ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ PADILLA & CÍA. LTDA, QUE BRINDE UNA ADECUADA PROTECCIÓN EN SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN.

SANDRA YOMAY SUAREZ PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2015

ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ PADILLA & CÍA. LTDA, QUE BRINDE UNA ADECUADA PROTECCIÓN EN SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN.

SANDRA YOMAY SUAREZ PADILLA

Monografía para optar al título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ELEONORA PALTA VELASCO
Ms(c) Ingeniería Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2015

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del tutor del proyecto

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., 01 de Octubre de 2015

“Dedicado a Dios todopoderoso por darme las fuerzas y sabiduría necesarias para seguir adelante, a mis padres que desde el cielo aún me guían y me protegen; a mis hijas Sandra y Diana quienes son mi razón de ser y que con su gran amor me han dado las fuerzas para poder cumplir esta etapa tan importante de mi vida; a mi esposo por su inmenso apoyo y por impulsarme siempre a que cumpla con éxito los retos que me presenta la vida; a Juan Pablo Castro quién fue mi soporte y ayuda en el desarrollo y cumplimiento de esta tesis y a mi familia que de una u otra manera me ayudaron a la consecución de esta meta personal y profesional”

Sandra Yomay Suárez Padilla

AGRADECIMIENTOS

En primer lugar agradezco a Dios por su infinita bondad y misericordia, a Suárez Padilla & Cía. Ltda por la colaboración recibida durante la etapa de recolección de información; a la Universidad Nacional Abierta y a Distancia y su Facultad de Tecnología e Ingeniería por mantener ese modelo innovador y flexible que me ha permitido hacer posible la culminación de este proyecto.

Mi especial gratitud a:

- ✓ El Ingeniero Carlos Julio Erazo, tutor del proyecto inicial por orientarme con sus aportes y a la Ingeniera Eleonora Palta Velasco, por compartir sus conocimientos, por su constante colaboración y sus recomendaciones que encaminaron a la realización del mismo.

- ✓ A mi familia, amigos y compañeros que confiaron en mis capacidades y que en algún momento de sus vidas soñaron verme cumplir esta meta.

CONTENIDO

pag.

LISTA DE TABLAS

pag.

LISTA DE FIGURAS

pag.

LISTA DE ANEXOS

pag.

GLOSARIO

ACTIVO DE INFORMACIÓN: recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

ALTA DIRECCIÓN: está conformada por la gerencia y directivos de la organización

AMENAZAS: eventos que pueden desencadenar un incidentes en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

ANÁLISIS DE RIESGOS: método sistemático de recopilación, evaluación, registro y difusión de información requerida para formular recomendaciones encaminadas a la adopción de una medida en respuesta a un determinado peligro.

CONTROL: medida preventiva o correctiva ante la presencia de diferentes riesgos.

EFECTIVIDAD: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

EFICACIA: grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

EFICIENCIA: relación entre el resultado alcanzado y los recursos utilizados.

ESTIMACIÓN DEL RIESGO: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

IMPACTO DE UN ACTIVO: consecuencia sobre éste de la materialización de una amenaza.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento o serie de eventos de seguridad de la información no deseados o esperados, que pueden comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: Datos relacionados que tienen significado para la organización.

ISMS: término en ingles de SGSI. Information Security Management System.

ISO: International Standard Organization. En español Organización de Estándares Internacionales.

PROBABILIDAD: posibilidad de que una amenaza aproveche la vulnerabilidad para materializar el riesgo.

PDCA: Acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

PROCESO: actividades relacionadas entre sí o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

PYME: pequeñas y medianas empresas

RIESGO: toda posibilidad de ocurrencia de una situación que pueda impedir el desarrollo normal de las funciones de la empresa dificultando el logro de sus objetivos.

RIESGO RESIDUAL: valor de riesgo tras la aplicación de uno o varios controles.

SEGURIDAD INFORMÁTICA: asegurar que los recursos del sistema de información de una organización sean seguro y confiables, mediante el establecimiento de normas, métodos y técnicas.

S.G.S.I: Sistema de Gestión de Seguridad de la Información

TRANSFERENCIA DEL RIESGO: Compartir con otra de las partes la pérdida de un riesgo.

VULNERABILIDADES: debilidades que son aprovechadas por amenazas y generan un riesgo

RESUMEN

El trabajo final de la especialización, describe los objetivos, el alcance, la expectativa del SGSI y la metodología asociada a la definición, planeación, identificación y diseño del modelo de seguridad de la información para la organización Suárez Padilla & Cía Ltda, basado en la norma ISO 27001:2013; iniciando con el análisis de la situación actual de la organización desde la óptica de los procesos críticos de la operación documental, ejecución del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para Suárez Padilla & Cía Ltda.

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). De acuerdo a las siguientes fases del proyecto:

- ✓ Definición de la situación actual.
- ✓ Análisis de Riesgos.
- ✓ Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
- ✓ Identificación de amenazas, evaluación y clasificación de las mismas
- ✓ Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2005 en la organización.
- ✓ Esquema Documental del sistema de gestión de seguridad de la información.
- ✓ Definición de Políticas, selección de objetivos de control y controles del anexo A de la norma ISO 27001; establecer estrategias de contingencia.

Palabras Clave: ANÁLISIS DE LA SITUACIÓN ACTUAL, SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, ANÁLISIS DE RIESGOS, VALORACIÓN DE ACTIVOS

INTRODUCCION

En el presente trabajo se lleva a cabo el proceso de análisis y diseño de un Sistema de Gestión de Seguridad de la Información aplicado a la empresa Suárez Padilla & Cía. Ltda, organización asesora de seguros. El objetivo primordial de un Sistema de gestión de seguridad de la información es proteger la integridad, confidencialidad e integridad de todos los activos de una organización y este se logra efectuando como primera medida un minucioso análisis de los riegos a los que se enfrentan los activos de información para luego, con este insumo implantar los controles necesarios que protegerán dichos activos.

En la actualidad las Pymes afrontan una problemática muy grande debido a que muchas de ellas no destinan recursos para afrontar la falta de seguridad, ni prevenir los riesgos de sus activos de información asociados a la misma, lo que en muchas ocasiones genera en la organización pérdidas tanto económicas como de información. Teniendo en cuenta lo anterior y buscando no verse afectada por un incidente mayor es que Suárez Padilla & Cía. Ltda ha decidido dar un paso adelante e iniciar con el proceso de establecer un Sistema de Gestión de Seguridad de la Información y así garantizar que los accedan a su información sean quienes estén autorizados.

Se presenta un modelo apoyado en estándares y normas internacionales tales como ISO/IEC 27001:2013 y el estándar ISO/IEC 27002, que buscan evitar, disminuir y/o prevenir ataques o desastres informáticos, antes que éstos ocurran. Se iniciará con un proceso de análisis de la situación actual de la empresa, luego se deberá realizar el inventario de activos y a partir de este llevar a cabo la definición del análisis de riesgos, para un posterior diseño de políticas, procesos y procedimientos claros que permitirán determinar y establecer los controles de seguridad que ayuden a gestionar los riesgos identificados.

Este trabajo se estructura en cinco (5) capítulos a saber: el Capítulo 1 Generalidades del proyecto donde se presenta temas como la formulación de problema, objetivos tanto general como los específicos, la justificación, los beneficios del proyecto, el alcance y limitaciones; en el Capítulo 2 encontramos el estado de arte del proyecto, en él se describen algunas investigaciones que se tuvieron en cuenta como referente para llevar a cabo el proyecto. El Capítulo 3 Marco Referencial con temas como Marco Teórico, Marco Conceptual y Antecedentes donde se detalla la teoría sobre la que se sustenta el proyecto. El Capítulo 4 se encuentra el Diseño Metodológico a aplicar y los aspectos administrativos. El Capítulo 5 encontramos las conclusiones, y finalmente la bibliografía consultada y los anexos correspondientes.

1. GENERALIDADES DEL PROYECTO

1.1 TITULO DEL PROYECTO

ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ PADILLA & CÍA. LTDA, QUE BRINDE UNA ADECUADA PROTECCIÓN EN SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN.

1.2 TEMA U OBJETO DE ESTUDIO

El presente proyecto se enfoca en llevar a cabo el diagnóstico de la situación actual de la seguridad de la información de la empresa de seguros Suárez Padilla & Cía. Ltda, y con base en este diagnóstico analizar y diseñar un Sistema de Seguridad de la Información que permita una adecuada implementación, en aras de que su funcionamiento y operación, garantice la integridad, confidencialidad y disponibilidad de su información.

1.3 LÍNEA DE INVESTIGACIÓN

La línea de investigación, está delimitada en la Cadena Ingeniería Electrónica, Telecomunicaciones y Redes

LINEA 1: Infraestructura tecnológica y seguridad en redes (Área Telecomunicaciones).

2. PROBLEMA DE INVESTIGACIÓN

2.1 FORMULACIÓN DEL PROBLEMA

En la actualidad las organizaciones y sus sistemas de información se deben enfrentar, cada vez más, con riesgos e inseguridades informáticas provenientes de una amplia variedad de fuentes, entre las cuales podemos incluir fraudes basados en informática, espionaje, sabotaje y adicional a esto daños ocasionados por virus informáticos y ataques de intrusión o de negación de servicios los cuales son cada día más comunes en una organización.

La Empresa de seguros Suárez Padilla & Cía. Ltda, recibe información personal y financiera tanto de sus clientes como de sus proveedores por múltiples fuentes, por diferentes medios y a través de múltiples canales (personal, telefónico, empresas de mensajería, electrónicos, redes de datos, sistemas en línea, entre otros); estos volúmenes de datos e información constituyen la materia prima para la gestión de la empresa, lo que la convierte en un activo de gran importancia que debe ser protegida desde su origen hasta su destino final.

Independiente de la manera como esta información se reciba, se comparta o almacene, debe tener una adecuada protección, sin embargo la seguridad informática establecida por la compañía en este momento es limitada e insuficiente, ante lo cual se optó como primera fase llevar a cabo un análisis minucioso de la situación actual y con base en el resultado, elaborar un Sistema de Gestión de la Seguridad de la Información para que posteriormente en una segunda fase sea implementado por parte de los funcionarios responsables de la seguridad de la información en la empresa Suárez Padilla & Cía. Ltda, involucrando a su personal como parte activa y creativa del proyecto; lo que se pretende es garantizar que los riesgos que afronta la empresa en términos de seguridad de la información sean conocidos por la alta gerencia a fin de determinar si serán , asumidos, gestionados y/o minimizados, permitiendo la creación de un entorno seguro para los datos, la información, las aplicaciones y los sistemas que sustentan su gestión.

3. JUSTIFICACIÓN DEL PROYECTO

Teniendo en cuenta el creciente aumento de amenazas informáticas que buscan sustraer de las empresas su información, para con ella llevar a cabo fraudes financieros, efectuar ataques de denegación de servicio o afectar a la imagen de una organización, como así lo demuestran en sus informes las empresas encargadas de los temas de seguridad, ha obligado a las organizaciones a darle prioridad al tema de la seguridad de la información ya que tanto la información como los procesos y los sistemas que hacen uso de la misma, son sus activos más valiosos.

Las organizaciones han entendido que si los mecanismos de protección informática implementados fallan, es necesario contar con procesos estructurados y personal especializado que maneje incidentes de seguridad de información y restablezca los temas en el menor tiempo posible (Georgia, 2003). Es por esto que en la actualidad poder asegurar la confidencialidad, integridad y disponibilidad de la información más sensible llegan a ser esenciales para ellas en aras de mantener sus niveles de competitividad, beneficio económico, conformidad legal e imagen empresarial obligatorios para lograr los objetivos de la organización, asegurando obtener beneficios económicos.

Los datos e información constituyen la materia prima para la gestión de la empresa de seguros Suarez Padilla y Cía Ltda y es deber de la organización garantizar la confidencialidad, integridad y disponibilidad de esta información; la dirección es consciente que la seguridad establecida por la compañía en este momento es limitada e insuficiente, es por esto que requieren como una primera etapa, se realice un análisis de la situación actual de la empresa en cuanto a la seguridad informática, y con base en este diagnóstico se diseñe un Sistema de Seguridad que permita ofrecer un mejor nivel de servicio en calidad, funcionalidad y facilidad en el uso de la seguridad, de manera tal que al ser implementado minimice costos a la organización.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Realizar el Análisis y Diseño de un Sistema de Gestión de Seguridad Informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización, en aras de mejorar la seguridad de las tecnologías de información y las comunicaciones en la empresa.

4.2 OBJETIVOS ESPECÍFICOS

4.2.1 Realizar el diagnóstico de la situación actual de la seguridad de la información de la empresa de seguros Suárez Padilla & Cía. Ltda.

4.2.2 Identificar los propietarios, responsables y ubicación de los activos de información a través de cuestionarios, entrevistas y otros.

4.2.3 Clasificar y valorar los activos de información.

4.2.4 Adelantar el análisis de riesgos de los activos a vincular a la matriz de riesgos.

4.2.5 Identificar mediante el análisis de riesgo, las amenazas y vulnerabilidades a las que están expuestas los sistemas de información.

4.2.6 Seleccionar los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información.

4.2.7 Sugerir políticas de seguridad que permitan hacer un uso aceptable de los activos de información.

4.3 BENEFICIOS DE REALIZAR EL ANÁLISIS Y GESTIÓN DE RIESGOS

4.3.1 Se establecerán metodologías de gestión de la seguridad informática de manera clara y estructurada.

4.3.2 Crear conciencia en los responsables de los procesos del negocio, de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.

