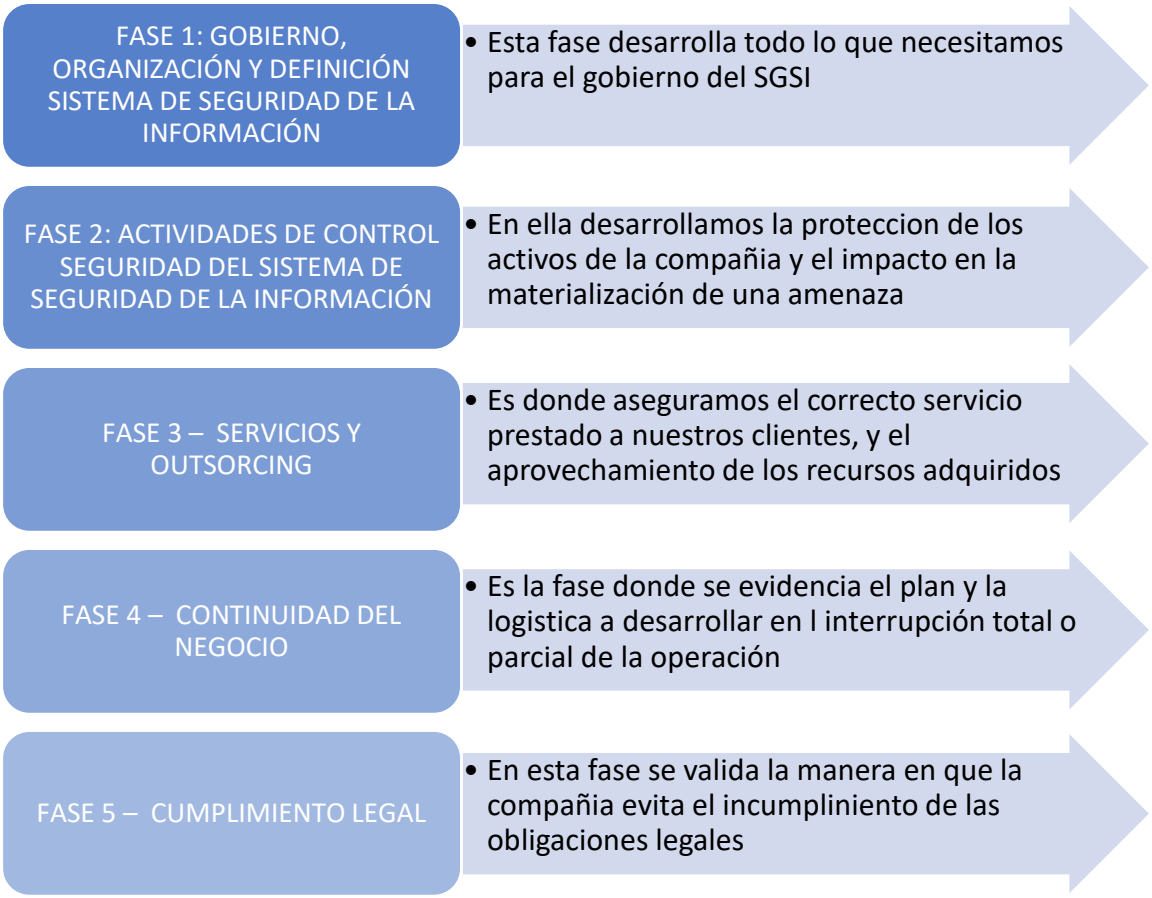


Ilustración 2: Fase En El Funcionamiento De La Herramienta

6.1.1 FASE 1: GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El gobierno corporativo es la estructura organizacional y dirección en la toma de decisiones, en él se definen los roles y responsabilidades del SGSI, permitiendo proveer la operación estratégica en la manera de actuar en caso de eventualidades, desarrolla la orientación para obtener una respuesta de manera inmediata y apropiada, con los recursos necesarios. Adicionalmente ayuda a alinear la visión a tener para el éxito del SGSI.

Fase 1: GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Gobierno de Seguridad de Información**
ISO - A5 Políticas de la seguridad de la información	
Objetivo	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes
Controles	**Evidencias**
Existe una/un conjunto de política de seguridad de la información	✓ Políticas, procedimientos y actividades de seguridad de la información
La política se encuentra debidamente firmada y aprobada por la alta gerencia	✓ Firma de la política, divulgación, aceptación en comités directivos
Ha sido divulgada y firmada por los funcionarios que la reconocen y la han leído	✓ Firma de empleado de la aceptación de la política y de su lectura
Se hace campañas de concienciación	✓ Documentos, correos, carteles, talleres entre otros, donde se observe el tema de la seguridad de la información
La política es evaluada periódicamente con el fin de mantenerla actualizada	✓ Fechas de actualizaciones y modificación, esto debe ser formal e informado en comités
ISO - A6 Organización de La Seguridad de La Información	
Objetivo	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización
Controles	**Evidencias**
Definición clara roles y responsabilidades sobre la seguridad de la información	✓ Definición a través de roles, perfiles y hojas de vida de cargos, la función de Seguridad de la Información
Separación y debida segregación de deberes de la Seguridad de la Información	✓ Verificar que la función de SI, no dependa de funciones que generen conflicto, ejemplo (SI -TI, SI – Contabilidad, SI - Auditoría)
Agenda, conocimiento y contactos con autoridades y grupos especiales de interés	✓ Registro y agendas con las autoridades pertinentes y grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
Existencia del Rol de Seguridad de la información en la gestión de proyectos	✓ Procedimientos, actividades, roles, en los proyectos de la empresa, como gestor de seguridad de la información

