CASO DE ESTUDIO DEL PROCESO DE IMPLEMENTACIÓN DE LAS NORMAS IEC/ISO 9001, IEC/ISO 27001 SOBRE UN MARCO DE REFERENCIA PROPUESTO POR NIST FISMA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL PRODUCTO DE UNA EMPRESA PRESTADORA DE SERVICIOS PAAS

Tenorio, Manuel.
manueltenorio@outlook.com
Universidad Piloto de Colombia

***Resumen*—**Esta es una compañía de software establecida en 1989 cuyo nombre es una abreviación de "negocios" y "agilidad"; la compañía diseña y desarrolla software empresarial para Business Process Management (BPM). Actualmente, la empresa está en proceso de certificación de la norma ISO27001:2013 y FedRamp para cumplir con las regulaciones y requisitos de los clientes de todo el mundo que están preocupados por la seguridad de la información que poseen en sus sistemas de información, para la empresa, estas certificaciones se ha convertido en un tema muy importante, porque quieren garantizar altos niveles de seguridad para la información pero, por parte de los empleados, han informado problemas e inconvenientes porque consideran que la norma ISO27001:2013 no proporciona valor para la empresa, en este artículo, el autor pretende mostrar los beneficios de la implementación de este estándar en (la) empresa**.**

***Abstract*—**This is a software company established in 1989. Its name is an abbreviation of "business" and "agility". The company designs and develops enterprise software for business process management (BPM). Currently, the company is in the process of certifying the ISO27001:2013 and FedRamp standards in order to comply with the regulations and requirements of worldwide customers that are worried about the security of the information they held in their information systems, for the company, this certification has become a very important issue, because they want to ensure high levels of security for the information, but, on the part of the employees, they have reported problems and inconveniences because they consider that the ISO27001:2013 standard does not provide value for the company, in this article, the author intends to show the benefits of the implementation of this standard in this company**.**

***Índice de Términos*—**Amenazas, cloud, FedRamp, información, ISO27001, NIST-FISMA, plataforma, riesgos, seguridad, vulnerabilidades.

I. INTRODUCCIÓN

En respuesta a los rápidos cambios medio ambientales y los diversos desarrollos comerciales que buscan mejorar continuamente los mecanismos de gestión de la información, muchas organizaciones consideran implementar sistemas de gestión relevantes que cumplan los estándares internacionales, para así, alinearse con sus objetivos comerciales, esta es una de las tendencias inevitables de los últimos años.

Un sistema de gestión generalmente debe seguir una gran cantidad de procedimientos y normas. Afortunadamente, muchos procedimientos y normas son iguales o similares. En este documento se pretende mostrar el proceso de integrar y estandarizar funciones iguales o similares, como controles de documentos y registros, toma de acciones correctivas y preventivas, auditorías, revisiones por la alta dirección y ciclos de gestión sobre el ciclo PHVA, esto podría facilitar efectivamente la implementación y el mantenimiento de múltiples sistemas de gestión.

Dado que ambos son estándares de sistemas de gestión basados en el ciclo PHVA, muchas cláusulas del estándar del Sistema de Gestión de la Calidad ISO9001 y del Sistema de Gestión de la Seguridad de la Información ISO27001 son similares. Antes de implementar un SGSI, muchas empresas ya cuentan con sistemas que cumplen con ISO9001, o viceversa. Mientras tanto, durante los cursos de implementación de sistemas que cumplen con ISO9001 o ISO27001, las organizaciones tendrán que documentar su conocimiento implícito y ser sistemáticamente administrados a través de marcos de institucionalización que respaldan los sistemas de

gestión certificados [1]. Sin embargo, a pesar de sus similitudes, existen algunas diferencias entre estos dos sistemas, que requieren ser identificados. El propósito de esta investigación es plantear un modelo de implementación integrado según las normas ISO9001, ISO27001 y FedRamp, con el fin de evitar errores y facilitar la eficacia de la gestión de múltiples sistemas de gestión basados en el ciclo PHVA en las futuras implementaciones de las sucursales a nivel mundial. Al final del documento, se explica el proceso de aplicación del modelo propuesto con un caso de estudio basado en la implementación de dichas normas en una empresa de software privada que funciona a nivel mundial enfocado en la gestión del riesgo en busca del mejoramiento de la seguridad de la plataforma.

II. Cuál es la importancia de la seguridad de la información

Hoy en día el "know-how" de las personas se almacena en activos de información, estos son instrumentos que permiten la operación del negocio, esto lleva, a que estos activos tengan que ser protegidos como lo más importante para la organización. Debido al alza de uso de internet, y la falta de conocimiento en mitigación de riesgos, ocasiona que se presenten incidentes de seguridad, es decir, cuando las amenazas aprovechan las vulnerabilidades y conllevan a la materialización de los riesgos, esto genera un impacto negativo en las organizaciones y como consecuencia se puede perder alguna de las características de la seguridad de la información: disponibilidad, confidencialidad o integridad.

Anualmente las empresas de software antivirus emiten reportes sobre el estado actual de la seguridad, en sus reportes anuales de soluciones de seguridad empresarial, mencionan que los ciber criminales todos los días están perfeccionando sus técnicas para eludir las defensas tradicionales para no ser detectados, por tanto, las empresas deben adaptarse a las situaciones con enfoques de varios niveles para asegurar sus activos de información, dando paso a la frase de Stephen Hawking que cita: *"La inteligencia es la capacidad de adaptarse a los cambios"*, esto quiere decir que, se debería adoptar buenas medidas de seguridad en las organizaciones para poder protegerse eficazmente [2].

Según Jeimmy Cano en su publicación: VII Encuesta Nacional de Seguridad Informática, llevó a cabo un sondeo que permite conocer el estado actual en materia de seguridad de la información a nivel empresarial, como conclusión de este estudio se evidencia que es muy frecuente la falta de apoyo por parte de la dirección y la falta de tiempo, como excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad, adicionalmente, la inversión en seguridad es costosa, pero la organización no reconoce que la materialización de los riesgos puede serlo mucho más [3].

Hoy en día el gobierno colombiano promueve normas como ISO27001, ITIL y Cobit como estándares y buenas prácticas para proteger la seguridad de la información a través de los departamentos de tecnologías de información [3], también, es evidente que es poca la oferta de especialistas en seguridad de la información ya que no hay programas académicos formales suficientes para suplir esa demanda, lo que conlleva a que las empresas opten por contratar profesionales con ninguna o poca experiencia en seguridad y formarlos localmente.

La problemática anterior muestra que los resultados de estudios mencionados señalan que es necesario diseñar y poner en marcha estrategias que permitan mejorar los mecanismos para preservar la información. En Colombia la norma ISO27001 es el estándar más utilizado [4], y poco a poco los requerimientos de seguridad conducirán a que las empresas en Colombia deban crear o mejorar sus SGSI (Sistemas de Seguridad de la Información), no solo por cumplir con lo establecido en la norma ISO27001 sino, para poder asegurar de manera correcta y confiable la información de la organización y sus usuarios.

III. Motivación

Nunca ha sido fácil la tarea de proteger la información y convencer a la alta gerencia sobre la importancia de la implementación de lineamientos para la seguridad de la información, ya que normalmente se delega esta tarea a las maquinas controladas por el departamento de TI, tales como firewalls, sistemas de detección y prevención de intrusos, entre otras, que la sociedad dice que al tenerlas, la organización se vuelve impenetrable, lo cual no es cierto, ya que el área de TI no puede controlar el factor humano, por tanto se ven forzados a exponer a la alta gerencia las fallas en seguridad y plantear en términos económicos, el costo de la implementación de una serie de mecanismos que permiten controlar de manera sistemática la gestión la seguridad de la información en toda la organización.

Pero a veces exponer un punto de vista en busca del mejoramiento de la seguridad de la información para la organización suele ser difícil, por tanto, si se quiere presentar los numeroso beneficios que tiene la implementación de la norma ISO27001, se pueden gastar horas y horas en reuniones, sin embargo, para el propósito de este documento, se hace un resumen de los aspectos, que según Agustín López Neira, especialista líder en ISO27001 son los más importantes para la generación de valor para el negocio [5].