4.3.3 Reducción de riesgo en cuanto a pérdida o robo lógico de la información.

4.3.4 Se brindará mayor confianza a los clientes al garantizar la confidencialidad de la información.

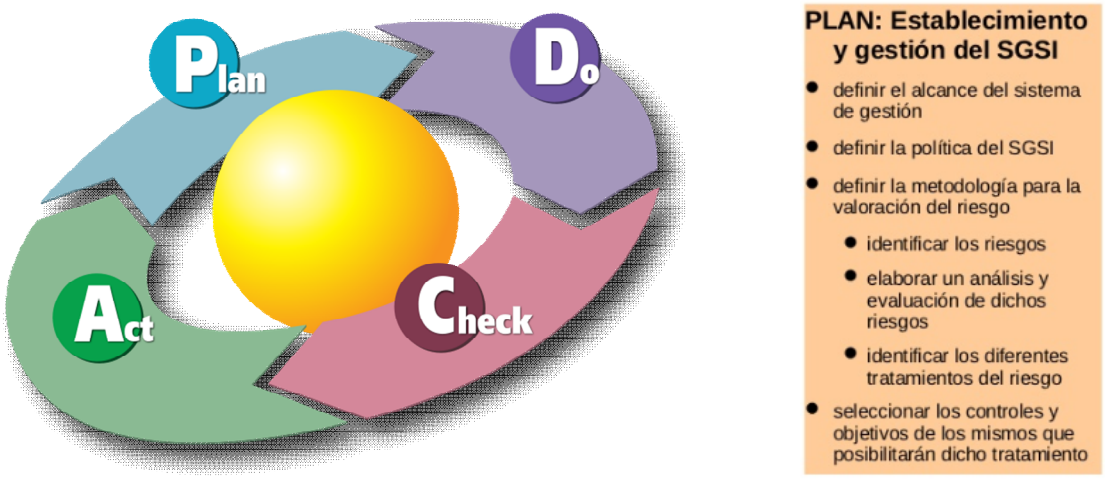
4.3.5 Al establecerse planes de contingencia Informático, se garantiza la continuidad del de negocio tras incidentes de gravedad.

5. ALCANCE Y LIMITACIONES

5.1 ALCANCE

El proyecto se llevara a cabo en la empresa de seguros Suárez Padilla & Cía Ltda y abarcará la fase del **Plan** del modelo PDCA del ciclo de Deming aplicado a un SGSI.

Figura 1. Fase del Plan del modelo PDCA del ciclo de Deming



Fuente: descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html

De acuerdo al estándar internacional ISO/IEC 27001:2013, re realizará un diagnóstico de la situación actual de la seguridad de la información, se evaluarán las amenazas, riesgos e impactos, permitiendo así un análisis comparativo de los controles a ser establecidos en la organización, respecto a los controles planteados en la norma.

Lo anterior teniendo en cuenta que con ellos se abordan las tres (3) áreas críticas de cualquier organización como son los activos, seguridad física y ambiental, y el control de acceso y adicionalmente estos dominios están directamente relacionados con los tres pilares básicos de la seguridad como son: la confidencialidad, integridad y disponibilidad.

5.2 LIMITACIONES

5.2.1 Geográfica. El Proyecto se desarrollara en las instalaciones de la empresa Suárez Padilla & Cía Ltda, ubicada en la CA 68 B 78 24 INT 6 de la Ciudad de Bogotá D.C., donde se diseñara un sistema de gestión de seguridad de la información.

5.2.2 Temporal. Este proyecto se ejecutará en un término de 2 Meses, de acuerdo con las diferentes actividades a realizar durante el desarrollo del mismo.

5.2.3 Conceptual. Los conceptos a manejar en este proyecto son los relacionados con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, Administración de Riesgos, Políticas de Seguridad de la Información y Controles.

5.2.4 Operativa. Este proyecto diseñará un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa de seguros Suárez Padilla & Cía. Ltda, en aras de lograr un excelente nivel de protección de los activos de información de acuerdo con el valor y riesgo que represente para la organización.

5.2.5 Personal. El estimular a las personas que laboran en Suárez Padilla & Cía Ltda sobre la importancia que tiene esta investigación en relación con sus labores diarias, permitiéndoles trabajar con mayor seguridad.

5.2.6 Económicas. A través de la realización de este proyecto, se proveerá de medios que permitan resolver los problemas que ahora se presentan, para que en el futuro no generen grandes gastos en relación a todo lo que sea seguridad de la información.

6. MARCO DE REFERENCIA

6.1 MARCO TEÓRICO

6.1.1 Estado del Arte. En la actualidad la seguridad de la información debe ser un componente crítico en la estrategia de negocio para cualquier organización, adicionalmente debe ser manejada en un proceso integral, que garantice "protección" en todos los aspectos (físicos, lógicos, humanos), bajo esta visión en los últimos años en Colombia las organizaciones tanto en el ámbito público como en el privado, vienen blindando sus infraestructuras tecnológicas contra todo tipo de amenazas, en aras de proteger su infraestructura crítica y por ende sus procesos vitales.

Resultado de este nuevo enfoque empresarial se han venido desarrollado estudios, investigaciones y proyectos de grado relacionados con el tema de seguridad informática, los cuales han sido tomados como referentes para el desarrollo del presente trabajo, los cuales se describen a continuación:

"Experiencia personal: dificultades en la implementación de un SGSI" [1] **- Leonardo Camelo.** A la hora de hacer la implementación y desarrollo de un plan de SGSI, es importante tener en cuenta los problemas con los que se va a encontrar, teniendo en cuenta que se aplicará sobre una empresa que ya se encuentra constituida y la implementación de estos planes precisan de cambios en distintas áreas tales como manejo de personal, manejo de información, cambio de políticas e inversión de recursos.

Dentro de las dificultades a la hora de implementar un SGSI quizá la más significativa es la del dinero, no se puede hablar de dinero sin haber hecho previamente una adecuada evaluación de riesgos la cual nos indique a que amenazas está expuesta la Organización, y allí si determinar cuáles serían los controles a implementar sabiendo obviamente cuales costos van a representar. Este tema si va en un solo sentido: no se puede hablar primero de dinero y luego de controles.

Aun así una vez se haga una adecuada evaluación de los riesgos será más controlable la variable riesgo.

[1] CAMELO, Leonardo. Seguridad de la Información en Colombia. Experiencia personal: dificultades en la implementación de un SGSI. [En línea].2010. [Consultado 26 de diciembre, 2014]. Disponible en Internet: (seguridadinformacioncolombia.blogspot.com.co/2010/02/experiencia-personal-dificultades-en-la.html)

“Marco Normativo (Normas y políticas) de un SGSI”[2] **- Leonardo Camelo.** El tema de reglamentación de seguridad de la información en Colombia es prácticamente inexistente, por lo que todo SGSI está fundamentado netamente en la 27001 con los controles de la 27002 (Anexo A de la 27001).

Para implementar con éxito un SGSI se debe constituir un modelo normativo el cual puede estructurarse mediante el documento de políticas, teniendo en cuenta uno a uno todos los dominios y normas que complementen a la política y que agrupen los objetivos de control existentes en la ISO 27002, obteniendo así 10 Políticas, y 30 normas o más en busca de cubrir completamente lo incluido en esta Norma.

“Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0”[3] **- Ministerio de Tecnologías de la Información y las Comunicaciones.** El documento presenta una estrategia de preparación por parte del Gobierno para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL) como modelo sostenible, y cubre desde la preparación de la organización para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del SGSI como modelo sostenible.

En el capítulo tres (3), se presenta la alineación del Modelo de seguridad de la Información con la arquitectura empresarial de la Estrategia de Gobierno en línea. En el capítulo cuatro (4), se presenta una estrategia de preparación por parte del gobierno central para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL) como modelo sostenible. Posteriormente, en el capítulo cinco (5), se cubre la preparación de la organización para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) como modelo sostenible.

“La importancia de un SGSI”[4] **- Federico Pacheco.** Para el autor de este artículo un SGSI permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, brindando la opción de observar los

[2] CAMELO, Leonardo. Seguridad de la Información en Colombia. Marco Normativo (Normas y políticas) de un SGSI. [En línea]. 2010. [Consultado 14 de diciembre, 2014]. Disponible en Internet: (seguridadinformacioncolombia.blogspot.com.co/2010/03/marco-normativo-normas-y-politicas-de.html).

[3] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. [En línea].Versión 2.0.2. 49p.Bogotá, 2011. [Consultado 15 de diciembre, 2014]. Disponible en Internet: (css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf)

[4] PACHECO, Federico. La importancia de un SGSI. Welivesecurity en Español. [En línea].2010. [Consultado 14 de diciembre, 2014]. Disponible en Internet: (www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/)

resultados obtenidos al aplicar las medidas de seguridad; con estos resultados la alta gerencia podrá tomar mejores decisiones estratégicas.

Adicionalmente define como punto importante a tener en cuenta el que un SGSI se debe documentar muy bien y debe darse a conocer a todo el personal de la organización en todos los niveles jerárquicos, teniendo en cuenta que será necesario implantar diferentes controles que ayudarán a mantener los riesgos potenciales en un nivel bajo

Una organización debe considerar dentro de sus prioridades establecer un SGSI si realmente quiere administrar la seguridad en su organización, especialmente para conseguir eficiencia y garantía en la protección de sus activos de información.

"Resumen Ejecutivo Memoria TFM Plan de Implementación del SGSI" - Robin J. Salcedo B[5]**.** Describe los objetivos, el alcance, la expectativa del SGSI y la metodología asociada a la definición, planeación, identificación y creación del modelo de seguridad de la información para la organización ISAGXXX, basado en la norma ISO 27001:2013; iniciando desde el entendimiento de la organización desde la óptica de los procesos críticos de la operación de energía, ejecución del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para ISAGXXX.

"Ciberseguridad, minuto y resultado: Los malos 3, Los buenos 0" [6] **- Javier Cao Avellaneda.** El autor hace una descripción de una manera diferente de su visión como Consultor en seguridad de la información sobre la Ciberseguridad y cómo "los malos" han impactado el mundo de los sistemas de información. Su visión la resume en tres goles que estos malos han marcado, donde el primer gol se debe a que no se le dio la suficiente importancia de la seguridad desde el diseño en la fabricación de software, ocasionando con ello productos inseguros.

El segundo gol se produce debido a que uno, las empresas no le dan la suficiente importancia al área de tecnología ocasionando la falta de recursos humanos

[5] SALCEDO, Robin. Plan de Implementación del SGSI basado en la Norma ISO 27001:2013. Memoria Trabajo Final Máster MISTIC. Barcelona: Universidad Oberte Catalunya. [En línea].2014. 43 p. [Consultado 13 de enero, 2015]. Disponible en Internet: (openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf)

[6] CAO, Javier. Sistemas de Gestión Seguridad de la Información. Los malos 3, Los buenos 0. [En línea]. 2014. [Consultado 13 de diciembre, 2014]. Disponible en Internet: (sgsi-iso27001.blogspot.com.co/2014/06/ciberseguridad-minuto-y-resultado-los.html)

especializados y recursos tecnológicos para afrontar los peligros cibernéticos generados por la conexión a Internet y que día a día acechan las empresas, pues como es sabido el delincuente online es internacional y el Internet no conoce fronteras; y dos la prioridad que se da a perseguir a los ciberdelincuentes es relativamente baja al igual que las penas por delitos cibernético, transmitiendo mensajes equivocados a la delincuencia online, la cual aumenta a gran velocidad.

El tercer gol se debe a que los malos desarrollaron una auténtica industria del malware logrado traspasar medidas de seguridad perimetral como Firewalls y antivirus. El malware ahora viene como un software inofensivo que el antivirus no detecta; en el fondo los malos están utilizando las mismas técnicas usadas en la protección legítima de datos pero para unas finalidades diferentes. Es por esto que con este nivel de sofisticación las medidas tradicionales ya están siendo superadas.

"Consejos de implantación y métricas de ISO/IEC 27001 y 27002" [7] **- Comunidad Internacional de implantadores de ISO27000 de ISO27001security.com.** Este documento pretende ayudar a otros que estén implantando o planeando implantar los estándares ISO/IEC de gestión de seguridad de la información. Al igual que los propios estándares ISO/IEC, se trata de un documento genérico y necesita ser adaptado a las necesidades específicas de cada uno.

Se considera la gestión de continuidad de negocio como un proceso con entradas provenientes de muchas funciones como: alta dirección, TI, operaciones, etc. y de diversas actividades entre ellas la evaluación de riesgos, asegurando la adaptación y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio. Deberían llevarse a cabo las pruebas pertinentes entre ellas simulacros, pruebas de failover, pruebas sobre el papel etc.) para de esa forma mantener los planes actualizados, aumentar la confianza de la alta dirección en los planes y por último familiarizar a los empleados relevantes con sus funciones y responsabilidades cuando se encuentren bajo condiciones de desastre.

[7] COMUNIDAD INTERNACIONAL DE IMPLANTADORES DE ISO27000 DE ISO27001SECURITY.COM. Consejos de implantación y métricas de ISO/IEC 27001 y 27002. Traducido por www.iso27000.es. [En línea] Versión 1, 16 p. 2007. [Consultado 26 de enero, 2014]. Disponible en Internet: (www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf)

“Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) Para La Realidad Tecnológica De La USAT”[8] **-** César Wenceslao De La Cruz Guerrero / Juan Carlos Vásquez Montenegro. El concepto central sobre el que se construye la norma ISO 27001, es el Sistema de Gestión de Seguridad de la Información (SGSI).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, el cual debe ser muy bien documentado y debe ser conocido por toda la organización.

No es posible garantizar el 100% de protección, ni siquiera si se dispusiera de un presupuesto ilimitado.

Según ISO 27001, la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad de la información y de los sistemas implicados en el tratamiento de la misma, dentro de una organización. Estos tres términos son la base sobre la que se construye el edificio de la seguridad de la información.