Tabla 5: Fase 1 Gobierno Seguridad De La Información

Fase 1: GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Riesgos de la seguridad de la información y tecnología**
COBIT - P02. Definir la Arquitectura de la Información.	
Objetivo	La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.
Controles	**Evidencias**
Existencia y definición de un esquema de Clasificación de Datos	✓ Existencia de un esquema de clasificación que aplique a toda la empresa, basado en que tan critica y sensible es la información (publica, confidencial, secreta entre otros) Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad
Gestión de la Integridad en la información guardada, modificada o enviada.	✓ Procedimientos, actividades para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.
Diccionario de Datos Empresarial, inventario de interfaces y Reglas de Sintaxis de Datos	✓ El diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización.
	✓ Inventario de interfaces y el tipo de información que se comparte con sus controles
ISO - A7 Seguridad de los Recursos Humanos	
Objetivo	Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI y de la organización, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar.
Controles	**Evidencias**
Establecimiento de un Marco de Trabajo de Administración de Riesgo	✓ Políticas, procedimientos, actividades relacionadas con la identificación de riesgos de la organización, incluyendo los de TI
Establecimiento del Contexto del Riesgo	✓ Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto significa, a verificación del ambiente y entorno en el que se esta trabajando
Evaluación de Riesgos de TI y de la Entidad, y la Identificación de Eventos	✓ Metodología de evaluación de forma recurrente la probabilidad e
	✓ Matrices de riesgos.
	✓ Incidentes de riesgos
	✓ Actualización de lo anterior.

Tabla 6: Fase 1 Riesgos de la seguridad de la información y tecnología

FASE 2 – ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Recursos Humanos**
ISO - A7: Seguridad de los Recursos Humanos	
Objetivo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran
COBIT - P07. Administrar los Recursos Humanos de TI.	
Objetivo	Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo practicas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.
Controles	**Evidencias**
Reclutamiento y Retención del Personal	✓ Procesos de reclutamiento
	✓ Alineación acuerdo a las políticas y procedimientos generales de personal de la organización
Selección y términos y condiciones del empleo	✓ Estudios de seguridad
	✓ Referencias
	✓ Documentación validad de la persona a contratar
	✓ Acuerdos contractuales
Asignación de Roles	✓ Perfil del trabajador
	✓ Actividades del trabajador
	✓ Definición del puesto de trabajo
	✓ Certificaciones, estudios o capacitaciones mínimos para el cumplimiento de labor
Entrenamiento del Personal de la organización, incluyendo	✓ entrenamiento
	✓ Cursos, diplomados para los funcionarios
	✓ Beneficios o formas para hacer que los trabajadores estudien
Evaluación y gestión del desempeño del Empleado	✓ Evaluaciones de desempeño.
	✓ Objetivos individuales derivados de las metas organizacionales.
	✓ Estándares establecidos y responsabilidades específicas del puesto

Tabla 7: Fase 2 Recursos Humanos

6.1.2 FASE 2 – ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

En esta fase se valida los controles de seguridad a los diferentes activos de la compañía auditada, busca asegurar y clasificar todos los activos:

- ✓ Financieros
- ✓ Legales
- ✓ Estratégicos
- ✓ Tecnológicos
- ✓ Personales entre otros.

FASE 2 – ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Seguridad De Los Activos**
ISO - A9 Control de Acceso	
Objetivo	Limitar el acceso a información y a instalaciones de procesamiento de información
Controles	**Evidencias**
Contar con políticas o esquemas para la	✓ Política de control de acceso ✓ Política de acceso y servicio a red

Tabla 8: Fase 2 Seguridad De Los Activos (1)

FASE 2 – ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Seguridad De Los Activos**
ISO - A9 Control de Acceso	
Objetivo	Limitar el acceso a información y a instalaciones de procesamiento de información
Controles	**Evidencias**
Contar con políticas o esquemas para la	✓ Política de control de acceso ✓ Política de acceso y servicio a red
ISO - A11 Seguridad Física y Del Entorno	
Objetivo	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización
Controles	**Evidencias**
Existencia de esquemas de seguridad perimetral	✓ Política de seguridad física ✓ Mecanismo de protección de activos físicos ✓ Bitácoras de acceso de dispositivos
COBIT - DS5 Garantizar la Seguridad de los Sistemas	
Objetivo	La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad , políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados . Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.
Controles	**Evidencias**
Procedimiento o esquemas para la administración de Identidad y cuentas de usuarios	✓ Política de gestión de identidad ✓ Matrices o actividades para relacionar los roles de los usuarios ✓ Procedimiento de creación de cuentas de usuario

Tabla 9: Fase 2 Seguridad De Los Activos (2)

FASE 2 – ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
Nombre de la evaluación	**Seguridad En Las Operaciones De La Entidad**
A12 Seguridad de las Operaciones	
Objetivo	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
DS13 Administración de Operaciones	
Objetivo	Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.
Controles	**Evidencias**
Esquema de protección de las operaciones en la Organización	✓ Procedimientos para el monitoreo de la Infraestructura de TI
	✓ Procedimientos estándar para operaciones de TI y áreas criticas de la entidad que garantizan que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos
	✓ Procedimientos para establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad

Tabla 10: Fase 2 Seguridad En Las Operaciones De La Entidad

6.1.3 FASE 3 – SERVICIOS Y OUTSORCING

En esta fase estructuramos la manera de actuar frente a los servicios prestados a clientes y proveedores que prestan un servicio a la empresa auditada, asegurando el cumplimiento de las responsabilidades y el adecuado aprovechamiento de las herramientas adquiridas.

Validar el desarrollo del plan de trabajado con los clientes, permitiendo mejorar los niveles de servicio y la imagen de la compañía auditada

FASE 3 – SERVICIOS Y OUTSORCING	
Nombre de la evaluación	**Adquisiciones**
A15 Relaciones Con Los Proveedores	
Objetivo	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
Controles	**Evidencias**
Gestión o actividades para la adquisición de recursos críticos	✓ Plan de Adquisición de Infraestructura Tecnológica ✓ Mantenimiento de la Infraestructura ✓ Protección y Disponibilidad del Recurso de Infraestructura

Tabla 11: Fase 3 Adquisiciones

FASE 3 – SERVICIOS Y OUTSORCING	
Nombre de la evaluación	**Proveedores**
DS2 Administrar Los Servicios de Terceros	
Objetivo	La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.
Controles	**Evidencias**
Contar con políticas, procedimientos o actividades de contratación	✓ Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y su documentación
Actividades establecidas para mitigar los riesgos del proveedor	✓ Procedimientos, actividades o políticas para identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad.
Procedimientos para evaluar el desempeño del proveedor	✓ Encuesta de calidad ✓ Calificación proveedor ✓ SLA o OLA
Esquemas de Tratamiento de la seguridad dentro de los acuerdos con proveedores	✓ Acuerdos establecidos y acordados con todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso.