1) Cumplimiento

Las organizaciones deben cumplir con los mandamientos que exige la ley (en Colombia, por ejemplo la ley 1581 de 2012, para la Protección de Datos Personales), por tanto, para cualquier organización que busque la protección de los datos, este aspecto es el que demuestra de manera más rápida un retorno de la inversión, esto se logra, con la implementación de un Sistema de Gestión de Seguridad de la Información, una metodología que este orientada a conseguir que la información esté asegurada desde su creación, transmisión y disposición final.

2) Ventaja de comercialización

Hace unos años, normalmente en las organizaciones se realizaban los procesos sin control alguno, esto ocasionaba que los productos no siempre cumplieran con requisitos internacionales de calidad, al darse a conocer la norma ISO9001, las empresas querían ser diferenciadoras de su competencia, entregando productos con un sello de calidad, esta es una situación se repite en la actualidad al implementar la norma ISO27001, se brinda un valor agregado al demostrar que la empresa está protegiendo su recurso más valioso: la información, ya que en los activos de información es donde se almacena el "know-how" del negocio.

3) Disminución de gastos

Cuánto podría costar a nivel financiero, o cómo se vería afectada la reputación de una compañía por una multa de filtración de información sensible, para algunas empresas puede llegar a ser como quitarle un "pelo a un gato", pero para otras, puede costarle la continuidad del negocio, por tanto, la implementación de estándares de seguridad en la compañía puede hacer que disminuyan los gastos ocasionados por incidentes de esta clase.

4) Organización del negocio

¿Determinar quién toma las decisiones? ¿Quién es responsable por los activos de información? ¿Quién autoriza los accesos a los sistemas de información? En una gran empresa puede llegar ser un trabajo tedioso, la norma ISO27001 es de gran utilidad para resolver estas cuestiones, ya que obliga a definir de manera clara y precisa las responsabilidades y obligaciones, así se logra tener una empresa más organizada estructuralmente.

Para terminar, aparte de ser una certificación más para tener colgada en la pared, la norma ISO27001, brinda una serie de controles que ayudan a las organizaciones a controlar aspectos de seguridad física y lógica con el fin de garantizar un nivel mayor de seguridad de la información.

5) Migración a la plataforma en la nube y sus problemas de seguridad adquiridos

El modelo de computación en la nube representa un nuevo cambio de paradigma en los servicios basados en internet que ofrece plataformas informáticas distribuidas altamente escalables en las que los recursos computacionales se ofrecen como un servicio. Aunque, el modelo de la nube está diseñado para obtener beneficios incontables para quiénes están interesados, tales como: los proveedores de servicios en la nube, los consumidores y los proveedores de servicios, el modelo todavía tiene varios problemas abiertos que afectan su credibilidad.

La seguridad se considera uno de los temas principales al adoptar el modelo de computación en la nube, según lo informado por IDC [6], una justificación razonable de tales preocupaciones crecientes de los modelos de seguridad que se incluyen en la nube son: la pérdida de control sobre los activos alojados en la nube, la falta de garantías de seguridad en los acuerdos de nivel de servicio entre los prestadores del servicio y los clientes y compartir recursos con competidores o usuarios maliciosos, en consecuencia, no importa cuán fuertemente se asegure el modelo, los consumidores continúan sufriendo por la pérdida de control y la falta de problemas de confianza, por otro lado, los prestadores del servicio luchan con los problemas de seguridad de la plataforma en la nube porque el modelo de la nube es muy complejo y tiene muchas dimensiones que deben considerarse al desarrollar un modelo de seguridad integral incluida en la compleja arquitectura de los modelos en la nube [6]. Estas dimensiones dan como resultado una gran cantidad de controles de seguridad heterogéneos que deben administrarse de forma coherente. Además, los consumidores que alojan servicios no siempre conocen los contenidos o los requisitos de seguridad que se aplicarán en estos servicios. Esto lleva a una pérdida de control de seguridad sobre estos servicios y las plataformas en la nube.

Para concluir con los motivos de la realización de este documento y para demostrar el uso del modelo planteado, se demuestra la utilización del prototipo del marco de gestión de seguridad en la nube basado en la colaboración para la plataforma en la nube que aloja una aplicación de BPM, finalmente, se evalúa este enfoque asegurando el servicio, suponiendo que la plataforma en la nube tiene varios usuarios que comparten la misma aplicación en la nube.

En el transcurso del documento se propone un escenario que permite resaltar el problema de investigación que se intenta abordar, en el cual se muestra una descripción general de los problemas de seguridad de la computación en la nube. De igual manera, se analiza paso a paso como se desarrolla el marco de referencia y se da un ejemplo de uso del marco desarrollado. Para terminar, se discuten las implicaciones del trabajo realizado al interior de la organización y los planes futuros para mejorar la seguridad en la aplicación.

IV. PLANTEAMIENTO DEL MARCO DE REFERENCIA PARA EL SISTEMA DE GESTIÓN DOCUMENTAL

A. Fase 1: Planteamiento del marco de referencia integrado

Según diversas reuniones con la alta dirección, en primera instancia, se toma la determinación de construir un marco común, que integra documentos de todos los niveles, originalmente pertenecientes a diferentes áreas de la organización, en una base de documentos compartidos que serán la base para combinar documentos con atributos iguales o similares. Si los documentos no son exactamente iguales se deben marcar las diferencias y luego, plantear todos los sistemas de gestión, incluidos los futuros, que puedan hacer referencia a esta base de documentos comunes.

Aquí, se deben unificar todos los documentos relacionados con el sistema de gestión, que abordan procedimientos de control, manuales, guías de trabajo, formatos, escritos comunes, procedimientos de control de registros, procedimientos de auditoría interna, medidas correctivas, y otras medidas preventivas.

Para esta fase se sugiere la formación un comité de revisión de gestión lo antes posible y se tenga todo el apoyo posible para que revisen y confirmen que los documentos de soporte integrados cumplen con los requisitos de ISO9001, ISO27001 y otras normas o leyes aplicables, este comité es de gran utilidad posterior a la implementación para que, luego de un corto período de prueba del sistema de gestión, los registros creados permitan verificar el cumplimiento de los estándares, ISO9001, ISO27001, y NIST-FISMA (para buscar el cumplimiento de FedRamp). Si algo sale mal, pueden ser necesarios ajustes en el sistema o los métodos planteados para el aseguramiento de la información.

B. Fase II: Integración de las políticas de los sistemas de gestión y reorganización de los grupos de trabajo

En esta fase, la más importante de la implementación, las viabilidades de las políticas de los sistemas de gestión y los grupos de trabajo correspondientes también son evaluadas por los líderes de las áreas de Productividad y Seguridad de la Información quiénes se reúnen para crear las políticas integradas del sistema de gestión. Estas políticas son las directivas para conducir a una correcta gestión de los sistemas y las disciplinas de las operaciones de gestión dentro de la organización, por lo tanto, deben integrarse como un conjunto

único sin conflictos. Esto genera una reorganización empresarial con el objetivo estratégico de asegurar la calidad al mantener los sistemas de gestión y brindar seguridad a la información, del mismo modo, optimizar y enfocar los recursos organizacionales en el proceso de implementación de los sistemas.

C. Fase III: Integrar actividades comunes para facilitar el mantenimiento del sistema

En esta última fase, las actividades para mantener un marco común deberían ser programadas de tal manera que la organización no afecte su disponibilidad laboral, es decir, se sugiere incluir estas actividades en el calendario anual de la organización sin afectar la operación diaria (actividades como: auditorías internas, reuniones de revisión de gestión y capacitaciones), luego de haberlas discutido con la alta gerencia y las unidades de negocio involucradas.

En la siguiente sección, luego de haber terminado la fase de integración de las normas ISO9001 e ISO27001, la presente investigación se centra en la gestión de riesgos de la plataforma en la nube de la compañía.