“Lo que no debes pasar por alto para gestionar la seguridad de la información”[9] **-** H. Camilo Gutiérrez Amaya. Para el autor al momento de integrar temas seguridad de la información con la organización lo más complicado es que estos no se orientan en las necesidades e intereses del negocio, razón por la cual revisa son los aspectos fundamentales que no se deben pasar por alto, tales como:

- ¿Qué debe garantizar nuestro Sistema de Gestión de Seguridad de la Información (SGSI)?
- La piedra angular: política de seguridad
- Clasificar la información corporativa
- Qué hacer y dónde enfocar esfuerzos: Análisis de riesgos

[8] DE LA CRUZ, César y VASQUEZ, Juan. Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT. Chiclayo: Universidad Católica Santo Toribio De Mogrovejo. [En línea], 2008, 160 p. Tesis de Grado Ingeniero De Sistemas y Computación. [Consultado 16 de diciembre, 2014]. Disponible en Internet: (cip.org.pe/imagenes/temp/tesis/42464064.doc)

[9] GUTIÉRREZ, Camilo. Lo que no debes pasar por alto para gestionar la seguridad de la información. En: Revista.Seguridad. [En línea]. no.22 (ago-sep.2014). p.04-06. [Consultado 26 de enero, 2015]. Disponible en Internet: (revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Num22.pdf)

- Lo que no se puede olvidar

“Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I”[10] **-** Miguel Ángel Mendoza López, Pablo Antonio Lorenzana Gutiérrez**.** En el ámbito de la seguridad de la información, una política es un documento donde se consignan las reglas o requisitos definidos y que deben cumplirse en una organización. Presenta una declaración formal, de manera breve y en un alto nivel, la cual que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada.

Las políticas de seguridad de la información proveen un marco para que los empleados de una organización sigan las mejores prácticas, permitiendo de esta manera minimizar riesgos y responder a incidentes inesperados, es por esto que al crearse el documento de las políticas es imprescindible tener en cuenta las operaciones cotidianas, los hábitos de sus empleados y la cultura organizacional, para así llegar a todas las audiencias logrando su aceptación y cumplimiento. Igualmente ayudan a la organización a asegurar sus activos, definir su postura ante la protección de la información frente a sucesos tales como: accesos no autorizados, modificación, divulgación o destrucción.

“Políticas Generales De Seguridad De La Información” - Ministerio de Ambiente y Desarrollo Sostenible[11]. Con el aumento en el número de incidentes de seguridad de la información en las organizaciones los cuales generan pérdidas financieras y reputacionales, se crea la necesidad de implementar un Sistema de Gestión de Seguridad de la Información donde se diseñen, documenten, implementen y monitoreen controles basados en una gestión de riesgos que minimice el impacto y/o la probabilidad, a fin de mantenerlos en niveles aceptables para la organización.

El Ministerio de Ambiente y Desarrollo Sostenible (MADS) decide establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI; por ello, divulga mediante este documento los aspectos relevantes en seguridad de la información de una forma general.

---

[10] MENDOZA, Miguel y LORENZANA, Pablo. Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I. En: Revista.Seguridad. [En línea]. no.16, (Ene-Feb 2013). p. 13-17. . [Consultado 17 de diciembre, 2014]. Disponible en Internet: (revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Seguridad_Num16_0.pdf)

[11] MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. Políticas Generales de Seguridad de la Información. [En línea]. Ver.1. 9p. Bogotá, 2014. [Consultado 14 de junio, 2015]. Disponible en internet: (https://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/Politica_de_seguridad__definitiva___pdf.pdf)

"Herramientas para la implantación de un SGSI[12]**" –** Oscar de la Cuesta. Listado de herramientas para la implantación de un Sistema de Gestión de la Seguridad de la Información.

"La norma ISO 27001:2013 ¿Cuál es su estructura?[13]**"** - ISOTOOLS EXCELLENCE. La norma ISO 27001:2013 no sólo establece cambios en el contenido sino también en la estructura, viéndose reflejada en otros documentos que hacen parte de la familia ISO 27000.

La norma ISO 27001:2013 se ha desarrollado con base en el Anexo SL, proporcionando un formato y una alineación conjunta que siguen el desarrollo documental de un Sistema de Gestión sin importarle el enfoque empresarial; todos los documentos que se relacionan con el Sistema de Gestión de Seguridad de la Información se alinean bajo la misma estructura evitando problemas de integración con otros marcos de referencia.

"Los pilares del SGSI"[14] **-** ISOTOOLS EXCELLENCE. Existe tres aspectos fundamentales que se deben tener en cuenta siempre y no se pueden descuidar, los cuales se resumen en tres pasos sencillos determinados cómo el ABC de la seguridad de la información:

- La seguridad en el negocio
- Buenas prácticas durante la gestión
- Concienciar a los usuarios

"¿Por qué implantar un SGSI basado en la norma ISO 27001?[15]**" -** ISOTOOLS EXCELLENCE. Según ISO-27001 un Sistema de Gestión de Seguridad de la Información eficaz, tiene que generar valor agregado a las organizaciones, ya que les permiten hacer mejor las cosas, es decir, de una forma mucho más económica y más rápida.

---

[12] DE LA CUESTA, Oscar. Herramientas para la implantación de un SGSI. [En línea]. 2015. [Consultado 16 de enero, 2015] Disponible en Internet: (www.palentino.es/blog/herramientas-para-la-implantacion-de-un-sgsi/)

[13] ISOTOOLS EXCELLENCE. SGSI. La norma ISO 27001:2013 ¿Cuál es su estructura? [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/)

[14] ISOTOOLS EXCELLENCE. SGSI. Los pilares del SGSI. [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/07/pilares-sgsi/)

[15] ISOTOOLS EXCELLENCE. SGSI. Por qué implantar un SGSI basado en la norma ISO 27001. [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/)

Implementar un Sistema de Gestión de Seguridad de la Información ISO 27001 ofrece la oportunidad de optimizar las áreas, dentro de la organización, relacionadas con la información que más le importan a la alta dirección de la empresa.

La norma ISO 27001 persigue un enfoque muy detallado hacía la Seguridad de la Información. Los activos necesitan proteger la información, ya sea en papel, en formato digital o los activos físicos, los empleados deben tener los conocimientos necesarios.

"Medición de un SGSI: diseñando el cuadro de mandos"[16] **- Javier Cao.** Implantar un SGSI debe siempre tener una motivación y unos objetivos concretos y tangibles. Por tanto, la medición que se debe instaurar dentro del sistema deberá tender a medir la realidad del cumplimiento de estos objetivos. Se pueden establecer tres grandes ejes donde colocar sensores de medición relacionados con las metas del SGSI, estos ejes son:

- De Metas de la Dirección
- Del riesgo
- Del tiempo

"Características deseables para un SGSI orientado a PYMES"[17] **-** Luís Enrique Sánchez, Antonio Santos-Olmo, Eduardo Fernández-Medina Y Mario Piattini. En este apartado, se analizan las metodologías deseables que debe tener un SGSI para su implantación y correcto funcionamiento analizado en el entorno de las PYMES. Estas características son el resultado del análisis detallado del estándar ISO27001 y el método de investigación en acción.

Estos aspectos se pueden cumplir de forma total, parcial o pudieron no haber sido abordados en el modelo. Los aspectos analizados son descritos a continuación:

[16] CAO, Javier. Medición de un SGSI: diseñando el cuadro de mandos. [En línea]. {12 de enero de 2011}. Disponible en Internet: (www.securityartwork.es/2011/01/12/medicion-de-un-sgsi-disenando-el-cuadro-de-mandos/)

[17] SÁNCHEZ CRESPO, Luis, *et al*. Características deseables para un SGSI orientado a PYMES. [En línea]. [03 de febrero de 2015]. 16p. Disponible en Internet: (www.researchgate.net/publication/232252352_Caractersticas_deseables_para_un_SGSI_orientado_a_PYMES)

Ciclo de SGSI: Se describen las fases de desarrollo, implantación y mantenimiento del SGSI.

Marco de trabajo: Describen los elementos que forman el SGSI luego de haberse implantado.

Niveles de madurez: Orientado a la implantación de una seguridad gradual basada en niveles.

Cultura de seguridad: Orientado hacia la cultura de la seguridad.

Guía de buenas prácticas: Contempla la integración de controles de seguridad o una guía de buenas prácticas.

Análisis y gestión del riesgo: Los activos del sistema de información deben ser sometidos a mecanismos de valoración y gestión de los riesgos.

Métricas: Mecanismos de medición de cumplimiento de los controles de seguridad.

Orientado a PYMES: Pensando particularmente en las PYMES.

Reutiliza el conocimiento: Adquiere conocimiento de las implantaciones, este conocimiento podrá ser reutilizado con el fin de facilitar implantaciones posteriores.

Dispone de herramienta software: herramienta que lo soporte.

Casos prácticos: Desarrollado a partir de casos prácticos.

6.2 MARCO CONCEPTUAL

6.2.1 Metodología de Gestión de riesgos. La Metodología de Gestión de Riesgos se enfocará a los activos de información de la organización que son identificados y valorados por cada responsable en Suárez Padilla & Cía. Ltda para poder diseñar, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI).

6.2.2 Identificación de activos de información. De acuerdo con la norma ISO/IEC 27001, “activo de información” se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido.

Según la anterior definición la primera actividad en la Gestión de Riesgos es identificar los activos de información y debe realizarse sin perder de vista el alcance definido y aprobado por la Alta Dirección para el Sistema de Gestión de Seguridad de la Información.

Para la identificación de los activos de información se tomará como fuentes los diferentes procesos de la organización junto con sus responsables que interactúan con el alcance establecido y aprobado para SGSI.

Actividades necesarias para la identificación de los activos de información:

- Identificar los procesos y agendar las entrevistas con sus responsables.
- Recolección de la información.
- Consolidar la información.
- Identificación de Propietario, responsable y ubicación

Los activos de información previamente identificados en el paso anterior, deben tener su respectivo Propietario, área o proceso donde se crea o custodia dicho activo; Responsable, es un funcionario perteneciente al área o proceso propietario de uno o un grupo de activos de información quien debe velar por que los controles de seguridad sean implementados; Ubicación, es el área física donde se mantiene el activo de información.

Actividades necesarias para la identificación de propietarios, responsable y ubicación:

- Identificar los propietarios, responsables y ubicación de los activos de información.

6.2.3 Clasificación de los activos de información. Se cuenta con nivel de clasificación de la información que ha sido establecido al interior de la organización con los siguientes criterios:

Interna: Información cuya divulgación no causa serios daños a la organización y su acceso es libre a través de cualquier otro medio de la organización.

Confidencial: Información cuya divulgación puede afectar considerablemente la misión de la organización, la divulgación de esta información, requiere de la aprobación del respectivo propietario o líder del proceso que se va a valorar.

Pública: Información que por sus características debe estar a disposición de persona natural o jurídica del Estado Colombiano.

Reservada: Información cuya divulgación causaría "serios daños a la organización si estuviera públicamente disponible.

Para los activos de información se cuenta con una clasificación de acuerdo a un tipo y clase en la organización:

Tabla 1. Clasificación de Activos de información

Tipo de activo	Clase de activo
Activos de Información Puros	Información Digital
	Información Física
	Activos de Información intangibles
Activos de Tecnologías de Información	Servicios de información
	Software
	Hardware de TI
	Controles ambientales

Tipo de activo	Clase de activo
Activos de Información Recurso Humano	Empleados
	Terceros

Tabla 1. (Continuación)

6.2.4 Valoración de los activos de Información. Seguidamente, los activos de información debe ser valorado de acuerdo a su impacto en términos de la pérdida de los tres (3) principios básicos de la seguridad de la información que son: la Confidencialidad, la Integridad y la Disponibilidad.

Partiendo de las tres (3) características de la seguridad de la información y el valor económico, se establece la escala de calificación que contempla cinco (5) niveles de impacto:

Tabla 2. Confidencialidad, Integridad y Disponibilidad

Valoración Cuantitativa	Valoración Cualitativa
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Tabla 3. Valoración Confidencialidad (C).

Escala Cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo**	Se puede acceder por cualquier usuario
2	**Bajo**	Se puede acceder solo por empleados o contratistas de la organización.
3	**Medio**	Se puede acceder por Líderes de Proceso.
4	**Alto**	Solo es posible el acceso para las personas citadas en lista de control de acceso.
5	**Muy Alto**	Solo es posible el acceso por personal de la Alta Dirección y externos pertenecientes al Estado, también

Fuente: El Autor

Tabla 4. Valoración Integridad (I).

Escala Cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo**	Puede ser modificado en cualquier momento por cualquier usuario
2	**Bajo**	Es posible la modificación por cualquier funcionario o contratista de la organización.
3	**Medio**	Es posible la modificación por Líderes de Proceso.
4	**Alto**	Solo se modifica bajo autorización del Comité de Gerencia.
5	**Muy Alto**	Solo se modifica con autorización de la Alta Dirección.

Fuente: El Autor

Tabla 5. Valoración Disponibilidad (D).

Escala Cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo**	El activo no está disponible por 1 semana y no afecta a la Organización
2	**Bajo**	El activo No está disponible hasta por 3 días y no afecta a la organización
3	**Medio**	El activo No está disponible hasta por 1 día y no afecta a la organización
4	**Alto**	El activo No está disponible hasta por 4 horas.
5	**Muy Alto**	El activo debe estar disponible siempre.

Tabla 5. (Continuación)

Cada activo de información será valorado en términos de Confidencialidad, Integridad y Disponibilidad.

El valor del activo de información está dado por:

Valor Activo = *C* + *I* + *D*

Donde:

C= Confidencialidad, **I** = Integridad, **D**= Disponibilidad

La valoración de los activos de información estará clasificada según la siguiente escala:

Tabla 6. Clasificación del Valor del Activo

Clasificación valor del activo	Rango según valor del activo	
Muy Alto	17	20
Alto	14	16
Medio	11	13
Bajo	7	10
Muy bajo	4	6

Fuente: El Autor

6.2.5 Análisis y Evaluación de Riesgos de Seguridad de la Información

a. Identificación de las amenazas. Las amenazas son de dos tipos de origen: natural o humano, igualmente pueden ser deliberadas o accidentales y pueden afectar a más de un activo generando diferentes impactos.

b. Identificación de las vulnerabilidades. Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo, una vulnerabilidad que no tiene una amenaza, puede no requerir de la implementación de un control, para lo cual es necesario identificarla y monitorear. Pero es necesario dejar claro que un control mal diseñado e implementado puede constituir una vulnerabilidad.