Tabla 12: Fase 3 Proveedores

FASE 3 – SERVICIOS Y OUTSORCING	
Nombre de la evaluación	**Mesa De Ayuda**
A16 Gestión De Incidentes De Seguridad De La Información	
Objetivo	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
DS8 Administrara La Mesa De Servicios Y Los Incidentes.	
Objetivo	Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.
Controles	**Evidencias**
Gestión o actividades para la adquisición de recursos críticos	✓ Establecer la función de mesa de servicio, o el organismo que haga las
	✓ Procedimientos para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados.
	✓ Los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información.
	✓ Encuestas de satisfacción del usuario final respecto a la calidad de la mesa de servicios o del organismo que haga la función de esta.
Actividades para la gestión de incidentes	✓ Responsabilidades y procedimientos de gestión de incidencias.
	✓ Formalización de los canales de reporte de incidentes
	✓ Metodología para la evaluación de los incidentes
	✓ Procedimientos o actividades para el cierre de incidentes
Procedimientos de benchmarking y análisis de tendencias	✓ Procedimiento para emitir reportes de la actividad de la mesa de servicios o que haga la función de esta, y gestor de incidentes para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta.
	✓ Actividades para análisis del entorno y verificación de actualidad

Tabla 13: Mesa de Ayuda

6.1.4 FASE 4 CONTINUIDAD DEL NEGOCIO

En esta fase se desarrolla el plan operacional y el marco logístico que brinda la resiliencia en caso de presentar un incidente que imposibilite la operación de la compañía de manera parcial o total. Se debe detallar desde el análisis crítico, el desarrollo de toma de decisiones y la capacitación a los empleados en la manera de actuar caso de interrupciones de servicio.

FASE 4 – CONTINUIDAD DEL NEGOCIO	
Nombre de la evaluación	**Continuación De La operación Del Negocio**
eA17 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio	
Objetivo	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización
DS4 Garantizar La Continuidad Del Servicio	
Objetivo	La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio
Controles	**Evidencias**
Gestión o actividades para la adquisición de recursos críticos	✓ Análisis critico de todas las áreas
	✓ Análisis critico de los sistemas de información
	✓ Análisis de cargos críticos
Plan de continuidad del negocio	✓ Plan de continuidad de negocio
	✓ Actualización del plan de negocio
	✓ Alineación de impacto de los servicios críticos y su restauración
Plan de continuidad de la Seguridad de la información	✓ Plan de continuidad de Seguridad de la información
	✓ Actualización del plan
Pruebas de los planes	✓ Resultados de las pruebas de continuidad
	✓ Lecciones aprendidas
	✓ Procedimientos para actualización y mejora del plan de continuidad y de seguridad según las pruebas realizadas
Entrenamiento del plan de continuidad	✓ Actividades para la realización de capacitación
	✓ Actas o listados de capacitación
	✓ Periodicidad de entrenamiento

Tabla 14: Fase 4 Continuación De La operación Del Negocio

6.1.5 FASE 5 – CUMPLIMIENTO LEGAL

El cumplimiento de los requisitos legales es uno de los controles importantes del SGSI, es donde validamos las particularidades y aspectos legales a cumplir la compañía auditada, para esto es necesario validar que la compañía cumpla con:

- ✓ Realizar las revisiones y verificaciones contantes del marco normativo y legal, ya que este constantemente varía y cambian en el país de operación
- ✓ Planear la manera de actuar al cumplimiento del marco normativo y legal.
- ✓ Validar la ejecución y el cumplimiento de todo el marco normativo y legal

FASE 5 – CUMPLIMIENTO LEGAL	
Nombre de la evaluación	**Marco Legal o Estatuario**
A18 CUMPLIMIENTO	
Objetivo	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad
ME3 Garantizar el Cumplimiento con Requerimientos Externos	
Objetivo	Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio
Controles	**Evidencias**
Actividades para la Identificación Leyes, Regulaciones y Cumplimientos	✓ Inventario de leyes, regulaciones, requerimientos externos locales e internacionales, que la Entidad debe de cumplir.
	✓ Alineación de los requerimientos externos con políticas, estándares, procedimientos y metodologías de la organización.
Metodología de respuesta a Requerimientos Externos	✓ Procedimientos y metodologías de TI y Seguridad para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados como es requerido
Esquemas para mantener la privacidad y protección de información de datos personales	✓ Procedimientos para asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

Tabla 15: Fase 5 Marco Legal o Estatuario

6.2 HERRAMIENTA HEPALU

6.2.1 DESCRIPCIÓN DEL SISTEMA

Esta herramienta fue desarrollada con las siguientes características:

- ✓ lenguaje de desarrollo c# .net
- ✓ Base de datos SQL 2014
- ✓ Componente para reportes Devexpress

HEPALU es una herramienta de auditoria y /o consultoría que sirva o pueda implementarse para crear o alinear un sistema de gestión de seguridad de la información, basado en marcos de referencia, mejores prácticas y estándares reconocidos internacionalmente, a partir de las directrices, políticas, lineamientos y procedimientos que surgen como oportunidades de mejora; cumpliendo las expectativas de la gerencia, sin importar su actividad económica.