V. TRABAJO PREVIO AL INTERIOR DE LA EMPRESA

A. Planteamiento de líneas bases de seguridad para el producto en la nube

El equipo de desarrollo propuso un enfoque por modelos para especificar los requisitos de seguridad para la plataforma sobre la nube de Azure. Cada instancia de la plataforma (compuesta por servicios y componentes) está soportada por una máquina virtual, estos supusieron que la seguridad de múltiples usuarios se mantiene mediante el uso de máquinas virtuales para cada cliente (el caso más simple, ya que cada cliente tiene una suscripción por separado), pero no consideran la seguridad externa de la infraestructura.

Posterior a la creación del equipo de seguridad, se propuso una idea con un mayor nivel de abstracción (basado en el riesgo, en lugar de los requisitos de seguridad mínimos). La Oficial de Seguridad de la Información, propuso un análisis de riesgo cuantitativo y un método de evaluación basado en la norma NIST-FIPS-199 [7].

Los esfuerzos de investigación relacionados con los riesgos de la plataforma incluye la aplicación de marcos de evaluación y gestión de riesgos como MagerIT [8] y Octave [9], adicionalmente, haciendo uso del recién creado, Sistema de Gestión de Seguridad de la Información basado en las políticas definidas y finalmente la gestión de la seguridad, basada en modelos previamente propuestos por proveedores de confianza [10] que se ajustan a lo propuesto anteriormente por el equipo de desarrollo. Este enfoque busca alcanzar la seguridad por medio de fases de retroalimentación y mejora. Estas fases se vuelven más críticas en el modelo de la nube, porque pasamos de la seguridad dentro de los límites de la empresa, a la seguridad de los recursos subcontratados en la nube.

B. Alineando el estándar NIST-FISMA con el modelo de arquitectura de la nube

El estándar de controles para la seguridad y privacidad en los Sistemas de Información Federales [11], define un marco para gestionar la seguridad de los sistemas de información que respaldan las operaciones de las agencias federales de los Estados Unidos. El marco tiene seis fases principales que incluyen: categorización de seguridad actual del servicio/plataforma, selección de controles de seguridad, implementación de controles de seguridad, evaluación de controles de seguridad, autorización para la implementación y monitoreo de seguridad.

1) Categorización de seguridad del servicio

Cada instancia de la plataforma en la nube es utilizada por un único cliente, este posee una adecuación de los servicios e información y al tener la potestad de decidir o cambiar la configuración de la plataforma, puede alterar el impacto de una posible pérdida de confidencialidad, integridad y disponibilidad de su información comercial. Cada cliente puede asignar diferentes niveles de impacto (bajo, medio o alto) a las violaciones de seguridad de su información que se presenten sobre su subscripción.

Según FedRamp [12], el proveedor de la plataforma debe especificar la categorización de seguridad de los servicios entregados en su plataforma, sin embargo, esto no es suficiente ya que no se tiene suficiente conocimiento sobre el impacto de las violaciones a la seguridad de la información en los objetivos comerciales de sus clientes. Desde este punto, el enfoque de trabajo permite que los clientes participen en la especificación de la categorización de seguridad de su información.

2) Selección de controles de seguridad

La selección de los controles de seguridad a implementar para proteger la infraestructura de los clientes tiene dos pasos: primero, la selección de controles de seguridad según la línea base propuesta por el equipo de producto acorde con lo propuesto por el estándar FISMA, el cual, proporciona un catálogo de plantillas de controles de seguridad categorizadas en tres líneas base (bajo, medio y alto). Con base en la categorización de seguridad previamente calculada para el cliente (según la formula, donde el cálculo del *riesgo* es igual a la multiplicación de la *probabilidad y el impacto*), seleccionamos la línea base inicial de los controles que se espera proporcionen el nivel de seguridad requerido por los clientes, segundo, se adapta la línea base de los controles de seguridad.

3) Proceso de evaluación del riesgo de la plataforma:

Según los controles de seguridad identificados para cubrir las vulnerabilidades, amenazas, riesgos y otros factores de la plataforma de la siguiente manera: este proceso se lleva a cabo en 3 etapas:

a) Identificación de vulnerabilidades*:*

Este paso requiere conocer la plataforma y la arquitectura en el entorno operativo. Se considera la participación del proveedor del producto que conoce la estructura interna del servicio proporcionado y el proveedor de servicios en la nube, quiénes conocen la arquitectura de la plataforma en la nube, que para este caso, sería la empresa en cuestión y Microsoft, quién provee guías estándares de seguridad para sus productos [10].

b) Identificación de amenazas*:*

Las posibles fuentes de amenazas y las capacidades de un servicio determinado pueden identificarse mediante la colaboración entre los proveedores del producto, los proveedores del servicio en la nube [13] y los clientes. Los

clientes están involucrados ya que tienen el conocimiento sobre el valor de sus activos y quién puede ser una fuente de violaciones de seguridad.

c) Determinar nivel de riesgo*:*

En función de las capacidades de las fuentes de amenazas, la naturaleza de las vulnerabilidades existentes y basado en los resultados del impacto y la probabilidad de ocurrencia, el riesgo se clasifica como bajo, medio o alto.

4) El proceso de adaptación de la línea base de controles de seguridad

Con base en el proceso de evaluación de riesgos, la línea base de los controles de seguridad seleccionados se pueden adaptar para mitigar nuevos riesgos y ajustarse de la siguiente manera:

a) Definición del alcance de los controles de seguridad*:*

En primera instancia se debe identificar los controles de seguridad comunes; el equipo de desarrollo decide qué controles de seguridad para la línea base planean implementar con un control de seguridad común (ya sea proporcionado por el proveedor de servicios en la nube o por los clientes), posteriormente se identifican los componentes críticos del sistema; aquí, el equipo de desarrollo define qué componentes son los más aptos para aplicar las configuraciones de seguridad y cuáles no (puede ser porque ya se encuentran en una zona confiable o poseen otros controles de seguridad), y por último, deben identificar controles de seguridad relacionados con la tecnología y el ambiente que los rodea, por ejemplo, el acceso de los administradores a través de una red externa a la organización

b) Compensación de los controles de seguridad*:*

Cuando los clientes encuentren que uno o más de los controles de seguridad en la línea base adaptada no se ajustan a sus condiciones de negocio o no están disponibles para implementar, pueden decidir reemplazar dichos controles con un control compensatorio.

c) Establecer parámetros de controles de seguridad*:*

El último paso en este proceso de adaptación de la línea base, es la configuración de parámetros de los controles de seguridad, por ejemplo: el tipo de autenticación a ser usado, el número máximo de intentos de inicio de sesión fallidos, la configuración de una red privada virtual, etc. Esto se hace mediante la colaboración entre el proveedor de la plataforma y el cliente. El resultado de esta fase es un plan de gestión de la seguridad que documenta la clasificación de la seguridad del servicio, los riesgos, las vulnerabilidades y la línea base de los controles de seguridad personalizados.

5) Implementación de controles de seguridad:

El plan de seguridad para cada cliente describe los controles de seguridad que implementará cada parte interesada en función de la categoría de control de seguridad (controles comunes o específico del servicio). La implementación común de los controles de seguridad es responsabilidad del proveedor del control común que pueden ser los proveedores del servicio en la nube/plataforma (en el caso de controles de seguridad internos de la infraestructura o el producto) o el cliente (en el caso de controles externos). La implementación de los controles de seguridad específicos del servicio es responsabilidad del proveedor del servicio. Cada parte interesada debe documentar las configuraciones de implementación de los controles de seguridad en el plan de gestión de seguridad.

6) Evaluación de los controles de seguridad:

Se requiere una evaluación de los controles de seguridad para garantizar que los controles de seguridad implementados funcionen correctamente y cumplan con los objetivos de seguridad especificados. Este paso incluye el desarrollo de un plan de evaluación de seguridad que defina cuáles son los controles que se evaluarán, cuáles son los métodos de evaluación que se utilizarán y cuáles son las medidas de seguridad para cada control de seguridad. Los resultados del proceso de evaluación están documentados en un informe de evaluación de seguridad. Este paso puede dar como resultado volver a los pasos anteriores en caso de identificar deficiencia en los controles implementados o continuar con los siguientes pasos.