La identificación de las vulnerabilidades se basa las entrevistas con los responsables de los activos de información y serán registradas en la *Matriz de Riesgos*.

c. Identificación de los Riesgos. Los riesgos en seguridad de la información se identificaran mediante el resultado de las pruebas de seguridad, identificación por parte de los empleados quienes tienen claridad y han experimentado la materialización de algunos riesgos en sus procesos. Los riesgos son relacionados

a las vulnerabilidades y amenazas de los activos de información los cuales se deberán listar en la matriz de riesgos.

Los riesgos se clasifican en: Lógico, Físico, Legal y Locativo

d. Selección de la Probabilidad de Ocurrencia. El valor de la probabilidad estará determinado por el responsable del proceso con base a su experiencia, de acuerdo a la estimación del riesgo asociado con la amenaza y vulnerabilidad de los activos de información.

Para los riesgos que no se han materializado en la organización y a los cuales no existe claridad por parte del responsable en el grado de estimación de la materialización, el valor de probabilidad estará sujeto a datos de referencias externas (Información de probabilidad de materialización en otras organizaciones) o finalmente por criterio de experto en riegos.

Luego se deberá consolidar una matriz que describe cada uno de los activos involucrados en el análisis. Con ella se revisa cada uno de los riesgos existentens en seguridad y se relacionaron con los activos de información.

e. Determinar el impacto de los Activos de Información. El impacto está determinado por el máximo valor de la calificación registrada en términos de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) de los activos de información.

f. Valoración del Riesgo Inherente. El marco de referencia utilizado en la evaluación del riesgo para los activos es la norma ISO 27005[18].

Para la valoración y evaluación de los riesgos se tendrán en cuenta las siguientes variables definidas anteriormente:

Valor del activo (VA).

Probabilidad P(A,V).

[18] ICONTEC "estándar Internacional ISO/IEC 27005:2008 Information Technology – Security techniques – Specification for an Information Security Managment System"

Valor Impacto (IMP).

*Donde Valor Riesgo = P(a,v) * Valor Impacto * Valor Activo* (2)

Con la anterior formula se obtendrá el valor del riesgo asociado a cada activo de información en términos de su confidencialidad, integridad, disponibilidad, valor económico, la probabilidad de ocurrencia y el impacto asociado al SGSI.

g. Identificación de controles existentes. Se realizará la identificación de controles documentados, implementados y monitoreados por la organización para la gestión del riesgo. Después será necesario verificar el valor del riesgo residual y determinar si es posible aplicar un plan de Tratamiento de Riesgo. Las acciones definidas para el tratamiento de los riesgos

Evitar: la acción que da origen al riesgo particular. Se evalúa y determina la viabilidad de si se puede o no evitar el riesgo en la compañía mediante el impacto que esto generaría.

Transferir: a organizaciones como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo. Para seleccionar una tercerización de un riesgo se evalúa el costo beneficio es decir sea la opción adecuada y económica en su implementación, adicionalmente se debe verificar que el riesgo residual este en los niveles de aceptación de la compañía tras su implementación.

Mitigar: mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda revaluar como aceptable.

Aceptar: con el conocimiento y objetividad, siempre que cumplan con la política de seguridad previamente establecida por la organización. Es la última decisión que se toma en el tratamiento de riesgos y aplica cuando no existe opción alternativa bien sea por costo económicos o por tiempos de implementación.

Figura 2. Gestión de Riesgos

Fuente: www.iso27000.es/sgsi_implantar.html#seccion1

El Análisis de Riesgos. Es uno de los procesos más relevantes y prioritarios para realizar la gestión de los riesgos y en la gestión de la seguridad de la información de una organización debe abordarse de primeras ya que es fundamental para realizar la gestión de los riesgos, es decir para tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos, así como determinar las necesidades de seguridad, las posibles vulnerabilidades y las amenazas a las que se encuentran expuestas.

Actualmente, existen varias metodologías para realizar el análisis de riegos, las cuales están fundamentadas tres variables esenciales (activos, las amenazas y las vulnerabilidades) que se identifican y se relacionan entre sí para determinar los riesgos; entre las metodologías más utilizadas se tienen ***Magerit, Octave y Mehari***, todas cumplen con el mismo objetivo, su diferencia se determina en la forma de presentación de los resultados.

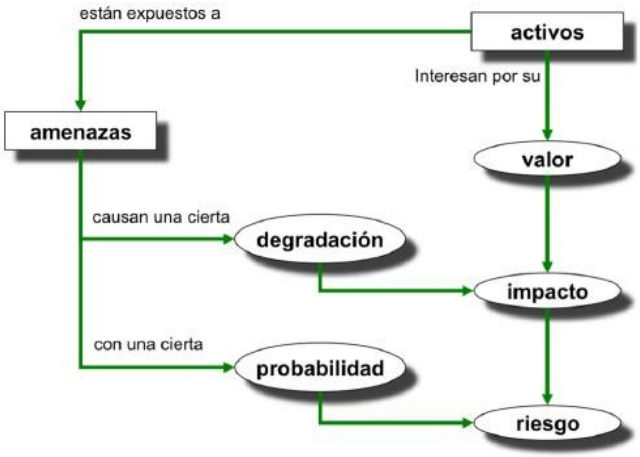
Figura 3. Elementos del Análisis de Riesgos

Fuente: datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/31_leccin_11_proceso_de_identificacin_del_riesgo.html

6.2.6 Metodología de análisis de riesgos MAGERIT. Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información.

- Determinar los activos importantes para la Organización, determinar su interrelación y el valor, en el sentido de qué costo supondría su degradación.
- Determinar las amenazas a que están expuestos estos activos
- Determinar si existe salvaguardas dispuestas y su eficacia frente al riesgo.
- Estimar el impacto, generado en caso de materializarse una amenaza.
- Estimar el riesgo o expectativa de materialización de la amenaza.

Figura 4. Elementos del análisis de riesgos potenciales



Fuente: Magerit v3 libro1 método

El análisis de los riesgos se realiza mediante la ejecución de siguientes tareas:

Tabla 7. Método de Análisis de Riesgos

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos MAR.11 – Identificación de los activos MAR.12 – Dependencias entre activos MAR.13 – Valoración de los activos MAR.2 – Caracterización de las amenazas

MAR – Método de Análisis de Riesgos
MAR.21 – Identificación de las amenazas MAR.22 – Valoración de las amenazas MAR.3 – Caracterización de las salvaguardas MAR.31 – Identificación de las salvaguardas pertinentes MAR.32 – Valoración de las salvaguardas MAR.4 – Estimación del estado de riesgo MAR.41 – Estimación del impacto MAR.42 – Estimación del riesgo

Fuente: Magerit v3 libro1 método Tabla 7. (Continuación)

MAR.1: Caracterización de los activos

En esta actividad se identifican los activos importantes y como resultado de la misma se genera el informe "modelo de valor". Como subtareas tenemos; la identificación de los activos, identificación de las dependencias entre activos y valoración de los activos

MAR.2: Caracterización de las amenazas

En esta actividad se identifican las principales amenazas sobre el sistema a analizar, arrojando como resultado el informe "mapa de riesgos". Consta de dos subtareas a saber: la Identificación de las amenazas y la valoración de las mismas

MAR.3: Caracterización de las salvaguardas

Se identifica las salvaguardas desplegadas en el sistema a analizar, como resultado de esta actividad se obtiene tres informes: Declaración de aplicabilidad; evaluación de salvaguardas y vulnerabilidades del sistema

Como Sub-tareas dentro de esta actividad se tiene la identificación de las salvaguardas y su valoración.

MAR.4: Estimación del estado de riesgo

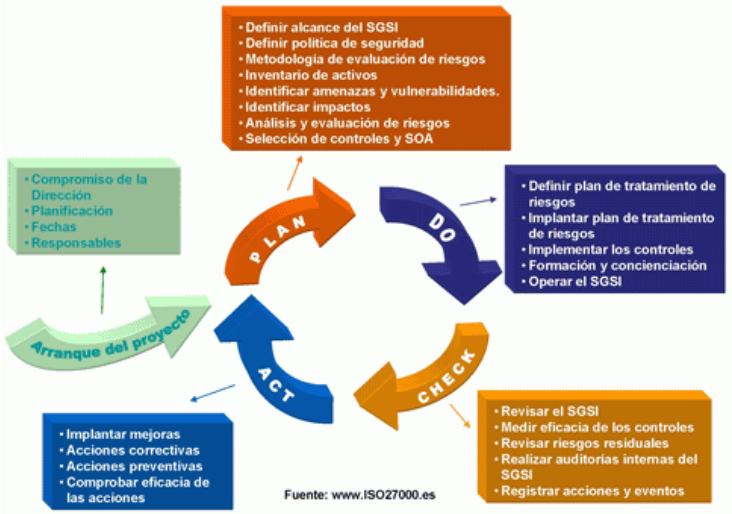
En esta actividad se procesan todos los datos recopilados en la ejecución de las actividades anteriormente relacionadas con el fin de realizar los siguientes informes:

• Estado de riesgo: estimación de impacto y riesgo, resultado de las dos subtareas de esta actividad

• Insuficiencias: Contiene las deficiencias o debilidades de las salvaguardas encontradas en el sistema.

Ciclo Deming (2005). Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basados en la norma ISO 27001:2005, se utiliza el ciclo continuo PDCA - Mejora continua

Figura 5. Ciclo Deming



Fuente: www.iso27000.es/sgsi_implantar.html#seccion1
Plan (planificar): Se establece el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorizar y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI.

6.3 MARCO LEGAL

6.3.1 Principios para el Tratamiento de datos personales[19]: A continuación se listan los principios que en materia de tratamiento de datos personales a reglado el gobierno colombiano a través del Artículo 4° de la Ley Estatutaria 1581 de 2012, la cual fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013.Estos son:

a) **Principio de legalidad**: El Tratamiento de los datos personales es una actividad reglada y debe estar sujeta a las disposiciones legales vigentes aplicables.

b) **Principio de finalidad:** El Tratamiento de datos personales debe obedecer a una finalidad legítima en consonancia con la Constitución y la Ley, por lo tanto se debe informar al titular de los datos personales.

c) **Principio de libertad:** El Tratamiento de datos personales sólo se puede realizar previo consentimiento expreso e informado por parte del titular, por lo tanto estos datos no podrán ser conseguidos o divulgados sin su previa autorización.

d) **Principio de veracidad o calidad:** Esta información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No se pueden tratar datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el Tratamiento de datos se debe garantizar al titular el derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de dato o de información del cual es titular.

f) **Principio de acceso y circulación restringida:** El Tratamiento de datos se sujeta a los límites que se derivan de la naturaleza de los mismos, en consecuencia este tratamiento solamente podrá hacerse por personas autorizadas

[19] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria de 2012. (17 octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. Bogotá D.C.: Alcaldía de Bogotá. 2012. [Consultado el 23 de mayo, 2015]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

por el titular, por tanto no debe estar disponible en internet u otros medios de divulgación, a excepción de la información que es pública.

g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable o Encargado del Tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas requeridas que brinden seguridad a los registros evitando así entre otras ser adulterada, consultada, usada, accesada sin autorización del titular.

h) **Principio de confidencialidad:** Todas las personas que administren, actualicen o intervengan en el Tratamiento de datos están obligadas a garantizar la reserva de la información y están obligados a mantener su confidencialidad y no revelarla a terceros inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

6.4 ANTECEDENTES

"Origen y posicionamiento del Estándar[20]:

ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotecnia) conforman un sistema especializado para los estándares mundiales.

JTC 1 (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto".

a. De los comienzos de la gestión de seguridad de la información hasta la ISO 27001:2005"[21]:

[20] CORLETTI, A. Análisis de ISO-27001:2005. [en línea], (abril 2006). [consultado 06 de mayo de 2015]. Disponible en Internet: www.criptored.upm.es/guiateoria/gt_m292g.htm

[21] ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD-AEC. La gestión de la seguridad en la empresa. En Revista Calidad. [en línea], (Junio 2006). p.12. [Consultado 26 de noviembre, 2014]. Disponible en internet: www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

A inicios de los 90, el Departamento de Comercio e Industria del Reino Unido dio comienzo al desarrollo de la norma británica BS, con el fin entre otros, de proteger y regular la gestión de la seguridad en la empresa. La primera norma (BS 7799:95) fue aprobada oficialmente en 1995 y nace como un código de buenas prácticas para la gestión de seguridad de la información.

Cronológicamente a este primer gran hito en la normalización de la gestión de la seguridad de la información le han precedido las siguientes normas y etapas:

1998, se publica la norma BS 7799-2, en ella se recogen especificaciones para la gestión de la seguridad de la información y por primera vez se "lanzan" requerimientos certificables.

1999, segunda edición, donde se en la que se agrega "e-commence" al alcance de la norma.

2000, Tras una revisión de ambas partes de la norma, en diciembre ISO aprueba la norma ISO 17799 Parte 1 Código de Práctica para los requisitos de gestión de seguridad de la información la cual no era certificable. Esta norma contiene un conjunto completo de controles que conforman las buenas prácticas de seguridad de la información, y que pueden ser aplicadas por toda organización sin importar cuál sea su tamaño.

2002, se realiza la revisión de la parte 2 de la BS (BS 7799-2:2002), ésta si es certificable, con el fin de armonizarla con otras normas de gestión (ISO 9001:2000 e ISO 14001:1996), y con los principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

2002, la norma es publicada norma UNE (UNE-EN ISO/IEC 17799/ 1:2002, prácticamente sin modificación y se establece exclusivamente en España otra norma, la "UNE 71502".

2005, se publica el estándar ISO/IEC 27001, esta es la principal norma de la serie y en ella se encuentra los requisitos del Sistema de Gestión de Seguridad de la

Información. Es originada por la ya anulada BS 7799-2:2002 y es la norma con la cual se certifican como auditores externos los SGSIs de las organizaciones.[22].

2005, Se revisa y actualiza la ISO 17799 la cual posteriormente se renombró como 2702: 2005.