Ilustración 3: Presentación de Herramienta HEPALU

Les recomendamos para ver el video de la presentación ctrl + click en la imagen

A continuación, una leve descripción grafica con la explicación de la misma:

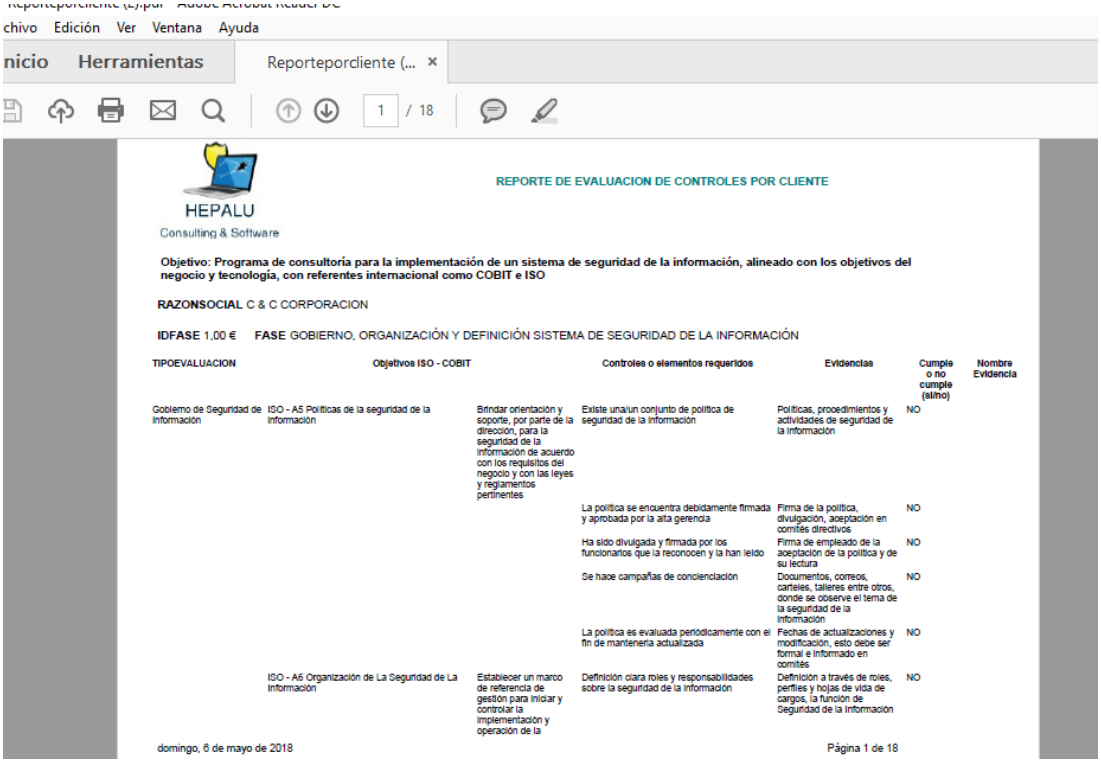
Ilustración 4: Pantalla Inicial HEPALU

Panta inicial del programa, donde permite al funcionario y/o consultar elegir donde ingresara, eligiendo actividades como reportes, calificación, controles, evaluación entre otros.

Ilustración 5: Menús Desplegables HEPALU

Cada menú es despegable, donde podrá seleccionar diferentes menús, los cuales son intuitivos.

Dentro de la misma, se puede ver y conservar los reporte e informes de las consultorías



chivo Edición Ver Ventana Ayuda

nicio Herramientas Reporteporcliente (... ×

1 / 18

HEPALU
Consulting & Software

REPORTE DE EVALUACION DE CONTROLES POR CLIENTE

Objetivo: Programa de consultoría para la implementación de un sistema de seguridad de la información, alineado con los objetivos del negocio y tecnología, con referentes internacional como COBIT e ISO

RAZONSOCIAL C & C CORPORACION

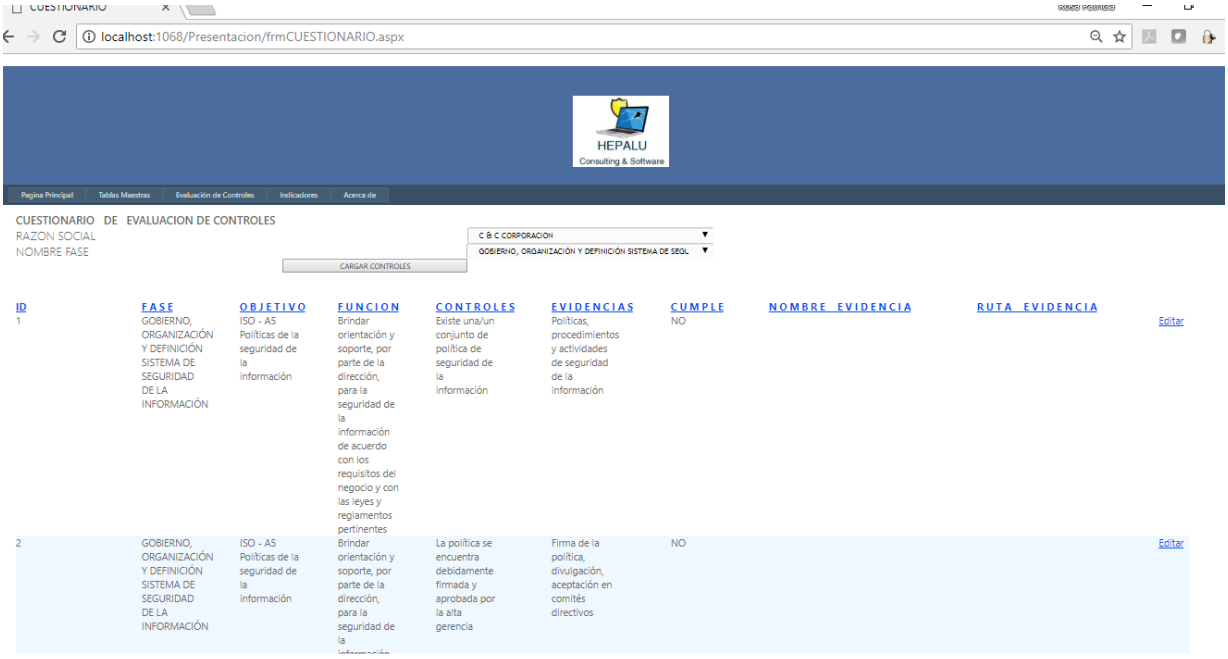
IDFASE 1,00 € **FASE** GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