7) Autorización de servicio:

Este paso representa la aceptación formal por parte de los clientes sobre los riesgos identificados involucrados en la adopción del servicio y las mitigaciones acordadas. El plan de seguridad y el plan de evaluación de seguridad serán los acuerdos de nivel de servicio con respecto a la seguridad de la plataforma.

8) Monitoreo de la efectividad de los controles de seguridad:

Los proveedores de la plataforma deben proporcionar herramientas de monitoreo de seguridad para ayudar a los clientes a monitorear el estado de seguridad de sus activos. Las herramientas de monitoreo deben tener la capacidad de capturar las métricas de seguridad planteadas e informar las medidas recopiladas en un informe de estado de seguridad ya sea basado en eventos o en una base periódica. Los resultados del proceso de monitoreo pueden requerir volver a plantear nuevos objetivos o controles plan de gestión de la seguridad para manejar nuevos cambios imprevistos.

C. Automatización de la seguridad [12]

Después de alinear el estándar FISMA con el modelo de nube propuesto, se establece un marco de referencia de vulnerabilidades estándar que sirven para ayudar a mejorar la automatización y su integración con las capacidades de seguridad existentes que fueron planteadas como línea base para los futuros clientes, en la figura 1, se muestra un diagrama de clases que muestra cómo se hace relación entre las diversas bases de datos de información sobre seguridad de la información para los productos y sus vulnerabilidades y así poder tener extraer un mejor análisis de riesgo.

1) Common platform enumeration (CPE) [14]

El CPE proporciona un esquema de nombres estructurado para los sistemas de TI, incluidos el hardware, los sistemas operativos y las aplicaciones. Usamos el CPE, como la convención de nombramiento de los activos de la plataforma en la nube, sus componentes y servicios. Esto ayuda a compartir el mismo nombre de servicio con otras plataformas en la nube y con las bases de datos de vulnerabilidades existentes.

2) Common weakness enumeration (CWE) y Common attack pattern enumeration and classification (Capec) [15] [16]

El CWE proporciona un catálogo del software reconocido por la comunidad y sus debilidades. El Capec proporciona un

catálogo de los patrones de ataque comunes. Cada patrón de ataque proporciona una descripción del escenario de ataque, la probabilidad, el conocimiento requerido y las posibles mitigaciones. Utilizamos CWE y Capec como referencia para el equipo de seguridad en la nube durante la fase de identificación de vulnerabilidades.

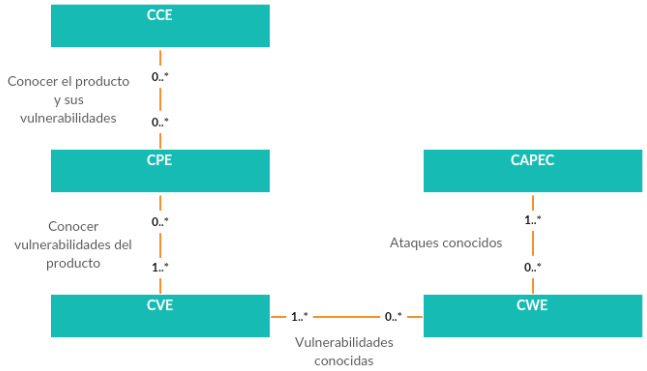

Fig. 1. Diagrama de clases del marco de referencia de vulnerabilidades estándar. [27] Traducido

3) Common vulnerability and exposure (CVE) [17]

El CVE proporciona un diccionario de las vulnerabilidades comunes, con una referencia al conjunto de los productos vulnerables (codificados en el CPE). También ofrece una calificación de las vulnerabilidades que refleja la gravedad de la vulnerabilidad. Usamos el CVE para recuperar las vulnerabilidades conocidas descubiertas la plataforma.

4) Common configuration enumeration (CCE) [18]

El CCE proporciona un nombre estructurado y único a las declaraciones de configuración de los sistemas para que estos puedan comunicarse y comprender tales configuraciones. Usamos el CCE en la fase de implementación de controles de seguridad. En lugar de configurar controles de seguridad manualmente, los administradores del equipo de seguridad pueden asignar valores a los parámetros de las plantillas de controles de seguridad.

El marco utilizado, hace uso de estas configuraciones para administrar los controles de seguridad seleccionados de manera que, se pueda identificar de mejor manera los vectores de ataque y como operan, también como poder remediar de manera rápida las vulnerabilidades encontradas mensualmente según el plan de detección y remediación.

VI. GESTIÓN DE LA SEGURIDAD PARA EL PRODUCTO EN LA NUBE

El marco para la gestión de la seguridad para el producto consta de tres capas principales: una capa de gestión, una capa de aplicación y una capa de retroalimentación. Estas capas que se muestran en la figura 2, representan la realización de las fases del SGSI descritas anteriormente, las cuales funcionan de la siguiente manera:

A. Capa de gestión

Esta capa es responsable de capturar las especificaciones de seguridad de los involucrados (proveedor de servicios en la nube, proveedor del servicio y cliente) y consiste en:

Categorizar el nivel de seguridad requerido por los clientes de la plataforma según la especificación de seguridad de su información mantenida en la nube.

La evaluación de riesgos donde todas las partes interesadas de la plataforma en la nube participan en el proceso de evaluación de riesgos con el conocimiento que poseen.

Los controles de seguridad a ser implementados por el administrador y que deben ser registrados en las plantillas de los controles de seguridad, también, la estructura y ubicación de los archivos de registro.

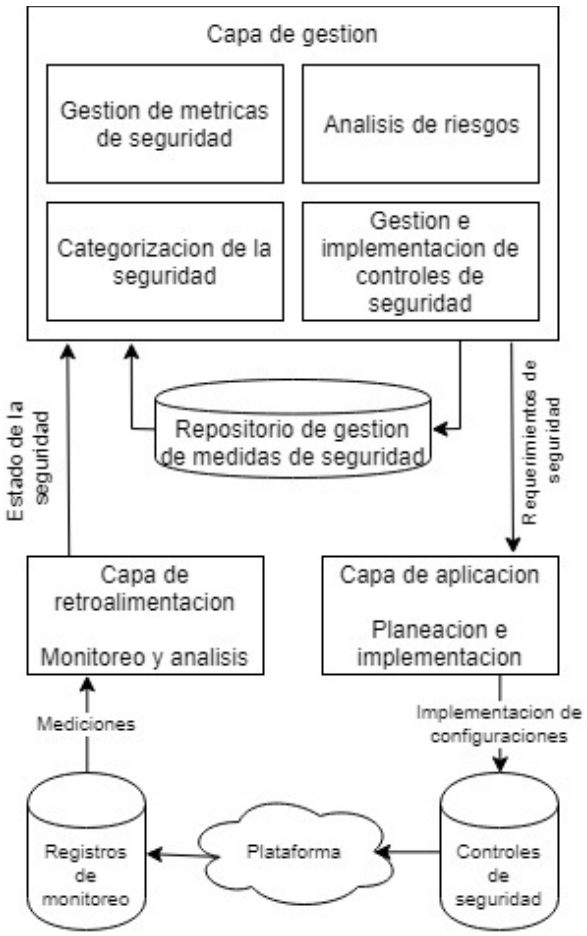

Fig. 2. Diagrama de funcionamiento del proceso de gestión para la seguridad de las plataformas en la nube. [27] Traducido

La recopilación de información para alimentar las métricas de seguridad utilizado por los interesados para medir la efectividad de esta.

Establecer los mecanismos de control por parte de los clientes para verificar el estado de seguridad de la plataforma, según los valores actuales de las métricas de seguridad y sus tendencias.