2006, BSI publica la BS 7799-3:2006, la cual se centra en la gestión del riesgo de los SGSI

2013, se publica la revisión aprobada de la ISO/IEC 27001:2013 donde se establecen cambios en el contenido y la estructura de la norma. En la misma fecha también es publicada la revisión aprobada de la ISO/IEC 2700:2013

Figura 6. Estructura de la ISO 27001:2005 /2013

Fuente:es.slideshare.net/fabiandescalzo/270012013-seguridad-orientada-al-negocio

b. Familia ISO-2700x. A continuación se hace un acopio del conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta al momento de implementar un SGSI:[23]

[22] PORTAL ISO 27001 EN ESPAÑOL. Origen serie 27K. [en línea]. [Consultado 28 de noviembre, 2014]. Disponible en internet: www.iso27000.es/iso27000.html

[23] PORTAL ISO 27001 EN ESPAÑOL. Serie 27000.Evolución [en línea]. [Consultado 29 de noviembre, 2014]. Disponible en internet: www.iso27000.es/iso27000.html

ISO/IEC 27000 Entrega información introductoria a la seguridad de la información y la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI.

ISO/IEC 27001 ISMS. Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27.001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar; Hacer; Verificar y Actuar (PHVA). Su filosofía principal se basa en la gestión de riesgos

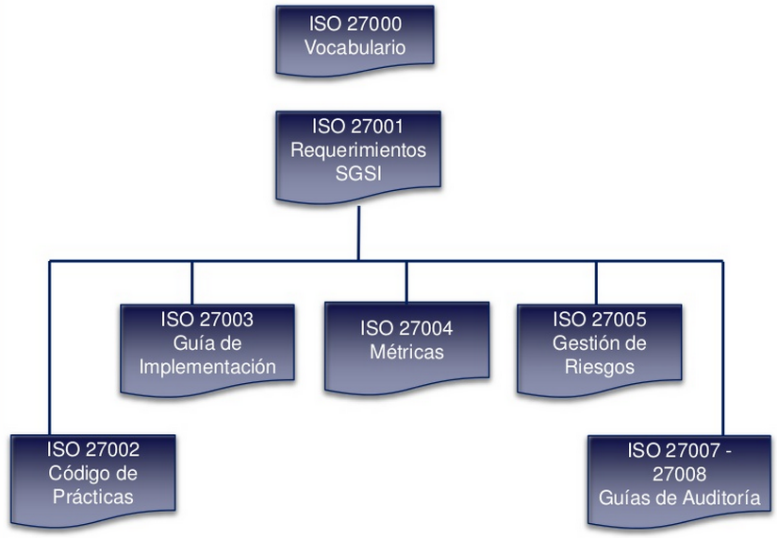
ISO/IEC 27002 Es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. La última edición de 2013 ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles

ISO/IEC 27003 ISMS Tiene su origen en el anexo B de la norma BS 7799-2.

ISO/IEC 27004 guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005 Publicada en segunda edición el 1 de Junio de 2011. Proporciona directrices para la gestión del riesgo en la seguridad de la información y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Figura 7. Familia ISO 27000 SI



Fuente: es.slideshare .net/Joha_pazmino/presentacin-iso-27001

7. DISEÑO METODOLÓGICO PRELIMINAR

El proyecto será ejecutado tomando como referencia una metodología de trabajo que permita en un futuro la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), bajo el estándar ISO 27001.

7.1 FASE 1. DIAGNOSTICO DE LA SITUACION ACTUAL

En esta etapa se desarrollarán las siguientes actividades:

7.1.1 Levantamiento de información e identificación de los activos de información que componen el proceso alcance del sistema SGSI, a través de la aplicación de metodologías que contemplen entrevistas y formatos.

7.1.2 Revisión y Análisis de las políticas y procedimientos de Seguridad existentes en la empresa.

7.1.3 Identificación de Riesgos. La Metodología utilizada estará soportada en el estándar de administración de riesgos ISO 27005 para Gestión de Riesgos en Seguridad de la Información.

7.1.4 Pruebas de Ingeniería Social

7.1.5 Generación de Matriz de Riesgos identificados

7.1.6 Analizar y evaluar los riesgos

7.2 FASE 2. DEFINICIÓN DE POLÍTICAS, NORMAS, PROCEDIMIENTOS Y ACCIONES DE SEGURIDAD INFORMÁTICA A IMPLEMENTAR (SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA).

Con base en el análisis y diagnóstico realizado, se deberá:

7.2.1 Definir y documentar las políticas de seguridad que deban implementarse.

7.2.2 Identificar y evaluar las distintas opciones de tratamiento de los riesgos

7.2.3 Seleccionar los objetivos de control y los controles del Anexo A de la Norma ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

7.2.4 Definir estrategias de contingencia y recuperación para los sistemas informáticos.

7.2.5 Recomendaciones para la implementación del SGSI.

7.3 RECURSOS DISPONIBLES

7.3.1 Talento Humano. El desarrollo del proyecto estará a cargo de la estudiante de la especialización de seguridad Informática de la UNAD Sandra Yomay Suárez Padilla y el aporte de dos ingenieros de la empresa de seguros Suárez Padilla & Cía Ltda, responsables de la supervisión del proyecto.

7.3.2 Materiales y Equipos. Para el Análisis y Gestión de Riesgos, se trabajará Magerit herramienta de software libre y un equipo portátil marca Lenovo L430 Core i5 de propiedad de la estudiante de la especialización de seguridad Informática de la UNAD Sandra Yomay Suárez Padilla.

7.3.3 Recursos Financieros. El resultado de este trabajo es benéfico tanto para la empresa Suárez Padilla & Cía Ltda y para la estudiante de la especialización de seguridad Informática de la UNAD Sandra Yomay Suárez Padilla, los recursos financieros serán distribuidos así:

Tabla 8. Presupuesto del proyecto

Ítem	Descripción	Cantidad	Unitario	Proyectado Mes 1	Proyectado Mes 2	Total
Ingresos		**0**	**$ 15.000.000**	**$ -**	**$ -**	**$ 15.000.000**
Valor del proyecto	Valor del proyecto		$ 15.000.000			
Gastos de Personal				**$ 1.500.000**	**$1.500.000**	**$ 3.000.000**
Sueldo	Ingeniero con estudios en especialización - Medio tiempo	1	$ 1.500.000	$ 1.500.000	$ 1.500.000	$ 3.000.000
Gastos Generales				**$ 860.000**	**$ 860.000**	**$ 1.880.000**
Transporte	Transporte			$ 80.000	$ 80.000	$ 160.000
Servicios Técnicos				$ 650.000	$ 650.000	$ 1.300.000
Materiales y suministros	Papelería, fotocopias, argollados, impresiones, etc.			$ 130.000	$ 130.000	$ 260.000
Servicios públicos	Luz, teléfono e internet			$ 80.000	$ 80.000	$ 160.000
Inversión				**$ 2.400.000**	**$ -**	**$ 2.400.000**
Equipo Portátil	Estación de trabajo	1	$ 2.400.000	$ 2.400.000	$ -	$ 2.400.000
GRAN TOTAL						**$ 7.280.000**

Fuente: El autor

8. RESULTADOS

8.1 FASE 1 ANALISIS Y DIAGNÓSTICO DE LA SITUACION ACTUAL

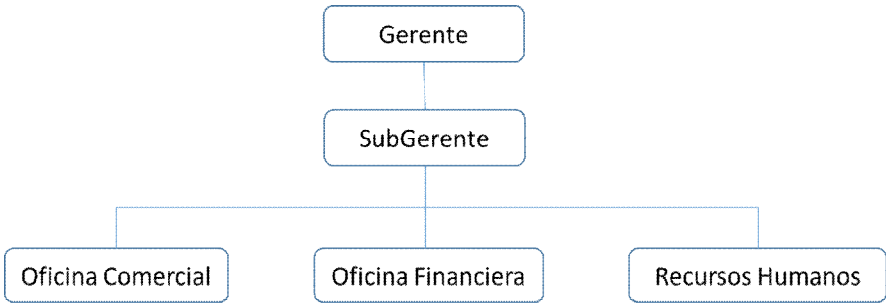
8.1.1 Descripción de la Empresa. **Agencia de Seguros Suárez Padilla & Cía. Ltda**. Agencia asesora de seguros con 20 años de experiencia, ubicada en la CA 68 B 78 24 INT 6 barrio Metrópolis de la Ciudad de Bogotá D.C, dedicada a la comercialización de pólizas de salud, seguros de vida, pensión, medicina prepagada y seguros generales.

a. Misión Suárez Padilla & Cía. Ltda. Somos una empresa dedicada a la asesoría y comercialización de seguros, con un equipo trabajo honesto y comprometido que pone a disposición de sus clientes, servicios de alta calidad, proporcionándoles soluciones integrales, de ahorro y protección tanto personal como empresarial a la medida de sus necesidades.

b. Visión Suárez Padilla & Cía. Ltda. En el 2.018 ser la compañía aseguradora preferida del Sector Solidario, las familias y las empresas, siendo reconocida por ser líderes en asesoría y comercialización de seguros; altamente reconocidos por el servicio al cliente, la honestidad y la experiencia, brindándoles seguridad a través de un amplio portafolio de servicios**.**

La Organización

Figura 8. Diagrama Organizacional



Fuente: El autor

Funciones por dependencia

Gerente: Es quien dirige, controla y supervisa las actividades de la empresa.

Subgerente

- Orientar la gestión del equipo comercial
- Administrar los recursos para controlar la generación de ventas con el fin de cumplir con los objetivos establecidos por la Gerencia
- Controlar el adecuado manejo de los activos de la empresa

Oficina Comercial: Está conformada por cinco (5) agentes comerciales encargados de visitar a los clientes ya establecidos y clientes potenciales, con el fin de dar a conocer el portafolio de servicios que presta la empresa.

Oficina Financiera: Está conformada por el contador y un auxiliar contable. Esta oficina es la encargada de mantener al día la información contable Financiera de la organización

Oficina de Recursos Humanos: Conformada por un jefe de personal y dos profesionales de nómina

- Se encarga de suplir cualquier puesto si es requerido.
- Gestión y pago de nómina de los empleados
- Velar por el bienestar de los empleados
- Velar por el cumplimiento de las normas fijadas por la empresa
- Realizar las labores administrativas

Adicionalmente la empresa cuenta con una secretaria, un mensajero y una persona de servicios generales.

Fuentes de Información

Las personas a entrevistar durante el desarrollo de este proyecto serán:

- Cristian Andrés Riaño: Subgerente
- María Victoria Martínez: Contadora
- Jackelinne Manosalva Cruz: Jefe Recursos Humanos
- Juan Carlos Rojas Castiblanco: Profesional de Nómina
- Pedro Pablo González Santos: Agente de seguros
- Clemencia Martínez Jurado: Auxiliar contable

Con el fin de identificar el estado actual de la organización en cuanto a la Seguridad de la Información se realizaron entrevistas con los responsables de los procesos, solicitando información y verificación de la documentación existente en cuanto a seguridad de la información.

8.1.2 Análisis de Riesgos

8.1.2.1 Activos

Tabla 9 Identificación de los Procesos

Procesos	Descripción	Frecuencia (Diario/Semanal Mensual)	Responsable
Soporte telefónico a solicitud o trámite	Los agentes de seguros tienen a su cargo un determinado número de clientes a los cuales dan soporte a cualquier solicitud o trámite con respecto a los seguros que hayan adquirido.	Diario	Pedro Pablo González Santos

Procesos	Descripción	Frecuencia (Diario/Semanal Mensual)	Responsable
Atención personalizada Clientes	Visita a clientes potenciales con el fin de mostrarles e informarles sobre el portafolio de servicios	Diario	Pedro Pablo González Santos
Legalización de pólizas	El agente recibe los documentos requeridos por la aseguradora. realiza el trámite de legalización de la póliza ante la aseguradora, haciéndole llegar el respectivo título al cliente	Según necesidad	Pedro Pablo González Santos
Control y verificación de pagos	Control y verificación de los pagos efectuados por los clientes con respecto a sus obligaciones en los seguros adquiridos; Control y verificación de los pagos de las primas giradas a la empresa por parte de las aseguradoras.	Semanal	María Victoria Martínez
Gestión de Nómina	Gestión de pago mensual de nómina para los empleados	Quincenal	Juan Carlos Rojas Castiblanco
Gestión de Talento Humano	Gestión de Contratos de trabajo, permisos, incapacidades, capacitación	Diaria	Jackelinne Manosalva Cruz

Fuente: El autor **Tabla 9** (Continuación)

Tabla 10 Sistemas que soportan el proceso

Nombre del Sistema	Descripción	Criticidad (*)	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación

Nombre del Sistema	Descripción	Criticidad (*)	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación
B.D Clientes	Aplicación en red desarrollada en Access para el manejo de la información de los clientes (registro de información personal y pólizas de seguros adquiridas por intermedio de la empresa	2	Servidor	7
Software "Humano"	Desarrollo a la medida hecho por Soporte Lógico, para la gestión del talento humano y liquidación de nómina, permite registrar la información de hoja de vida de los empleados.	3	Servidor	4
Interpaciolo	Software Contable Administrativo y Financiero desarrollado por Softstation	2	Servidor	2

Fuente: El autor

Tabla 11 Recursos de Hardware de los procesos

Tipo de Hardware	Detalles del Modelo/Configuración	Distribuidor	Criticidad (*)	Localización
Servidor de Aplicaciones	PowerEdge R410, Windows Server 2008 R2 Standard 64-bit	DELL	3	Sala de equipos
PC's	APU AMD Dual-Core E1-2500 con gráficos Radeon HD 8240 (1,4 GHz, 1 MB de caché), Memoria: DDR3 de 4 GB, Disco Duro SATA de 500 GB, 7200 rpm	HP (Compaq)	3	Oficinas

Fuente: El autor **Tabla 11** (Continuación)