TIPOEVALUACION	Objetivos ISO - COBIT		Controles o elementos requeridos	Evidencias	Cumple o no cumple (si/no)	Nombre Evidencia
Gobierno de Seguridad de Información	ISO - A5 Políticas de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	Existe una/un conjunto de política de seguridad de la información	Políticas, procedimientos y actividades de seguridad de la información	NO	
			La política se encuentra debidamente firmada y aprobada por la alta gerencia	Firma de la política, divulgación, aceptación en comités directivos	NO	
			Ha sido divulgada y firmada por los funcionarios que la reconocen y la han leído	Firma de empleado de la aceptación de la política y de su lectura	NO	
			Se hace campañas de concienciación	Documentos, correos, carteles, talleres entre otros, donde se observe el tema de la seguridad de la información	NO	
			La política es evaluada periódicamente con el fin de mantenerla actualizada	Fechas de actualizaciones y modificación, esto debe ser formal e informado en comités	NO	
	ISO - A6 Organización de La Seguridad de La Información	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la	Definición clara roles y responsabilidades sobre la seguridad de la información	Definición a través de roles, perfiles y hojas de vida de cargos, la función de Seguridad de la información	NO	

domingo, 6 de mayo de 2018 Página 1 de 18

Ilustración 6: Reporte PDF HEPALU

Los reportes pueden ser extraídos en formato PDF, los cuales se entregan a la empresa evaluada.



localhost:1068/Presentacion/frmCUESTIONARIO.aspx

HEPALU
Consulting & Software

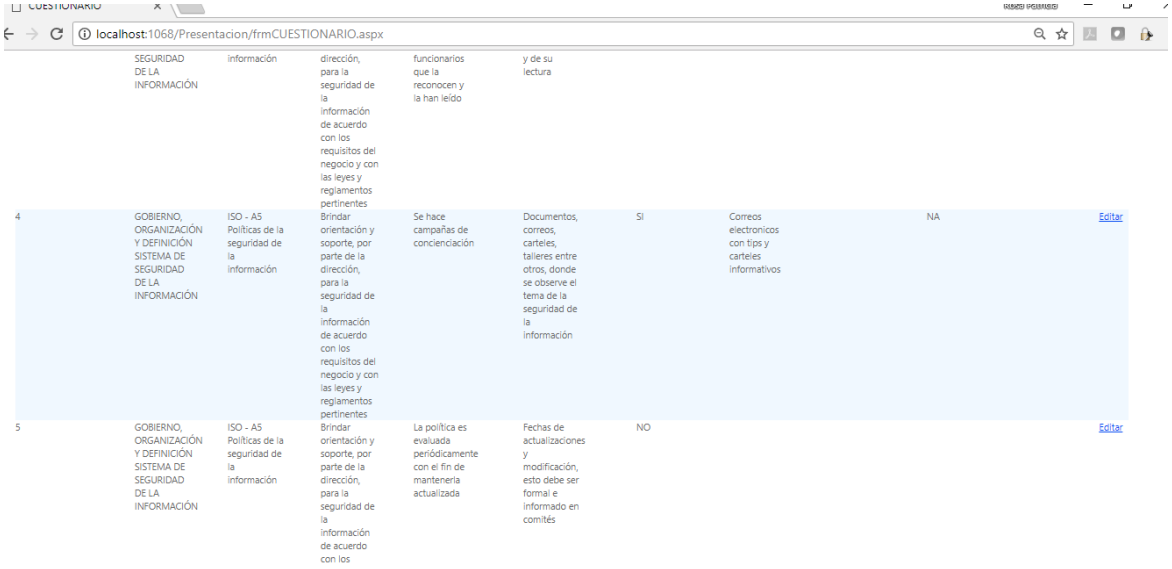
Pagina Principal | Tablas Maestras | Evaluación de Controles | Indicadores | Acerca de

CUESTIONARIO DE EVALUACION DE CONTROLES
RAZON SOCIAL C & C CORPORACION
NOMBRE FASE GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGU
CARGAR CONTROLES

ID	FASE	OBJETIVO	FUNCION	CONTROLES	EVIDENCIAS	CUMPLE	NOMBRE EVIDENCIA	RUTA EVIDENCIA	
1	GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A5 Políticas de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	Existe una/un conjunto de política de seguridad de la información	Políticas, procedimientos y actividades de seguridad de la información	NO			Editar
2	GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A5 Políticas de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la	La política se encuentra debidamente firmada y aprobada por la alta gerencia	Firma de la política, divulgación, aceptación en comités directivos	NO			Editar

Ilustración 7: Visor de Ayuda al Consultor

Vista de solicitud de información y ayuda al consulto o auditor, donde se encuentra ordenadamente los pasos y fases que se deben seguir para aplicar.



	SEGURIDAD DE LA INFORMACIÓN	información	dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	funcionarios que la reconocen y la han leído	y de su lectura				
4	GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A5 Políticas de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	Se hace campañas de concienciación	Documentos, correos, carteles, talleres entre otros, donde se observe el tema de la seguridad de la información	SI	Correos electronicos con tips y carteles informativos	NA	Editar
5	GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A5 Políticas de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los	La política es evaluada periódicamente con el fin de mantenerla actualizada	Fechas de actualizaciones y modificación, esto debe ser formal e informado en comités	NO			Editar