B. Capa de aplicación.

Esta capa es responsable de la planificación e implementación de la selección de controles de seguridad en función de los riesgos identificados. Estos controles seleccionados están documentados en el plan de gestión de seguridad. Este plan es importante ya que mantiene la línea base de los parámetros de configuración de los controles de

seguridad y la asignación de dichos parámetros sobre los componentes de la infraestructura.

C. Capa de retroalimentación y análisis

El monitoreo de registros es responsable de recopilar los resultados de las medidas establecidas en la herramienta de control de registros de la plataforma que permite determinar el nivel de efectividad de las medidas de seguridad y almacenarlas en el repositorio de registros de seguridad para ser utilizado en el análisis de las medidas recopiladas para asegurarse de que el sistema esté funcionando dentro de los límites definidos para cada métrica. Si hay una desviación de los límites predefinidos, el servicio de análisis dará alertas para actualizar las configuraciones actuales.

VII. Caso de estudio

A. Motivos de la implementación del SGSI.

No se puede negar que la información es invaluable en una organización, por tanto, se toma como referente la definición: "*La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente*" [19], según lo anterior, es necesario que las empresas que deseen certificarse, tomen las medidas necesarias para buscar la protección de la información al igual que los sistemas en los cuales se encuentra almacenada esta.

Es así, como se crea un vínculo entre la información y los sistemas de cómputo, primero, es el activo fundamental de los procesos, segundo son los que procesan y almacenan la información en los diversos equipos de la organización (discos, memorias, respaldos, etc.), por esto es importante que se implementen sistemas que permitan resguardar la información, a través de controles efectivos que no permitan a los delincuentes entrar a los sistemas con mala intención y que puedan afectar la continuidad del negocio.

Analizando lo dicho, se evidencia lo esencial que es implementar un SGSI, para gestionar los riesgos y minimizar la materialización de estos, según la norma ISO27001 se define el término "Gestión de riesgos" como: "*las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo*" [20].

Con relación al ambiente corporativo, es evidente que no es suficiente con identificar las vulnerabilidades del sistema informático, también hay que contemplar quién se puede ver afectado por daños o robos de la información de la empresa, pueden ser desde amenazas externas como competidores o aficionados a acceder a la información, hasta trabajadores internos que simplemente sin darse cuenta, genera un incidente de seguridad.

Los incidentes de seguridad presentados anteriormente llevan a la empresa a realizar un análisis de las amenazas y de negocio, que lleva a la conclusión, que el riesgo más latente son los posibles ataques informáticos para la infraestructura de desarrollo, donde se presentó recientemente un ataque de denegación de servicios como fachada para el robo del 78% del servidor de código fuente, que alberga el código del servicio en la nube; este es un producto nuevo en el mercado y se presenta como novedoso para usuarios actuales que desean continuar con él como su herramienta de BPM, que gracias a su bajo costo y facilidad de implementación y gestión se ha vuelto muy atractivo para nuevos clientes, especialmente del sector financiero y gubernamental según el cuadrante de Gartner [21], pero que, al momento de realizar los estudios de seguridad de proveedores, determinan que el producto en la nube no es apto para ser elegido, ya que no cuentan con políticas que garanticen la seguridad de la información en sus productos, generando perdida de contratos importantes para el posicionamiento de la organización, razón por la cual se hace necesaria la implementación de manera rápida de un SGSI en la organización pero, las personas encargadas de seguridad del producto no cuentan con suficiente conocimiento para su implementación, lo que impide evitar la materialización de los riesgos dando lugar a otro ataque donde se filtra información valiosa en un ambiente de un cliente.

B. Propuesta de análisis del negocio

Para el presente documento se analizó el grupo de empleados dentro del alcance de la certificación, enfocado especialmente en los gerentes de las áreas involucradas (10 empleados), y la Oficial de Seguridad de la Información; quiénes son los responsables de la implementación del Sistema de Gestión de Seguridad de la Información.

Se ha considerado conveniente para la investigación, hacer una reunión previa con la Oficial de Seguridad de la Información, para informar la realización del presente documento de investigación con el fin de obtener un consentimiento informado, sin embargo, por parte de Ésta, se informa que como medida de confidencialidad, el documento será revisado previa entrega a la Universidad Piloto de Colombia para prevenir que los datos aquí contenidos, permitan identificar a la organización y asegurar que los datos de los empleados participantes de las entrevistas sean mantenidos en estricta reserva, guardando total confidencialidad de la información obtenida en las mismas.

El principal instrumento utilizado para realizar el proceso de levantamiento de información ha sido la revisión de documentos generados en el proceso de implementación y entrevistas a la Oficial de Seguridad de la Información. En este tipo de investigaciones, la herramienta primordial en la recolección de los datos es el investigador, ya que ha estado presente en cada una de las etapas de implementación de este proyecto, y que, a través de diversos métodos o técnicas, es Éste quién recoge los datos y los analiza.

C. Estado actual de la Implementación del SGSI

Esta es una empresa pragmática, que busca resultados rápidos para sus actividades, por el momento no cuentan con ninguna certificación para sus procesos, en materia de seguridad, consideran que esta es una tarea del departamento de TI, quiénes deben asegurar que los sistemas estén blindados contra ataques informáticos, pero su labor se ve dificultada por decisiones de la alta dirección como: tener permisos de administrador en las maquinas, el personal de desarrollo pueda inactivar el software antivirus al momento de compilación, accesos remotos para la prestación del servicio a través de sistemas que no cumplen con altos estándares de seguridad, entre otros, por tanto, en el área de TI se hace un sobre esfuerzo con el objetivo de brindar seguridad; la empresa solamente cuenta con controles básicos como software antivirus, firewalls, redes virtuales, y cintas de

respaldo como medidas para proteger la información de la organización.

Según expertos, estiman que el tiempo de implementación de un Sistema de Gestión de Seguridad de la Información, basado en los requisitos que brinda la norma ISO27001:2013, determinan que, para una empresa de más de 500 trabajadores se puede necesitar un tiempo de entre 12 a 15 meses para su implementación [22], por temas contractuales e indicaciones de la alta gerencia se determinó un plazo de 10 meses para conseguir certificar la norma para su proceso de soporte, este corto tiempo de implementación repercute en la brevedad con que se debe dar la ejecución, ocasionando que la gente se sienta presionada para entregar los resultados esperados, pero a su vez sin tener que descuidar sus labores regulares.

Los problemas se comienzan a evidenciar cuando es necesario que los líderes de las áreas involucradas estén presentes para construir el inventario de activos y realizar los análisis de riesgos y vulnerabilidades, en las reuniones citadas, estos no se encuentran presentes en la mayoría de las ocasiones debido a la carga laboral que tienen; adicionalmente el poco conocimiento en materia de seguridad, ocasiona que los resultados de los análisis no reflejen con objetividad el estado actual de la compañía, ya que, según los resultados, el 76% de los activos de información presentan un gran nivel de exposición al riesgo, lo que ocasiona que se deban definir planes de tratamiento bastante agresivos para la organización.

Sumado a lo anterior, al definir la lista de controles que se deberían aplicar estos incurren en gastos excesivos y cambios de mentalidad organizacional por la necesidad de adoptar nuevos procedimientos e incurrir en inversión de tiempo y recurso humano para conseguir un nivel apropiado de gestión documental.

Debido al corto tiempo de implementación se decide realizar la contratación de una empresa de consultoría externa para brindar apoyo en la implementación del SGSI y el recurso humano destinado para esta labor consideran que un SGSI es una implantación que debe ser realizada por unos pocos.

Para el Gerente de Operaciones, hablar de temas como: seguridad de la información y costos, es harina del mismo costal, pero desde el punto de vista de la Líder del SGSI, la aceptación del sistema debe vencer el miedo de la dirección a tener desequilibrios en su presupuesto, con el fin de lograr la seguridad de la información de la organización y conseguir la tan anhelada certificación.