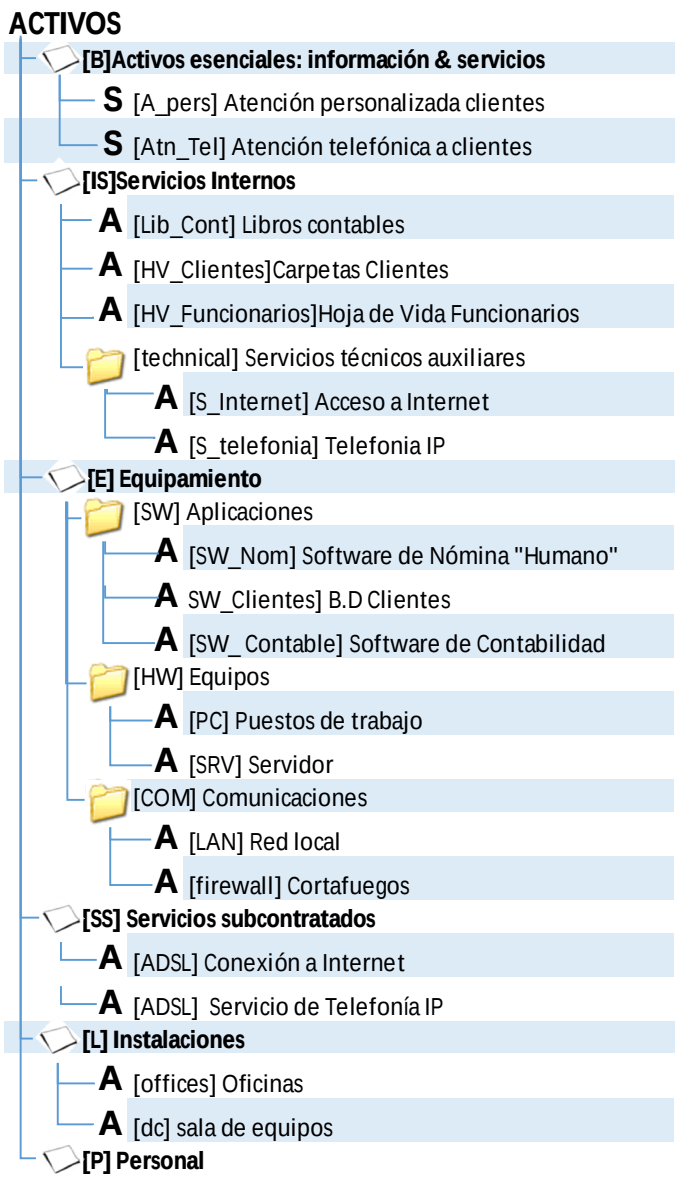
Tabla 12 Otros activos

Descripción	Tipo	Criticidad (*)	Localización
Switch 5500G-EI 24 Puertos	Equipos Activos	2	Sala de equipos
FIREWALL CISCO ASA 5520	Equipos Activos		Sala de equipos
Aire Acondicionado Marca YORK 9000 BTU		3	Sala de equipos
Línea RDSI de comunicaciones	Comunicaciones	2	Sede Principal

Fuente: El autor

Se hace uso de la herramienta PILAR aunque no llegó la licencia solicitada se realizó un trabajo largo y dispendioso dentro de los cuales se incluye la identificación de los activos:

Figura 9 Identificación de activos - Metodología Margerit



Fuente: El autor

a. Valoración de Activos: De acuerdo con los preceptos estipulados en la norma ISO 27001:2013 los activos de información deben ser valorados con base a la disponibilidad, confidencialidad e integridad. La valoración que cada activo reciba se relacionará con base a las entrevistas o a información suministrada por el responsable del activo.

De igual manera se tendrá en cuenta el valor económico del activo de información el cual corresponde al costo inicial que la entidad suministro para obtener el activo de información.

La valoración de la integridad, disponibilidad, confidencialidad y valor económico se realizará de uno a cinco donde 1 es la calificación más baja y cinco es la calificación más alta como se puede ver en la tabla 13, en la cual también se relaciona al valor cuantitativo una calificación cualitativa para cada activo de información.

Tabla 13 Calificación y Clasificación

Calificación: Integridad, Confidencialidad, Disponibilidad	Clasificación
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

El valor del activo corresponde a la suma de la confidencialidad, disponibilidad, integridad y valor económico, dónde 3 es la calificación más baja y 20 la calificación más alta. De igual forma la clasificación del activo corresponde a la caracterización cualitativa del valor del activo antes mencionado, según los rangos definidos en la tabla 6.

Figura 10 Valoración de activos –

ACTIVOS	[D]	[I]	[C]	[VE]	[VT_ACTIVO]
[B]Activos esenciales: información & servicios					
S [A_pers] Atención personalizada clientes	[4]		[4]	[3]	[11]
S [Atn_Tel] Atención telefónica a clientes	[3]		[4]	[3]	[10]
[IS]Servicios Internos					
A [Lib_Cont] Libros contables	[1]	[3]	[4]	[5]	[13]
A [HV_Clientes]Carpetas Clientes	[2]	[5]	[5]	[1]	[13]
A [HV_Funcionarios]Hoja de Vida Funcionarios	[1]	[4]	[2]	[2]	[9]
[technical] Servicios técnicos auxiliares					
A [S_Internet] Acceso a Internet	[2]			[2]	[4]
A [S_telefonia] Telefonia IP	[3]			[3]	[6]
[E] Equipamiento					
[SW] Aplicaciones					
A [SW_Nom] Software de Nómina "Humano"	[3]	[5]	[4]	[5]	[17]
A SW_Clientes] B.D Clientes	[3]	[5]	[5]	[3]	[16]
A [SW_Contable] Software de Contabilidad	[3]	[5]	[5]	[4]	[17]
[HW] Equipos					
A [PC] Puestos de trabajo	[1]			[2]	[3]
A [SRV] Servidor	[5]	[4]	[4]	[4]	[17]
[COM] Comunicaciones					
A [LAN] Red local	[4]			[5]	[9]
A [firewall] Cortafuegos	[2]			[4]	[6]
[SS] Servicios subcontratados					
A [ADSL] Conexión a Internet	[2]			[2]	[4]
A [ADSL] Servicio de Telefonía IP	[2]			[2]	[4]
[L] Instalaciones					
A [offices] Oficinas	[2]			[3]	[5]
A [dc] sala de equipos	[4]	[5]		[5]	[14]
[P] Personal	[4]	[5]	[5]	[5]	[19]

b. Identificación de Amenazas: Las amenazas son los eventos inesperados con potencial para causar daños. La siguiente es la lista de amenazas aplicables al contexto de Suárez Padilla & Cía. Ltda encontradas en el análisis y acordados con la empresa.

(E) Fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema/ de la seguridad
[E.4] Errores de configuración
[E.8] Difusión de software dañino
[E.15]Alteración de la información
[E.18] Destrucción de la información

[E.19] Fugas de Información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento/ actualización de programas (software)
[E.23] Errores de mantenimiento/ actualización de programas (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos

(A) ataques deliberados o intencionados
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de Identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de la información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.28] Indisponibilidad del personal
[A.26] Ataque destructivo

(I) De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación medio ambiental
[I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información

(N) Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

c. Identificación de Vulnerabilidades. En el marco de las posibles amenazas que pueden llegar a materializarse, las siguientes son las vulnerabilidades referenciadas por los entrevistados e identificadas durante las visitas a sitio y que

pueden ser explotadas para convertir una amenaza en un riesgo real causando daños graves en la empresa:

- Existencia de materiales inflamables como papel o cajas
- Cableado inapropiado
- Mantenimiento inapropiado del servicio técnico
- Deficiencia en la capacitación y concienciación en temas de seguridad de la información
- Ausencia de política de seguridad
- Derechos de acceso incorrectos
- Ausencia de un sistema de extinción automática de fuegos/humos
- Ausencia de control de cambios de configuración eficiente y efectiva
- Descarga incontrolada y uso de software de Internet
- Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales
- Protección física de equipos inadecuada
- Ausencia de un Plan de recuperación de incidentes
- No se exige el uso de contraseñas seguras para los accesos a los sistemas de información
- No se han implementado políticas o procedimientos para la asignación, modificación, eliminación y revisión de privilegios en los Sistemas de Información.

- No se cuenta con bloqueos automáticos o políticas de bloqueo manual para la pantalla

- No se cuenta con registros de los privilegios asignados a los Empleados y contratistas

- No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad

- No se han implementado políticas para evitar el consumo de líquidos y alimentos cerca a los equipos

- No se cuenta con plan de continuidad en la Empresa

- No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad

- No se cuenta con actualización del software, aplicaciones.

d. Evaluación del Impacto. Las entrevistas también permitieron establecer los siguientes impactos tipificados según la norma ISO 27005:

Tabla 14 Evaluación del Impacto

Amenaza	**Impacto**
Fallos no intencionados	□ Alteración/pérdida o Fuga de Información □ Daño/ Pérdida de activos o indisponibilidad colateral de otros servicios □ Costos excesivos □ Información para toma de decisiones errada o inoportuna □ Interrupción del servicio o del negocio □ Pérdida de credibilidad, competitividad o imagen de la empresa □ Pérdida de productividad de los empleados

Amenaza	Impacto
Ataques deliberados o intencionados	Alteración/pérdida o Fuga de Información Daño/ Pérdida de activos o indisponibilidad colateral de otros servicios Fraude/Robo o malversación de fondos Interrupción del servicio o del negocio
De origen industrial	Alteración/pérdida o Fuga de Información Daño/ Pérdida de activos o indisponibilidad colateral de otros servicios Costos excesivos Interrupción del servicio o del negocio Ingresos Deficientes Pérdida de productividad de los empleados
Desastres naturales	Interrupción del servicio o del negocio Pérdida de credibilidad, competitividad o imagen de la empresa

Fuente: El autor Tabla 14. (Continuación)

e. Evaluación del Riesgo

Tabla 15 Evaluación del Riesgo

No	Riesgo	Probabilidad			Impacto			Tratamiento
		A	M	B	L	M	C	
Software								
R1	Incorrecta implementación de políticas de Firewalls		X				X	Mitigar
R2	Instalación de software no licenciado y autorizado		X			X		Mitigar
R3	Recursos Compartidos por defecto	X				X		Mitigar
R4	Error en la aplicación de las Políticas de seguridad del Sistema.		X			X		Mitigar
R5	Falencias en monitoreo y auditoria de ingresos operaciones en los sistemas de información	X					X	Mitigar

No	Riesgo	Probabilidad			Impacto			Tratamiento
		A	M	B	L	M	C	
R6	Falta de actualización del Software		X		X			Mitigar
R7	Aplicaciones cliente desactualizadas	X				X		Mitigar
R8	Instalación de software con las opciones por defecto		X			X		Mitigar
R9	Sistemas de información que no controlan el desbordamiento de buffer		X			X		Mitigar
R10	Parches de seguridad desactualizados.	X				X		Mitigar
Datos								
R11	Falta de respaldo en copias de seguridad			X			X	Mitigar
R12	Uso de dispositivos de almacenamientos externos para el transporte de información	X					X	Mitigar
Hardware								
R13	Falla de los equipos por falta de mantenimiento		X				X	Eliminar
R14	Falta de control de altibajos de energía en la conexiones eléctricas de los equipos de cómputo.			X		X		Eliminar
R15	Mal sistema de ventilación		X			X		Eliminar
Redes y Comunicaciones								
R16	Acceso de personal no autorizado, al cuarto de comunicaciones			X			X	Mitigar
R17	Deficiencia del cableado estructurado			X		X		Eliminar
R18	Acceso al FTP a través de acceso anónimo			X			X	Eliminar
R19	Puertos Abiertos	X				X		Eliminar
R20	Incorrecta configuración de los equipos de red		X				X	Eliminar
R21	Transporte de información por conexiones no seguras	X				X		Mitigar

No	Riesgo	Probabilidad			Impacto			Tratamiento
		A	M	B	L	M	C	
Personal								
R22	Falta de capacitación y concienciación	X				X		Eliminar
R23	Continua rotación del personal			X			X	Mitigar

TABLA 15 Continuación

IMPACTO / PROBABILIDAD	LEVE (L)	MODERADO (M)	CATASTROFICO (C)
ALTO (A)		**R3,R7,R10, R19,R21,R22**	**R5,R12**
MEDIO (M)	**R6**	**R2,R4,R8,R9, R15**	**R1,R13,R20**
BAJO (B)		**R14,R17**	**R11,R16, R18,R23**

8.1.3 Pruebas de Ingeniería Social

8.1.3.1 Suplantación Mesa de ayuda: A continuación se hace referencia a las pruebas de ingeniería social mediante llamadas telefónicas realizadas a los empleados y contratistas de Suárez Padilla & Cía. Ltda, donde se solicitó información de datos de acceso entre otras, las cuales buscaban inducirlos al error y así obtener información confidencial o sensible, así como a validar el nivel de conocimiento de los empleados en cuanto a la Seguridad de la Información.

Se realiza una suplantación a la mesa de ayuda de la empresa Seguros Bolívar, entidad con la que los empleados de Suárez Padilla & Cía Ltda tienen ingreso a su plataforma web. Se aplicaron técnicas de engaño para hacer creer al usuario que se estaba realizando una llamada telefónica del grupo de soporte de dicha entidad.

En esta prueba se siguió un guion el cual fue validado y aprobado por el subgerente de la compañía. El guion utilizado en esta prueba fue:

Tabla 16 Guion llamada telefónica

Guion:

Buenas tardes señor(a)
Habla Kelly, lo llamamos de la Mesa de Ayuda de Soporte Técnico de Seguros Bolívar por un caso reportado por usted

Respuestas del usuario:
o No he puesto el caso si
o No recuerdo ningún caso
o Me esa confundiendo

Si señor(a) es el caso número 18143 y aparece reportado que no puede acceder a nuestra plataforma vía web.

Respuesta del usuario:
o Yo no tengo ningún caso

Para total claridad y poder cerrar nuestro caso le quiero pedir su amable colaboración y validar el ingreso.
¿Ingreso sin contratiempo?
Respuesta del usuario

- Si pude entrar sin ningún problema
- Ya estoy dentro del portal

Perfecto muchas gracias. Vamos a probar ahora el acceso desde mi sistema para validar que todo está bien, por favor me ayuda con los datos para yo validar el ingreso desde aquí.