Ilustración 8: Reporte de Calificación. Evaluación Madurez SGSI

Procedimiento de calificación del modelo con la información de la empresa piloto

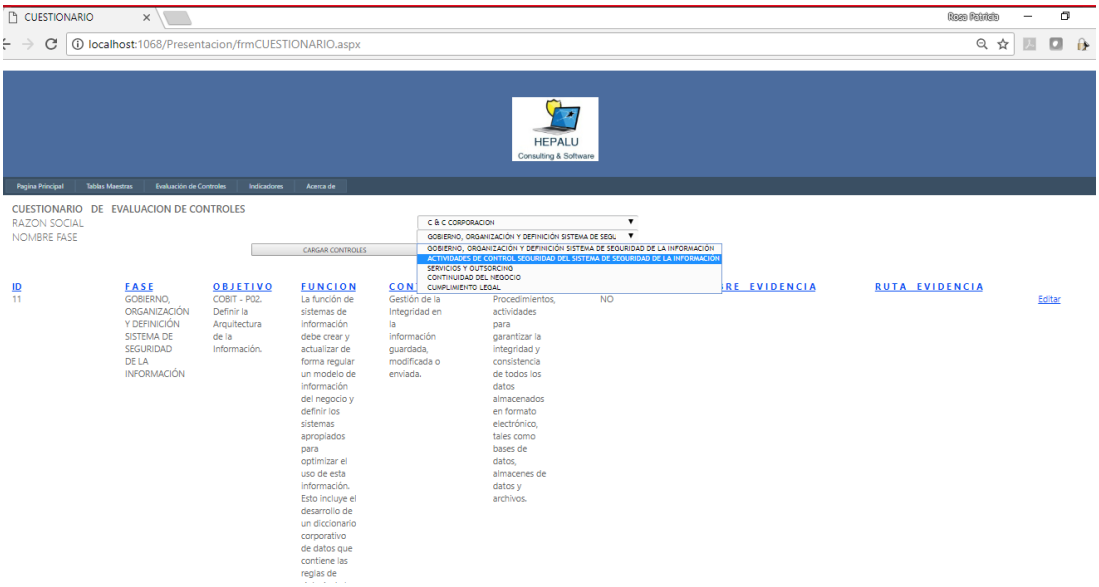
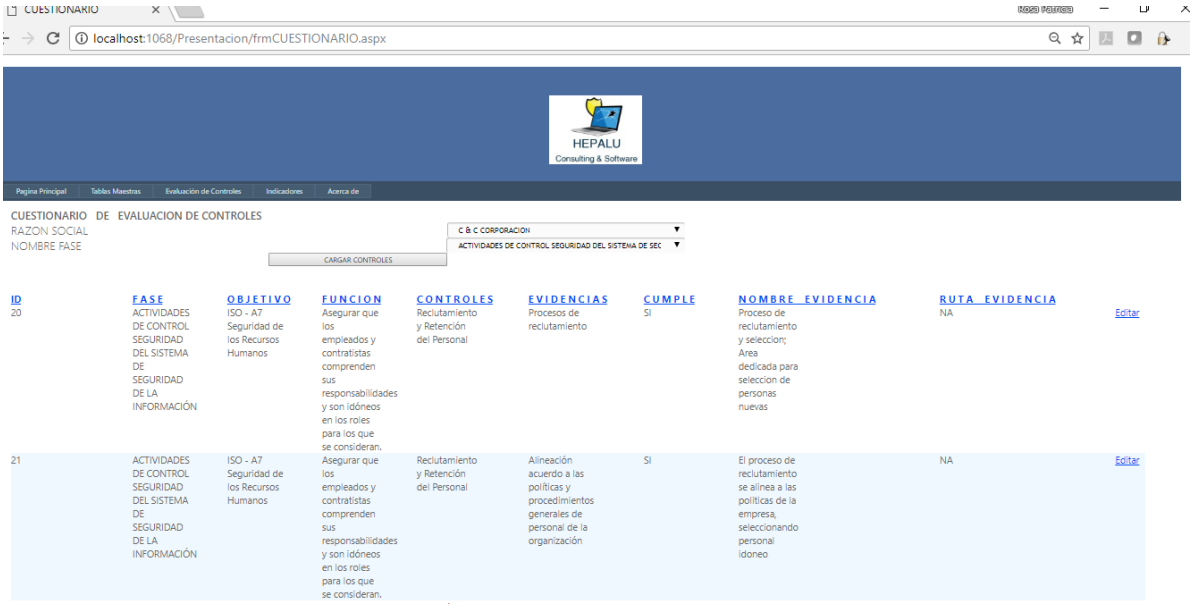


Ilustración 9: Desarrollo de 5 Fases (1)

En la vista se observa las cinco fases, el programa permite calificación desorganizada o simplemente de las fases que se quieran evaluar.



ID	FASE	OBJETIVO	FUNCION	CONTROLES	EVIDENCIAS	CUMPLE	NOMBRE EVIDENCIA	RUTA EVIDENCIA	
20	ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A7 Seguridad de los Recursos Humanos	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	Reclutamiento y Retención del Personal	Procesos de reclutamiento	SI	Proceso de reclutamiento y seleccion; Area dedicada para seleccion de personas nuevas	NA	Editar
21	ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	ISO - A7 Seguridad de los Recursos Humanos	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	Reclutamiento y Retención del Personal	Alineación acuerdo a las políticas y procedimientos generales de personal de la organización	SI	El proceso de reclutamiento se alinea a las políticas de la empresa, seleccionando personal idoneo	NA	Editar

Ilustración 10: Desarrollo de 5 Fases (2)

Ejemplo de otra fase con los datos proporcionados por la empresa

6.2.2 MODELO ENTIDAD RELACIÓN

Este es el modelo entidad relación creado para HEPALU CONSULTING SOFTWARE, el cual representa los campo y las relaciones existentes y sus propiedades con el Software.