Por último, el ámbito legal está influyendo en reconsiderar un cambio de estrategia para la implementación del SGSI debido a los incidentes de seguridad graves que se han presentado al interior de la empresa y en otras organizaciones del sector, esto fue utilizado como un mecanismo para inducir al cambio de mentalidad con respecto a la seguridad por parte de los empleados de la organización.

D. Aplicación del modelo colaborativo

Para demostrar las capacidades del marco de seguridad de computación en la nube propuesto al interior de la organización, el primer paso en nuestro enfoque es registrar en el repositorio de activos, los componentes de la infraestructura en la nube para que pueda ser consultado por los clientes y administradores de de la plataforma en la nube. Este paso se desarrolla usando la herramienta Eramba. En este paso, usamos el nombre de CPE como identificación del activo de información, como se aprecia en la figura 4.

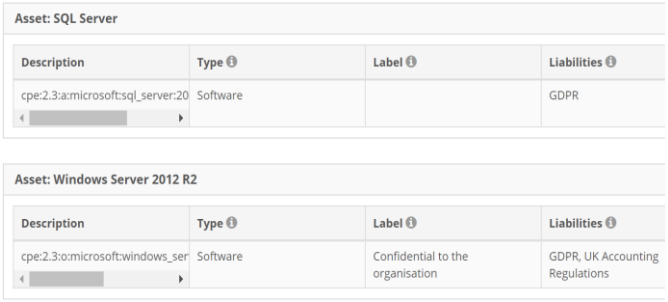

Fig. 4. Muestra del listado de activos y su información según lo propuesto por el marco colaborativo diseñado. [28]

Una vez todos los clientes tienen los activos de información registrados, pueden usar nuestra herramienta para mantener centralizados sus activos de la siguiente manera:

1) **Categorización de la seguridad del servicio**:
El Líder Técnico de desarrollo en la nube, en conjunto con el cliente, especifican el nivel de impacto de perder la confidencialidad, la integridad y la disponibilidad de los datos mantenidos por la plataforma. Cada vez que un nuevo cliente registra sus activos en Eramba y define su categorización de seguridad de los datos procesados por el servicio, Eramba actualizará la categorización general de la seguridad del servicio.

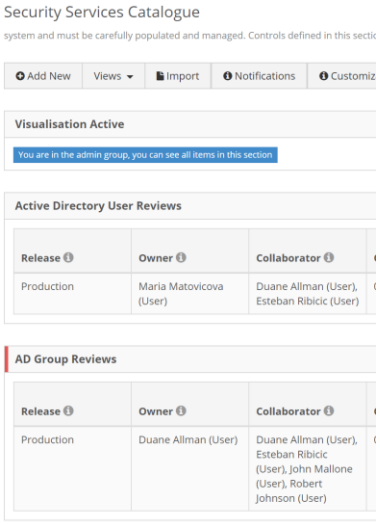

Fig. 5. Listado del catálogo de controles de seguridad. [28]

2) **Selección de controles de seguridad**:
Los clientes pueden registrar sus propios controles de seguridad utilizando el servicio de controles de seguridad, Eramba genera una línea de base de las plantillas de controles de seguridad que han sido previamente definidos y ajustados acorde a la información de otros clientes. Esta línea de base identifica las plantillas de los controles de seguridad que están: satisfechas (coinciden con uno de los controles de seguridad registrados), faltantes (no coinciden con los controles de seguridad registrados) y duplicados (más de un control compatible), como se muestra en la

figura 5.

Durante el proceso de evaluación del riesgo de la plataforma, las vulnerabilidades son identificadas por primera vez en Eramba con la ayuda del equipo de producto, quiénes conocen la arquitectura de la plataforma en la nube, de igual manera, tienen la responsabilidad de mantener la lista de vulnerabilidades del servicio actualizada para determinar de manera rápida las brechas de seguridad que puedan afectar a los clientes. El marco de trabajo permite sincronizar las vulnerabilidades de la plataforma o servicio contra la base de datos de vulnerabilidades de la comunidad o NVD. De igual manera, se sugiere que cada cliente realice escaneos de vulnerabilidades para anexar cualquier amenaza que falte. El marco se integra con las bases de datos CWE y Capec para ayudar a los interesados a identificar posibles vulnerabilidades cuando el servicio no tiene vulnerabilidades registradas en el NVD.

3) **El proceso de adaptación y ajuste de los controles de seguridad:**
El proceso de ajuste y adaptación de los controles de seguridad es realizado por los clientes, quiénes deciden qué controles de seguridad de la línea base generada por Eramba planean implementar o reemplazar acorde a la situación actual de sus controles de seguridad. Aquí los clientes definen las configuraciones de los parámetros de los controles de seguridad. El resultado final de este paso es un plan de administración de seguridad que documenta la categorización de la seguridad del servicio, las vulnerabilidades, las amenazas, los riesgos y los controles de seguridad personalizados por cada cliente que permiten mitigar las posibles violaciones de seguridad identificadas, como se muestra en la figura 6.

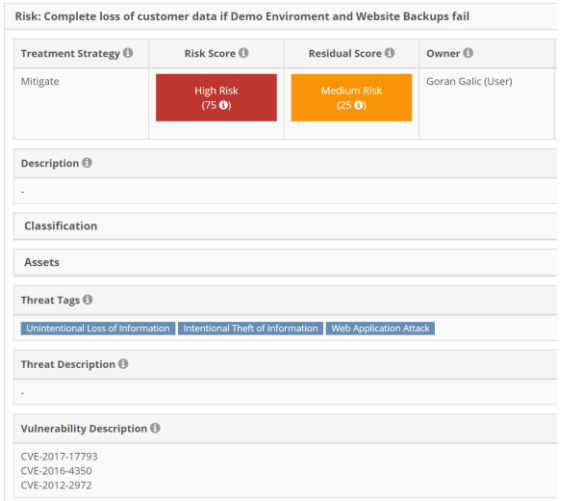

Fig. 6. Análisis de riesgo generado por la aplicación [28]

4) **Implementación de controles de seguridad**:
Cada parte interesada, implementa los controles de seguridad bajo su responsabilidad como se establece en el plan de seguridad y las configuraciones de controles de seguridad son especificadas en el paso anterior.

5) **Evaluación de los controles de seguridad implementados:**
Los clientes definen los controles que se evaluarán y los objetivos de la evaluación y se documentan en el plan de evaluación de seguridad cliente. La ejecución de dicho plan, el proceso de evaluación se sugiere que sea realizado por un tercero. El resultado de la fase de evaluación es un informe de evaluación de seguridad.

6) **Autorización de servicio**:
Finalmente, los clientes dan su aceptación formal del plan de seguridad, plan de evaluación y los informes de la evaluación. Esta aceptación representa la decisión de permitir monitorear la efectividad de los controles de seguridad para recopilar las métricas de seguridad definidas según el plan de evaluación y generar un informe sobre el estado de seguridad para los clientes. De igual manera, este informe sirve como retro alimentación para poder incrementar los niveles de seguridad para los futuros desarrollos de la plataforma, como se aprecia en la figura 7.

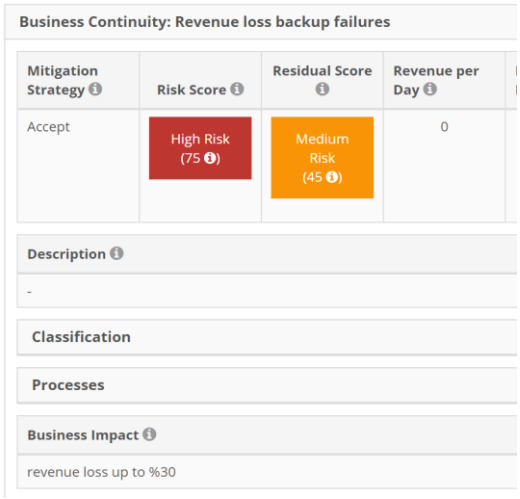

Fig. 7. Categorización del estado de seguridad de la plataforma. [28]

E. Factores que actualmente impiden la implementación del SGSI

A continuación, se muestra un resumen los grandes aspectos que están siendo recopilados en la base de datos de conocimiento del Equipo de Seguridad, y el análisis de los comentarios depositados en el buzón de sugerencias; que actualmente están generando problemas para los analistas de seguridad de la organización en su camino para la certificación del SGSI.