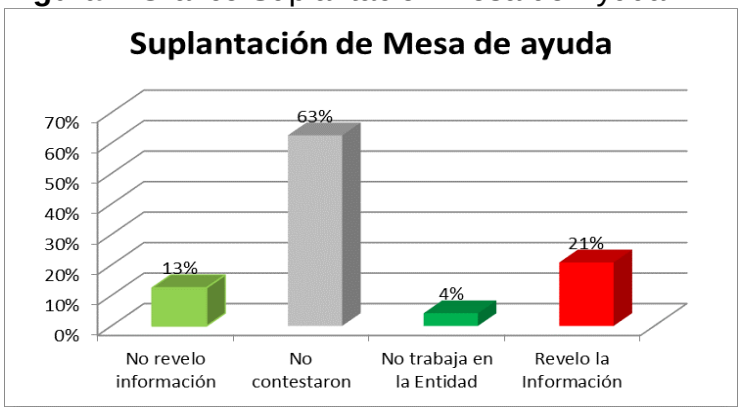
Respuesta del usuario

- Mis datos de ingreso son:

Muchas gracias por su colaboración, el caso ha sido cerrado correctamente, recuerde que habló con Kelly de la Mesa de Ayuda de Soporte Técnico de Seguros Bolívar.

En esta prueba los resultados se vieron afectados debido a que de las llamadas realizadas un gran porcentaje no contesto el teléfono al momento de la prueba.

Figura 4 Gráfico Suplantación Mesa de Ayuda

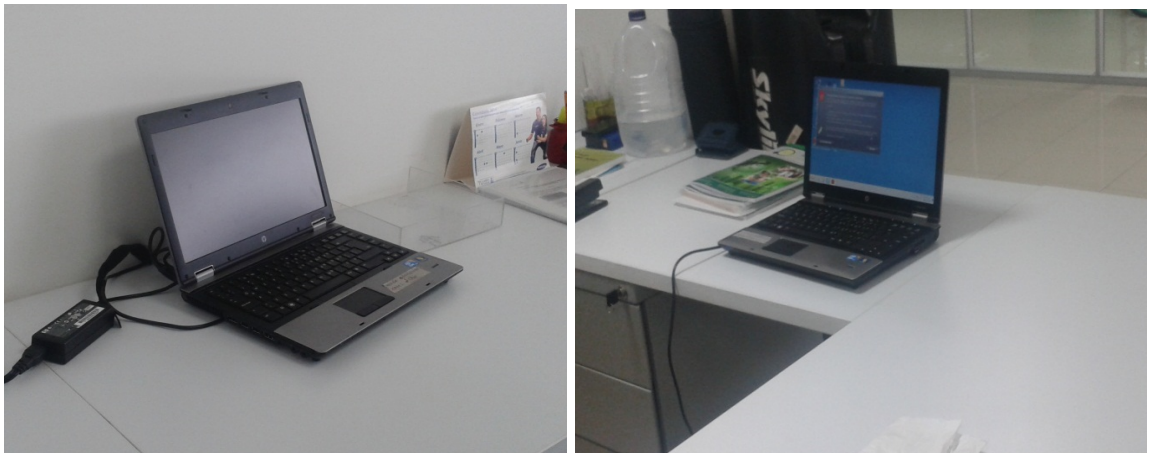


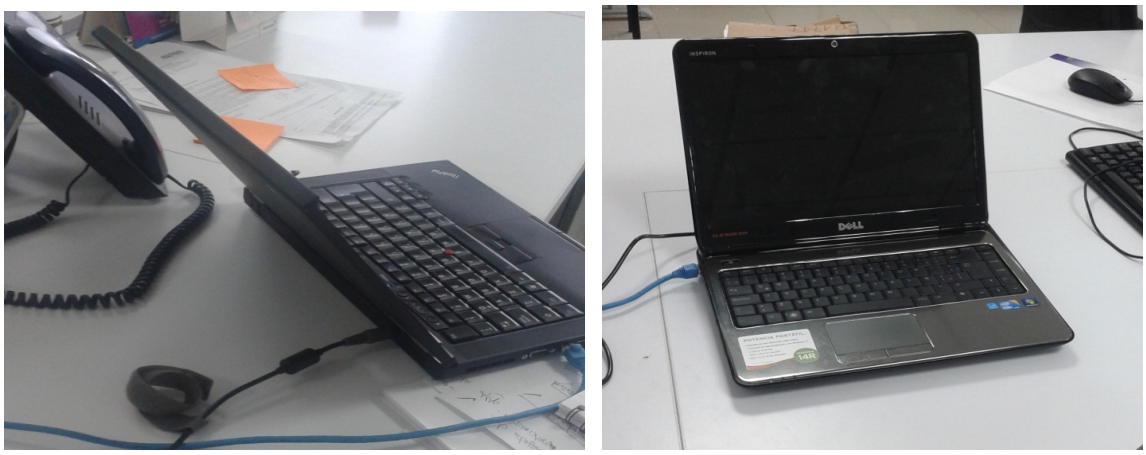
Fuente: El autor

En total 5 usuarios brindaron la información solicitada mediante la llamada. Se pudo evidenciar que los datos eran correctos cuando se ingresaron al sistema de información.

8.1.3.2 Equipos portátiles sin asegurar: Se realizaron visitas a diferentes áreas de la organización para evidenciar posibles brechas de seguridad en temas físicos, hallándose equipos portátiles sin seguridad los cuales podrían en algún momento ser extraídos de la organización.

Figura 5 Portátiles sin asegurar





Fuente: El autor

8.1.3.3 Equipos desatendidos: En esta prueba se evidencia la falta de política o ausencia de la verificación de la implementación en bloqueo manual y/o automático del sistema operativo. Durante las visitas se evidenciaron equipos sin bloqueo de pantalla en ausencia del responsable.

Figura 6 Equipos desatendidos

Fuente: El autor

Con las anteriores pruebas se pudo evidenciar que aunque existen controles de seguridad física como son el personal de vigilancia, es posible acceder a

información sensible, equipos de cómputo que se encuentran desatendidos o sustraer portátiles, generando riesgos de pérdida y fuga de información, por tanto queda en evidencia la importancia de realizar capacitaciones y sensibilizaciones a todos los empleados de Suárez Padilla & Cía. Ltda, en seguridad de la Información con el fin de mitigar riesgos de ataques de tipo ingeniería social.

8.1.4 Hallazgos Seguridad De La Información En Suarez Padilla & Cia & Ltda. Se utilizaron técnicas para conocer el estado actual de la organización en materia de seguridad de la información con el fin de establecer los tiempos de diseño del SGSI según la norma ISO/ IEC 27001:2013. Las herramientas y técnicas utilizadas fueron:

- Diseño de lista de requisitos de la norma ISO/ IEC 27001:2013.

- Realización de entrevistas sobre seguridad de la información a los responsables de los procesos del alcance del proyecto.

- Visitas para identificación de controles de seguridad física en la organización.

Se realizaron las entrevistas con los responsables de los procesos, logrando identificar un panorama del estado de la organización en cuanto a Seguridad de la Información de cara al cumplimiento de la norma ISO/IEC 27001:2013.

8.1.4.1 Cumplimiento Respecto a la Norma ISO/IEC 27001:2013. De acuerdo con los datos aportados por los entrevistados, en la actualidad la organización Suárez Padilla & Cía Ltda no cuenta con un SGSI, el compromiso de la seguridad de la información está en manos de todos sin existir personal idóneo que realice las actividades propias a este respecto.

Concluidas las entrevistas se pudo observar que existen directivas administrativas que cubren algunos aspectos de la seguridad de la información, sin embargo es importante que la organización adopte mayor cantidad de prácticas que permitan gestionar la seguridad de la información y así establecer mayor cantidad de responsabilidades.

Tabla 17 Cumplimiento Norma ISO/IEC 27001:2013

SUÁREZ PADILLA & CÍA LTDA- NORMA ISO/IEC 27001:2013		
Numeral	**Requisito Normativo**	**Observación**
4. Contexto de la Organización		
4.1	Comprender la organización y su contexto	El entendimiento de modelo de negocio en la organización es vital para el logro de los resultados del SGSI en la organización, es por ello que se ha iniciado con esta primera fase del SGSI.
4.2	Comprender las necesidades y expectativas de las partes interesadas	
4.3	Alcance del SGSI Documentado	De acuerdo con los requisitos para definir el alcance del SGSI, debe estar expresado en el ámbito de asuntos internos y externos, necesidades de las partes interesadas e interfaces y dependencias entre las actividades realizadas por la organización y organizaciones terceras.
4.3	Alcance del SGSI Aprobado	
5 Liderazgo		
5.1	Liderazgo y compromiso	Se debe tener un liderazgo por parte de la alta dirección de la organización en cuanto a definir los objetivos del SGSI, proporcionar los recursos necesarios para la implantación y asegurar que se logren lo resultados esperados del SGSI.
5.2	Política General del SGSI Documentada	La política de seguridad, debe establecer directrices de gestión en cuanto al propósito de la organización, objetivos de seguridad, garantizar una mejora continua entre otros requisitos, los cuales no se evidencian en la organización por cuanto no existe un documento sobre políticas de seguridad de la información. Se requiere definirlas, documentarlas e implementarlas, procurando el compromiso de la Alta dirección.
5.2	Política General del SGSI Aprobada	
5.2	Política General del SGSI Difundida	
5.3	Roles organizacionales, responsabilidades y autoridades	Se deben establecer roles y responsabilidades de seguridad de la información a los empleados, contratistas y terceros que hagan parte del funcionamiento del SGSI.
6 Planificación		
6.1	Acciones para abordar los riesgos y oportunidades	Es necesario identificar los riesgos estimando las posibles pérdidas de confidencialidad, integridad y disponibilidad de acuerdo al alcance establecido del SGSI, los riesgos deben tener responsables y es necesario priorizar mediante un plan de tratamiento a dichos riesgos.

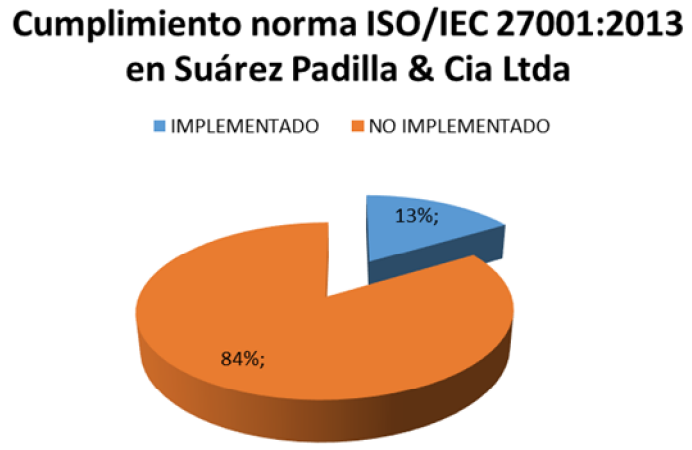
SUÁREZ PADILLA & CÍA LTDA- NORMA ISO/IEC 27001:2013		
Numeral	**Requisito Normativo**	**Observación**
6.2	Objetivos de seguridad de información y planes para alcanzarlos	Se deben establecer objetivos a la política se seguridad de la información que sean medibles que tenga en cuenta los requisitos y necesidades del SGSI.
7 Soporte		
7.1	Recursos	Para la implantación y funcionamiento del SGSI deben existir recursos, lo que se puede evidenciar en el presente proyecto, donde se cuenta con un equipo idóneo para el desarrollo del SGSI a fin de identificar y controlar los riesgos en seguridad de la información.
7.2	Competencia	El equipo de personas que establece, monitorea y realiza mejoras al SGSI debe tener un adecuado nivel de conocimiento o disponer de los recursos para hacer que se logren los objetivos propuestos. Debe existir evidencia de los procesos de capacitación en seguridad de la Información. En la organización no se evidencian capacitaciones en SI.
7.3	Conocimiento	El personal que trabaja dentro del alcance del SGSI debe ser consciente de la importancia del SGSI, se les debe proporcionar capacitaciones de sensibilización y beneficios del sistema. No se evidencia este tipo de sensibilizaciones al interior de la organización.
7.4	Comunicación	Deben existir vías para la comunicación dentro del SGSI, necesidades internas y externas en materia de comunicación donde se establezcan: que se va a comunicar, cuando se realiza, a quien, entre otras. No se evidencia
7.5	Información Documentada	No se cuenta con el procedimiento de control de documentos.
8 Funcionamiento		
8.1	La planificación operativa y control	La organización debe planificar, implementar y controlar los procesos necesarios para garantizar los requisitos e implantar las acciones necesarias para la gestión del riesgo. De acuerdo con lo anterior no se evidencia una planificación operativo y control
8.2	Seguridad de la información de evaluación de riesgos	No se cuenta con una metodología de gestión de riesgos.

Tabla 17 Continuación

SUÁREZ PADILLA & CÍA LTDA- NORMA ISO/IEC 27001:2013		
Numeral	**Requisito Normativo**	**Observación**
8.3	Seguridad de la información tratamiento del riesgo	No se evidencia la documentación e implementación de planes de tratamiento acordes a la evaluación de riegos en la organización.
9. Evaluación del desempeño		
9.1	Seguimiento, medición, análisis y evaluación	No se ha evaluado el rendimiento y la eficacia del Sistema de Gestión de Seguridad de la Información mediante monitoreo, evaluación y análisis, debido a que hasta ahora se inicia con la etapa de diseño del SGSI
9.2	Auditorías internas al SGSI	No se han realizado auditorías internas al Sistema de Gestión de Seguridad de la Información.
9.3	Revisión por la dirección, Generalidades	La revisión por la dirección no se ha realizado debido a que aún no se ha estructurado el SGSI en la organización.
10. Mejora		
10.1	Acciones correctiva del SGSI	No se evidencia acciones correctivas al Sistema de Gestión de Seguridad de la Información.
10.2	Mejora continua al SGSI	No se evidencia mejoras al Sistema de Gestión de Seguridad de la Información.