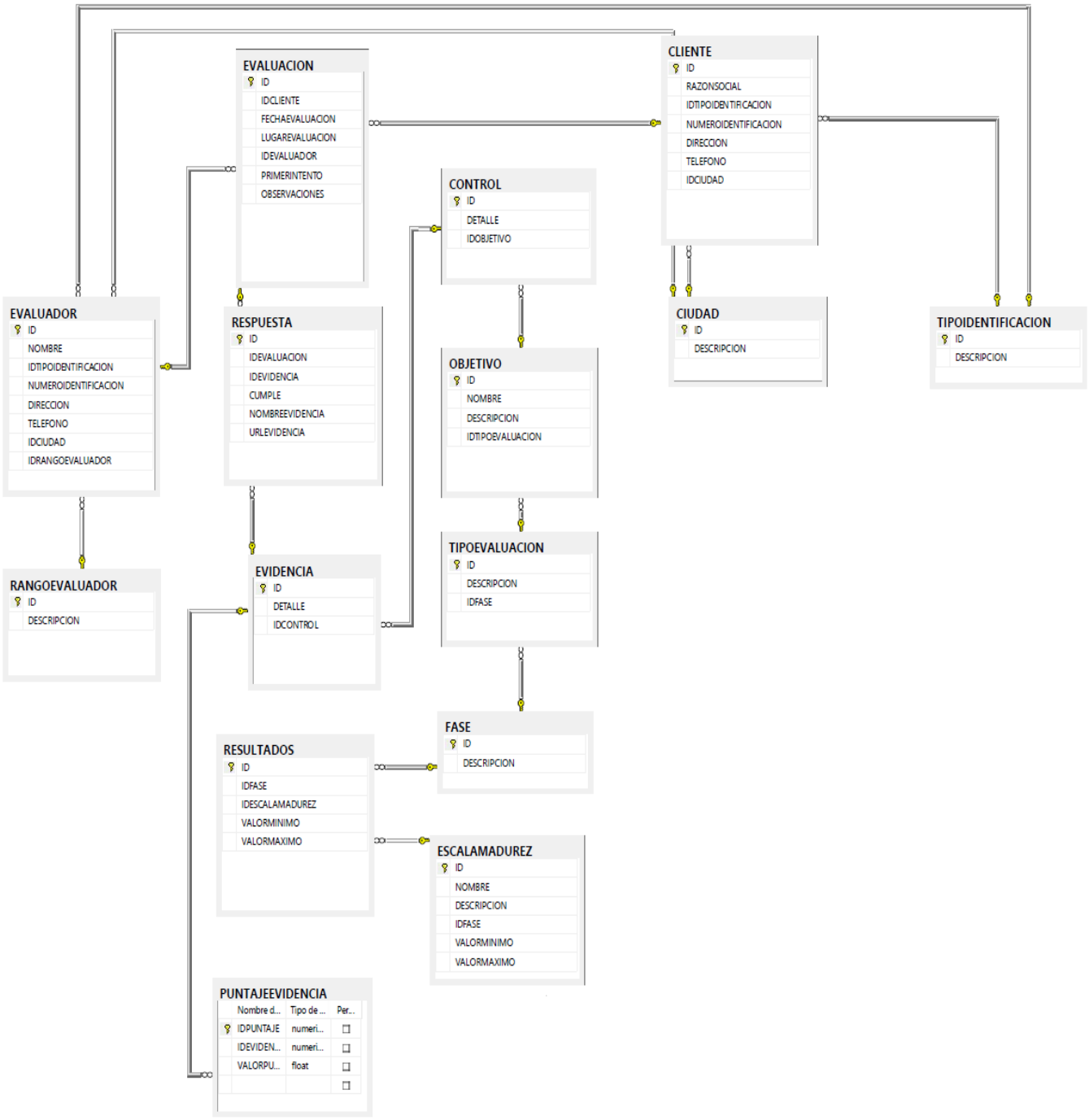


Ilustración 11: Modelo Entidad Relación HEPALU

6.3 RESULTADOS EMPRESA PILOTO

Una vez aplicada la metodología empelada en el trabajo de grado, identificamos las oportunidades de mejora que pueden encaminar a la empresa a la protección de la información:

Dentro de las cinco fases, los resultados arrojaron niveles de:

1. Fase 1 GOBIERNO, ORGANIZACIÓN Y DEFINICIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN: **No existente**, donde se observa que el gobierno de seguridad de la información no se ha tenido en cuenta dentro de la estrategia de la empresa, donde no se ha clasificado la información y aplicado controles para la protección de la misma.

2. Fase 2 ACTIVIDADES DE CONTROL SEGURIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN: **Repetible**, cuando se realizó el levantamiento de la información, se analizó y observó que muchas actividades de protección de la información la hacen por instinto o porque son actividades que repiten a diario con las mejores medias de control, sin embargo, estas no se encuentran definidas, documentadas ni formalizadas.

3. Fase 3 SERVICIOS Y OUTSORCING: **Repetible**, se cuentan con procedimientos para la adquisición de activos de información y selección de personal, minimizando los riesgos que esto conlleva, estas actividades están delegadas a las personas, que por su actividad diaria hacen los mejores procesos intuitivamente evitando problemas.

4. Fase 4 CONTINUIDAD DEL NEGOCIO: **Inicial,** se cuenta con procesos establecidos para la recuperación del negocio, el encargado de tecnología conoce las herramientas a reestablecer, los funcionarios operativos conocen de forma estructurada que hace en caso de que no se puede ejecutar la funcionas.

5. Fase 5 CUMPLIMIENTO LEGAL: **Repetible**, esta fase es una las notas más elevadas, ya que la empresa cuenta con unas actividades sobre todos los requerimientos legales, conocen los incumplimiento y sanciones que podrían incurrir y trabajan en ellos para evitarlo, si embargo, no ha formalizado los riesgos o identificados

Esta información fue obtenía al aplicar las actividades del presente trabajo de grado, la cual se observa en las siguientes imágenes extraídas del reporte de HEPALU Consulting & Software:

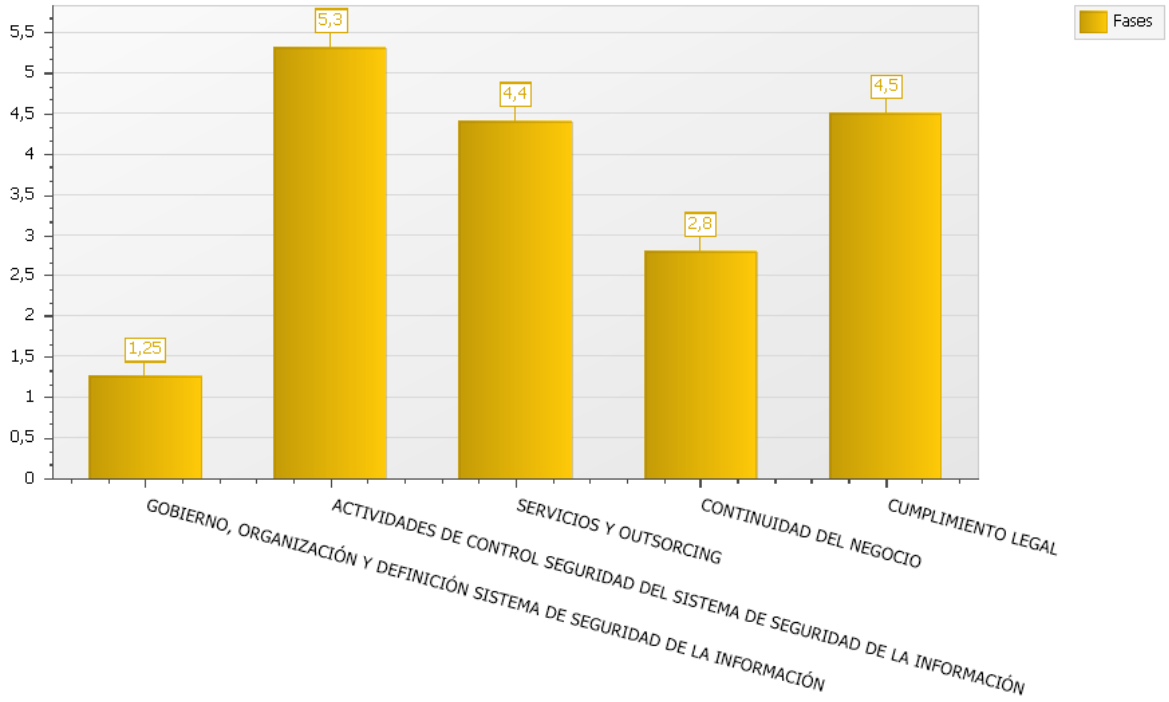


Ilustración 12: Grafica de Madurez SGSI C&C Corporación

FASE	ESCALA	DETALLE	VALOR PUNTAJE
Gobierno, organización y definición sistema de seguridad de la información	No existente	No se cuenta con o no se ha tenido la necesidad de dar organización a la infraestructura de la seguridad de la información o su respectivo gobierno	1
Actividades de control seguridad del sistema de seguridad de la información	Repetible	La adquisición de todo tipo de recursos se hace a través de actividades estructuradas	5
Servicios y outsorcing	Repetible	Los servicios prestados internamente o adquiridos se hacen a través de actividades estructuradas	4
Continuidad del negocio	Inicial	Algunas actividades pueden ser restablecidas a través de procesos ad – hoc desorganizados	3
Cumplimiento legal	Repetible	Se conocen la leyes y normatividad que la Entidad debe cumplir, pero las actividades no se realizan con el fin de cumplirlas.	5

Tabla 16: Tabla de Madurez SGSI C&C Corporación

La alta gerencia estuvo de acuerdo con la escala, lo propuesto y pondrá en práctica en planes de acción las mejoras dadas.

Nota: debido a las cláusulas de confidencialidad establecida con la empresa, se debe omitir información que, al caer en manos de terceros, pueda afectar la imagen o exploten estos riesgos.

6.4 ENTREGABLES

A continuación relacionamos los diferentes entregables:

ENTREGABLE	ARCHIVO
Modelo Entidad Relación	(20180507)modelo entidad relacion.png
Presentación proyecto entrega final	(20180507) PRESENTACION PRO`
Video Funcionalidad De Herramienta HEPALU	https://www.youtube.com/watch?v=2kcte3-kc0Y&feature=youtu.be
Ejecutables	Instaladores.rar
Modelo Reporte Madurez HEPALU	Reportes.rar

7 CONCLUSIONES

Una vez concluido el desarrollo del trabajo de grado, la construcción de la herramienta y aplicación de esta en una empresa piloto, se identificó los siguientes aspectos:

1. Nos se identificaron o encontraron herramientas en el mercado, que alineen estos dos marcos de referencia.

2. La herramienta es intuitiva y puede desarrollarse en cualquier tipo de empresa.

3. La herramienta entrega con sus diferentes reportes el estado (madurez) de la empresa objetivo, entregando resultados de fácil entendimiento.

4. La empresa objetivo recibió y acepto con agrado los resultados.

5. Varios de los temas desarrollados en la estructura, no fueron entendidos o no se había interiorizado, sin embargo, una vez explicados fueron del agrado y de mejoramiento para la empresa piloto.

BIBLIOGRAFÍA

1. *Encuesta nacional de Seguridad informática 2017, Desafíos de la cuarta revolución industrial.* **Junco, Andrés Ricardo Almanza.** 2017, ACIS, págs. 18-36 .

2. **27000, ISO.** www.iso27000.es. [En línea] mayo de 2018. http://www.iso27000.es/download/doc_sgsi_all.pdf.

3. *¿Cómo integra COBIT 4.1 el estándar ISO 27001 para obtener un gobierno de seguridad de la información?* **Páez Yenny, Páez Yenny.** s.l. : Universidad Piloto.

4. *Colombia es Pionera en America Latina en Seguridad Digitañ.* **Orozco, Lina.** 23 Junio 2016 : s.n., 2016. https://www.larepublica.co/empresas/colombia-es-pionera-en-america-latina-en-seguridad-digital-2392666.

5. **Pulido Chadid, Andrea Marcela.** Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes soho en el sector transporte de Bogotá. *Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes soho en el sector transporte de Bogotá.* BOGOTA : Universidad Buenaventura, 2011.

6. *Cultura de seguridad de la información .* **Cano, Jeimy J.** 127, s.l. : ACIS- Revista Sistema. http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/134-cultura-de-seguridad-de-la-informaci%C3%B3n.

7. **ISOCRUNCH.** ISOCRUNCH FOR IT MANAGER. [En línea] http://www.isocrunch.com/.

8. **ITGI, ISACA -.** *COBIT 4 - 5.* 2012.

9. **ICONTEC, Intituto Colombiano De Normas Tecnicas y Certificación.** *NORMA TECNICA NTC-ISO-IEC COLOMBIANA 27001.* 2014.

10. **Manaure, Adolfo.** ISACA Presenta un Programa de Evaluación de COBIT para Ayudar a las Empresas a Asegurar sus Procesos. *CIO AMERICA LATINA.* [En línea] 12 de 2011. http://www.cioal.com/2011/12/26/isaca-presenta-un-programa-de-evaluacion-de-cobit-para-ayudar-a-las-empresas-a-asegurar-sus-procesos/.

11. ISACA Presenta un Programa de Evaluación de COBIT para Ayudar a las Empresas a Asegurar sus Procesos. *CIO AMERICA LATINA.* [En línea] 12 de 2011. http://www.cioal.com/2011/12/26/isaca-presenta-un-programa-de-evaluacion-de-cobit-para-ayudar-a-las-empresas-a-asegurar-sus-procesos/.

12. ISOTOOLS. *ISOTOOLS EXCELLENCE COLOMBIA.* [En línea] https://www.isotools.com.co/.