1) Mala gestión en involucrar el personal de la organización a la implementación del SGSI

Cabe hacer énfasis que esta compañía no está organizada para trabajar por procesos, pero la ISO27001 establece que, como punto de arranque, es necesario que la empresa realice sus actividades, enfocada en la ejecución de procesos. Lo que surge como recomendación, es la aplicación del estándar ISO9001 para asegurar la ejecución y calidad de los procesos durante todo el ciclo PHVA para la implementación de la norma los resultados de la entrevista se pueden visualizar en la tabla 1: comentarios sobre la gestión del SGSI.

TABLA I
COMENTARIOS SOBRE LA GESTIÓN DEL SGSI

Positivos	Negativos
Conceptos del SGSI se afinan periódicamente	Desconocimiento y temor por parte de los empleados, con respecto a los cambios que pueda acarrear la implementación, debido al despido de personal al realizar la auditoría interna
La implementación del SGSI está haciendo tomar conciencia de los riesgos de seguridad presentes en la organización	Falta de organización estructural de la organización, se está manejando por funciones y no enfocado en procesos Se relaciona la implementación del SGSI con el área de IT, por tanto, las solicitudes se están perdiendo en la casilla de correo de "soluciones informáticas" No hay conocimiento de gestión por procesos por parte de los empleados de la organización Falta de conocimiento e implementación en normas como la ISO9001, que ocasión retrasos por la falta de gestión documental

Tabla 1. Aspectos positivos y negativos sobre la gestión del SGSI por parte de los involucrados [23]

2) Falta de apoyo institucional

Hay que tener en cuenta que es primordial dentro del marco de implementación del SGSI el respaldo de la alta gerencia, a pesar de que esta sabe de su existencia e importancia, no se evidencia sus aportes para contribuir al éxito de este objetivo organizacional.

Una de los aportes por parte del representante de la alta gerencia es el reconocimiento de la falta de apoyo necesario para el SGSI, haciendo la salvedad que por parte del equipo de seguridad tiene que venderse la idea de que la seguridad de la información es algo que aporta valor agregado a las actividades de la organización; por tanto, se sugiere plantear y poner en marcha una estrategia de toma de conciencia para los directivos de la alta gerencia para explicarles con detalle la importancia de la implementación del SGSI.

Bajando un poco en el organigrama, se llevan a cabo capacitaciones, pero, se evidencia que los empleados dentro del alcance de la certificación no se comprometen con el objetivo y olvidan que deben hacer un esfuerzo en apropiarse de los procesos que se encuentran mencionados en la documentación del SGSI.

TABLA II
FALTA DE APOYO INSTITUCIONAL

Positivos	Negativos
Ninguno reportado.	No se evidencia compromiso por parte de la alta gerencia para la ejecución de los procesos.

Tabla 2. Aspectos positivos y negativos del apoyo institucional [23]

3) Falta de experticia del personal que compone el equipo de seguridad

La falta de profesionales especializados en seguridad de la información debido a la escasez de vacantes. Es muy común que el cargo de Oficial de Seguridad de la Información recaiga en un profesional sin la experiencia necesaria en este tipo de tareas, para este caso, el gerente de TI asumió la responsabilidad por ser conocido de la alta gerencia y las dependencias de la institución.

La empresa para ese entonces estaba en un proceso de separación, lo que disminuyó en gran medida la disponibilidad del gerente de TI, desencadenando la contratación de la Oficial de Seguridad de la Información, quién actualmente lidera este proceso; sin embargo, es necesario ampliar el departamento para tener personal especializado con conocimientos avanzados en este tema con el objetivo de formarlos en el monitoreo y avance de la implementación del SGSI.

TABLA III
FALTA DE PERSONAL CAPACITADO EN LA ORGANIZACIÓN [23]

Positivos	Negativos
La contratación y formación de personal especializado está avanzando	Falta de experiencia de empleados del área de seguridad Falta de experiencia sobre conciencia en seguridad a nivel general

Tabla 3. Aspectos positivos y negativos sobre la falta de personal capacitado en la organización [23]

F. Hallazgos de auditoría interna

La compañía, actualmente se encuentra en proceso de certificación, habiendo completado la primera auditoría interna, que dio lugar a 135 hallazgos, los cuales se están corrigiendo para poder cumplir la meta de conseguir la certificación; a pesar de que este proceso no ha terminado, se presentan a continuación los errores más frecuentes que se han presentado a lo largo de la implementación del SGSI.

1) Falta de adaptación al cambio

Para la compañía ha sido complicado adoptar buenas prácticas que permitan resguardar de manera segura la información, la falta de compromiso por parte de los líderes de área para la definición de los objetivos de seguridad planteados ocasionó un diseño de SGSI por encima de las posibilidades de la organización.

Adicionalmente se cree que la implantación y el mantenimiento de un SGSI es responsabilidad única del Departamento de Seguridad, los empleados no son conscientes del papel que juegan dentro del sistema ya que se requiere que modifiquen, perfeccionen o diseñen nuevamente la forma en que llevan a cabo sus funciones; en repetidas ocasiones se ha mencionado que en este proyecto se deben ver involucradas personas de muchas áreas ya que todos en diferentes medidas manejan información que puede ser de carácter sensible.

2) Dependencia absoluta del sistema a una consultora externa.

La consultoría externa que se contrató para ayudar en la implementación del SGSI no fue acorde con las necesidades de la organización, se pretendía copiar partes de SGSI de otras empresas, sin conocer de antemano las actividades habituales de la compañia.

3) Mentalidad demasiado optimista

La empresa es nueva en el tema de certificaciones de todo tipo y desde la dirección se quiso diseñar un SGSI que supla

muchos requerimientos, pero no se tuvo en cuenta que, en el proceso de implementación, las personas involucradas deben aportar tiempo de sus tareas diarias; por tanto, la prioridad que se tiene que dar al SGSI no fue la esperada.

Se piensa que una vez se obtenga la certificación el proceso del SGSI termina y se generan más clientes, pero en ningún caso se tiene éxito en la implantación de este sistema con el único fin de conseguir la acreditación, lo que genera valor para la organización es el mantenimiento constante y continuo en el tiempo.

G. Recomendaciones

Se deben establecer políticas estandarizadas de seguridad de la información que sean diseñadas con el fin de suplir correctamente las necesidades del negocio para no incurrir en gastos de recursos; también es preciso inculcar a las personas que la seguridad no es un tema más de la organización; por el contrario, se busca que estas se integren de manera transparente al trabajo que es realizado día a día por los empleados, sin perder el foco de la aplicación de las nuevas normas organizacionales en materia de seguridad de la información.

Se debe proporcionar instrumentos que sean de fácil manejo para que los empleados se acostumbren al manejo asertivo de documentos.

Buscar a corto plazo la implementación del SGSI para que las buenas prácticas en seguridad de la información sean funcionales para operar a nivel de toda la organización.

Buscar apoyo por parte de entidades externas que puedan llegar a ser un "compañero", es decir, que primero se enfoquen en entender bien el negocio y sus objetivos, así se puede enfocar de mejor manera los esfuerzos en la construcción de un SGSI que se adapta correctamente a la compañía.

Las estrategias para la toma de conciencia del personal en temas de seguridad de la información, debe ser a través de la ejecución de un plan operativo de concientización para buscar la mejor manera de ser implementado (ya sea una vez por mes o al momento de ingresar la persona a la organización), este debe ser orientado según el público objetivo ya que los departamentos involucrados en muchas ocasiones no tienen amplios conocimientos del tema.

Basado en el estado actual de la empresa, es necesario que se determine un presupuesto inicial, siendo conscientes que este permita realizar las tareas propuestas para conseguir la certificación ISO27001. Sin este presupuesto es muy difícil garantizar la adquisición de controles que permitan mitigar el riesgo que hay presente en la organización.

VIII. CONCLUSIONES

La compañía considera que la certificación es "un sello" útil en temas de imagen, y que es urgente conseguir para que el personal recupere sus actividades, tal y como eran antes de la implantación.

Por otra parte, en otras empresas que logran la certificación con éxito pero que sufren dificultades a mediano plazo para mantener sus SGSI, por no haber localizado con antelación los recursos necesarios que garanticen estas labores básicas.

Como menciona You Cheng Hwee, consultor especializado en seguridad y auditor principal SGSI reconocido por IRCA, *"Las compañías que desean proteger el flujo de la información interna y conseguir mayor confianza de sus socios comerciales no deberían apresurarse. El 80% de estas compañías ha fallado en la implantación de la norma ISO27001 en seguridad."*. [5]

Se deben focalizar los esfuerzos en las tareas de implementación de la norma con el objetivo que el proyecto sea económicamente rentable y permita alcanzar la certificación en un corto plazo; tareas como el análisis de procesos de negocio para añadir al SGSI puede aplicarse para potenciar estrategias de negocio que brinden una ventaja competitiva al cliente e incremente los beneficios a mediano y largo plazo.

El objetivo final de este documento es, que durante el desarrollo de este, se muestre el estado actual y los beneficios suficientes para animar al consejo directivo y al lector a buscar nuevas estrategias para la correcta implementación del SGSI en la compañía, y lograr que aquellos procesos clave de negocio estén dentro de su propio ámbito de gestión e intereses particulares.

El procedimiento analizado para el caso de estudio debería aplicarse no solo a los servicios publicados, sino también a los servicios de la plataforma en la nube; en este caso, utilizamos el marco de seguridad desarrollado por la organización para administrar la seguridad de la plataforma desde la perspectiva del cliente.

El enfoque de este marco proporciona un proceso de gestión de seguridad, un conjunto de modelos basados en estándares para describir la plataforma y sus servicios, las necesidades de seguridad de diferentes partes interesadas, amenazas conocidas, riesgos y mitigaciones para un despliegue en la nube; finalmente, una herramienta que respalda el desarrollo del plan de seguridad para la automatización parcial de un plan de seguridad ajustado a las necesidades del cliente. Este enfoque es integral y busca respaldar todas las perspectivas de las partes interesadas que colaboran, permitiendo que desarrollen un modelo de seguridad de manera mutua.

Se aborda la naturaleza multi-cliente de los servicios alojados en la nube cuando los clientes tienen diferentes requisitos de seguridad, esto se logra manteniendo y administrando múltiples perfiles con múltiples controles de seguridad según la línea base proporcionado por Eramba. Dichos controles son entregados por diferentes proveedores de seguridad; esto permite gestionar la trazabilidad entre los controles, los riesgos encontrados e identificar cuáles son los aún no mitigados.

La creación de planes de gestión de riesgos para un servicio en la nube tiene dos escenarios posibles: el primero, es dejar que cada cliente realice todo su plan como si fuera el único usuario del servicio; el segundo, consiste en acumular todos los requisitos de seguridad de los clientes en uno integrado. El último escenario es más sencillo porque permite que, las partes interesadas colaboren juntas para asegurar la plataforma y sus servicios con un conjunto de requisitos de seguridad.

Actualmente se está explorando un proceso de desarrollo de controles e ingeniería de seguridad en la nube para desarrollar servicios más flexibles que se ajusten a los requisitos de más clientes según lo investigado para plataformas "on-premise". Según lo pactado con el comité directivo, este marco necesita

una mayor extensión para lograr una automatización en la fase de implementación de controles de seguridad; esto requiere poder transformar las configuraciones base de la plantilla del plan de seguridad que permitan un despliegue rápido de la configuración de controles de seguridad específicos.

REFERENCIAS

[1] M. &. I. Bureau of Standards, Un estudio en la internacionalizacion de estandares nacionales ” „ 2006.

[2] CISCO, "Informe anual de seguridad," 2016. [Online]. Available: https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf. [Accessed 24 Abril 2018].

[3] J. Cano, "VIII encuesta nacional de seguridad informatica," 2007.

[4] J. Cano, "Seguridad de la informacion en latinoamerica tendendicias 2009," 2009.

[5] A. L. Neira, "Privacidad y beneficio economico en un SGSI," 2006.

[6] A. &. O. A. &. K. S. &. C. A. Omotunde, "Survey of Cloud Computing Issues at Implementation Level," *Journal of Emerging Trends in Computing and Information Sciences*, no. 4, pp. 91-96, 2013.

[7] Standards for Security Categorization of Federal Information and Information Systems, Febrero 2004. [Online]. Available: https://citadel-information.com/wp-content/uploads/2012/08/FIPS-PUB-199-final.pdf. [Accessed 18 Abril 2018].

[8] Ministerio de Hacienda y Administraciones Públicas, Gobierno de España, "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.," Octubre 2012. [Online]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Accessed 18 Abril 2018].

[9] Software Engineering Institute, "Introducing OCTAVE Allegro: Improving the information security risk assesment process," May 2007. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf. [Accessed 18 Abril 2018].

[10] Microsoft, "Introduction to Azure Security," 21 Noviembre 2017. [Online]. Available: https://docs.microsoft.com/en-us/azure/security/azure-security. [Accessed 18 Abril 2018].

[11] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed 18 Abril 2018].

[12] M. P. Surya Nepal, in *Security, privacy and trust in cloud systems*, 2013, p. 459.

[13] Microsoft, "Microsoft cloud services compliance and risk assesment," 2017. [Online]. Available: https://www.microsoft.com/en-us/trustcenter/guidance/risk-assessment. [Accessed 20 Abril 2018].

[14] MITRE, "Common platform enumeration," [Online]. Available: https://cpe.mitre.org/. [Accessed 20 Abril 2018].

[15] MITRE, "Common Weakness Enumeration," [Online]. Available: https://cwe.mitre.org/data/index.html. [Accessed 20 Abril 2018].

[16] MITRE, "Common attack pattern enumeration and classification," [Online]. Available: https://capec.mitre.org/. [Accessed 2018 Abril 2018].

[17] MITRE, "Common vulnerabilities and exposures," [Online]. Available: https://cve.mitre.org/. [Accessed 20 Abril 2018].

[18] NIST, "Common configuration enumeration," [Online]. Available: https://nvd.nist.gov/config/cce/index. [Accessed 20 Abril 2018].

[19] J. C. Najar Pacheco and N. E. Suarez Suarez, "La seguridad de la información: un activo valioso de la organización," *Vinculos*, vol. 12, 2015.

[20] International Standard Organization, "ISO 27001," 2013.

[21] Gartner, "Magic Quadrant for Intelligent Business Process Management Suites," 2016.

[22] D. Kosutic, «Cuatro beneficios clave de la implementación de la norma ISO 27001,» [En línea]. Available: https://advisera.com/27001academy/es/knowledgebase/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001/.

[23] C. O. Manager and S. Officer, Interviewees, *Entrevista sobre estado actual de la implementacion del SGSI en Bizagi*. [Interview]. December 2017.

[24] ISO Tools, "12 Beneficios de Implantar un SGSI de acuerdo a ISO 27001," 30 Marzo 2016. [Online]. Available: http://www.isotools.cl/12-beneficios-de-implantar-un-sgsi-de-acuerdo-a-iso-27001/. [Accessed 25 Octubre 2017].

[25] Kaspersky Lab Iberia, "Soluciones de seguridad flexibles para empresas," España, 2015.

[26] J. G. I. M. M. Almorsy, "An analysis of the cloud computing security problem," 2010.

[27] Bizagi, *Cloud Platform Security Framework*, Bogota, 2017.

[28] Eramba, *Bizagi compliance and risk management application*, London, 2018.

Manuel Francisco Tenorio Sánchez
Ingeniero de sistemas de la Fundación Universitaria San Martin (2014), actualmente estudiante de la Especialización en Seguridad Informática ESI_34