Tabla 17 Continuación

Figura 7 Cumplimiento de la norma ISO/IEC 27001:2013



Fuente: El autor

8.1.4.2 Controles del anexo A de la Norma ISO/IEC 27001:2013. A continuación se describe la revisión del cumplimiento de los objetivos de control y controles descritos en el anexo A de la norma ISO 27001:2013:

Tabla 18 Cumplimiento Anexo A de la Norma ISO 27001

SUÁREZ PADILLA & CÍA LTDA ANEXO A de la NORMA ISO 27001
Dominios de Control
Dominio 5 Política de Seguridad de la Información
En la revisión documental No se evidencia la política de seguridad de la Información en la organización, la aprobación por parte de la alta dirección ni su divulgación a empleados, contratistas y terceros.
Dominio 6 Organización de la Información
A.6.1 Organización Interna
En la organización cada uno de los empleados tiene asignadas la realización de actividades que hacen parte de sus procesos, los cuales No están documentados en un Manual de Procesos y Procedimientos, en los cuales se establecen los responsables y controles en materia de manejo de la información. Igualmente no se evidencia las asignación de roles y responsabilidades en seguridad de la Información. La organización no cuenta con contactos de grupos de interés en seguridad de la información.
A.6.2 Dispositivos móviles y teletrabajo
Durante las entrevistas realizadas a los empleados y contratistas se menciona que no cuentan con políticas de seguridad de la Información.
Dominio 7 Seguridad en los Recursos Humanos
A.7.1 Antes del empleo
Suárez Padilla & Cía Ltda, tiene documentado el procedimiento de administración de personal, en el cual se realiza el ingreso de los empleados cumpliendo con los requisitos establecidos en la normativa vigente. Uno de los requisitos que debe cumplir el candidato a ingresar a la organización es el no tener antecedentes disciplinarios, ni fiscales, ni penales.
A.7.2 Durante el empleo
Durante la contratación no se evidencian capacitaciones en seguridad de la información a los empleados y contratistas, como lo sugiere el control A.7.2.2
A.7.3 En el momento de terminación o cambio de empleo

SUÁREZ PADILLA & CÍA LTDA ANEXO A de la NORMA ISO 27001
Dominios de Control
Suárez Padilla & Cía Ltda, tiene documentado el procedimiento de administración de personal, el cual está definido lo correspondiente al retiro de los empleados, acorde a la normativa vigente.
Dominio 8 Gestión de los activos

Tabla 18 Continuación

A.8.1 Responsabilidades de los activos
Suárez Padilla & Cía Ltda no cuenta con un inventario de activos de información consolidado donde tenga asociado los responsables.
A.8.2 Clasificación de la Información
En la organización se cuenta con clasificación de la información en cuatro grandes tipos: Interna, Confidencial, Pública y Reservada.
A.8.3 Manejo de medios
Los medios físicos en tránsito, gestión de medios removibles no se encuentran controlados ni existen políticas donde se mencione su manejo.
Dominio 9 Control de accesos
A.9.1 Control de accesos a los requerimientos de negocio
Durante las entrevistas realizadas a los empleados y contratistas se menciona que no cuentan con políticas de seguridad de la Información.
A.9.2 Gestión de acceso de usuarios
La organización cuenta con la creación de usuarios en directorio activo donde se gestiona algunos privilegios en la red y la implementación de proxy para navegación. Los puntos más importantes por trabajar son: Revisión de los Derechos de Acceso de usuarios; Equipo de usuarios Desatendido; Política de puesto de trabajo despejado y Pantalla Limpia; Desconexión automática de sesión; Limitación del tiempo de conexión, entre otras.
A.9.3 Responsabilidades de usuarios
En la organización cada uno de los empleados tiene asignadas la realización de actividades que hacen parte de sus procesos, los cuales No están documentados en un Manual de Procesos y Procedimientos, en los cuales se establecen los responsables y controles en materia de manejo de la información. Igualmente no se evidencia las asignación de roles y responsabilidades en seguridad de la Información.
Tabla 18. (Continuación)

SUÁREZ PADILLA & CÍA LTDA ANEXO A de la NORMA ISO 27001
Dominios de Control
A.9.4 Control de acceso a sistemas y aplicaciones
Se cuenta con creación y asignación de privilegios en el directorio activo y al Software de Nómina "Humano".
Dominio 10 Criptografía
A.10.1 Controles Criptográficos
No se cuenta con sistemas de autenticación segura mediante cifrado en el servidor.
Dominio 11 Seguridad física y ambiental
A.11.1 Áreas Seguras
La organización ha implementado controles de acceso físico, cuenta con un vigilante.
A.11.2 Equipos
Existe cableado estructurado en buen estado, se realiza mantenimiento a los equipos de cómputo, se cuenta con control de ingreso y salida de equipos.
Dominio 12 Seguridad en las operaciones
A.12.1 Responsabilidades y procedimientos operacionales
Los procedimientos operacionales se encuentran parcialmente documentados y tienen asignación de responsables.
A.12.2 Protección contra malware
Suárez Padilla & Cía Ltda, tiene implementado antivirus en los equipos de cómputo, cuenta con controles de acceso lógico mediante un firewall.
A.12.3 Backups
Las copias de respaldo se realizan a las Bases de Datos de Clientes, de Nómina "Humano" y de Contabilidad, de forma completa con una frecuencia quincenal.
A.12.4 Monitoreo y registro
No se realiza monitoreo de las bases de datos de la organización.

Tabla 18 (Continuación)

SUÁREZ PADILLA & CÍA LTDA ANEXO A de la NORMA ISO 27001
Dominios de Control
A.12.5 Control de software en el sistema operativo
Existe bloqueo de instalación de software por medio de políticas establecidas en el Directorio Activo.
A.12.6 Gestión de vulnerabilidades técnicas
La organización no cuenta con procedimientos documentados o implementados para atención, monitoreo, seguimiento y prevención de incidentes de seguridad de la información.
A.12.7 Controles de auditorías a los sistemas de información
Dominio 13 Seguridad en las comunicaciones
A.13.1 Gestión de seguridad en las redes
Suárez Padilla & Cía Ltda, cuenta con la implementación de controles en las redes con firewall, y políticas de directorio activo.
A.13.2 Transferencia de información
A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.14.1 Requerimientos de seguridad en los sistemas de información
Cuando se realiza las solicitudes de nuevos desarrollos, la organización solicita requerimientos de seguridad en los sistemas de información.
A.14.2 Seguridad en el desarrollo y soporte de procesos
A.14.3 Datos de prueba
Para la validación de los sistemas de información se realiza con datos de producción, los cuales son eliminados al momento de finalización de las pruebas.
A.15 Relación con proveedores
A.15.1 Seguridad en la relación con proveedores
En el proceso de contratación se tienen definidas las pólizas de cumplimiento, acuerdos de niveles de servicio, entre otros.
A.15.2 Gestión de la prestación de servicios con proveedores
La oficina de Talento Humano es la encargada de supervisar el cumplimiento, monitoreo y gestión del contrato.

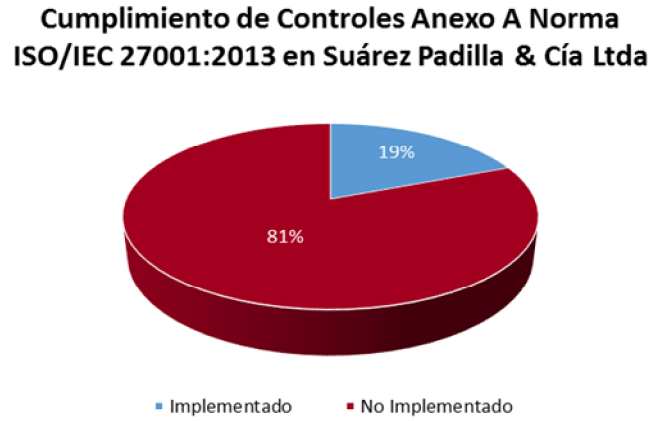
Tabla 18 Continuación

SUÁREZ PADILLA & CÍA LTDA ANEXO A de la NORMA ISO 27001
Dominios de Control
A.16 Gestión de incidentes de seguridad de la información
A.16.1 Gestión de incidentes de seguridad de la información y mejoras
La organización no cuenta con procedimientos documentados o implementados para atención, monitoreo, seguimiento y prevención de incidentes de seguridad de la información.
A.17 Aspectos de seguridad de la Información en la gestión de la continuidad del negocio
A.17.1 Seguridad en la continuidad del negocio
Suárez Padilla & Cía Ltda no cuenta con Plan de continuidad de negocio o plan de recuperación de desastres de forma que se pueda mantener la operación de los sistemas críticos de la organización ante la materialización de escenarios catastróficos. Se requiere dar una mayor relevancia a este dominio ya que se está arriesgando la subsistencia de la organización.
A.17.2 Redundancia
Suárez Padilla & Cía Ltda, no cuenta con redundancia en firewall, canales, UPS
A.18 Cumplimiento
A.18.1 Revisiones de seguridad de la Información
A.18.2 Cumplimiento con requerimientos legales y contractuales

Tabla 18 (Continuación)

A continuación se muestra gráficamente el estado general de cumplimiento de los controles del anexo A de la norma ISO 27001 en Suárez Padilla & Cía Ltda

Figura 8 Implementación de controles Anexo A Norma ISO 27001



Fuente: El autor

El Diagnóstico realizado definió el porcentaje máximo de cumplimiento que posee actualmente la organización, haciendo la claridad que dichos cumplimientos están sujetos a acciones de mejoramiento una vez se esté ejecutando la implementación del SGSI. Dichas acciones de mejoramiento reforzarán el cumplimiento de la norma y se enfocarán en la madurez, seguimiento y control del SGSI.

8.2 FASE 2. DEFINICIÓN DE POLÍTICAS, NORMAS, PROCEDIMIENTOS Y ACCIONES DE SEGURIDAD INFORMÁTICA A IMPLEMENTAR (SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA)

8.2.1 Políticas De Seguridad De La Información De Suárez Padilla & Cía Ltda. La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información de acuerdo con el procedimiento de “creación de políticas de gestión de seguridad de la información”, demostrando así su compromiso con la seguridad de la información en Suárez Padilla & Cía Ltda. Una vez aprobadas dichas políticas, debe velar por su divulgación, mantenimiento y cumplimiento al interior y con los terceros que interactúen directamente con la organización.

La Alta Dirección debe revisar periódicamente la aplicabilidad y vigencia de las siguientes Políticas específicas de Seguridad de la Información y efectuar los ajustes necesarios sobre ellas para que sean funcionales y se pueda seguir exigiendo su cumplimiento por parte de todos los empleados y personal suministrado por terceras partes que provean servicios a Suárez Padilla & Cía Ltda.

OBJETIVOS

✓ Proteger los recursos de información de la empresa Suarez Padilla & Cía. Ltda y los recursos tecnológicos utilizados para su procesamiento, frente a amenazas, tanto internas como externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

✓ Asegurar la implementación de las medidas de seguridad enmarcadas en este documento

RESPONSABILIDAD

Todos los Integrantes de la Alta Dirección, Empleados, Contratistas o Terceros son responsables de la implementación de las siguientes Políticas de Seguridad de la Información.

Las Políticas de Seguridad de la Información son de Carácter Obligatorio para todo el personal de la organización, cualquiera sea su situación laboral, el proceso al que pertenece y cualquiera que sea el nivel organizacional en el que se encuentre.

Los usuarios de la Información y de los Sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

Nota: Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

• Las políticas de seguridad de la información deben ser revisadas al menos una vez al año y actualizadas según las necesidades o los cambios en procesos y tecnología que se realicen en la organización.

ORGANIZACIÓN DE LA SEGURIDAD

- Suárez Padilla & Cía Ltda debe definir responsabilidades y deberes con respecto a la seguridad de la información, y asegurar la concientización de empleados y terceros con respecto a la importancia y el cumplimiento de la normatividad definida.

- La organización debe estar suscrita a páginas o grupos de investigación de seguridad de la información para mantener actualizada la gestión de vulnerabilidades y demás temas en seguridad.

- A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los siguientes Organismos Especializados en temas relativos a la seguridad de la información:

CIRTISI – Colombia: (Centro de información y respuesta técnica a incidentes de seguridad informática de Colombia)

Delegatura para la Protección de Datos Personales (DPDP) de la Superintendencia de Industria y Comercio (SIC): tiene el mismo nivel de otras delegaturas sobre temas tradicionales a cargo de la SIC. Como la protección al consumidor, la Promoción y protección de competencia, la propiedad industrial, el control y verificación de reglamentos técnicos y metrología legal.

- Los terceros que efectúen el tratamiento de información propia de Suárez Padilla & Cía Ltda o sobre la cual la organización sea responsable, deben cumplir con la Política de Seguridad de la Información vigente.

- El uso de dispositivos móviles para trasmitir, recibir, procesar o almacenar información es responsabilidad de cada funcionario o contratista y deberá velar por la seguridad de la información, en caso de incurrir en un incidentes de seguridad se aplicará el proceso disciplinario vigente de la organización.

- Las comunicaciones externas a la infraestructura de la organización deben realizarse por canales seguros que garanticen la confidencialidad de los datos de acceso y la comunicación que se transfiere y deberá ser aprobada por el líder del proceso de Talento Humano.

SEGURIDAD EN EL RECURSO HUMANO

- Se debe llevar a cabo un proceso de Selección adecuado según los perfiles a los que esté aspirando, por medio de la verificación de Antecedentes de los Empleados, Contratistas o Terceros, los controles del proceso de verificación cumplirán con los Requerimientos y Disposiciones legales de la Normatividad Vigente.

- La organización debe implementar capacitaciones y divulgaciones en seguridad de la información, de las políticas y procedimientos del sistema de gestión de seguridad de la información. Los empleados deben conocer la normatividad relacionada con la seguridad de la información de Suárez Padilla & Cía Ltda ya que el desconocimiento de la misma no los exonerará de los procesos disciplinarios definidos ante violaciones de las políticas de seguridad.

- La organización debe realizar un proceso de desvinculación de personal donde se garantice la eliminación de privilegios y eliminación de datos de acceso a los sistemas de información.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

- La organización debe identificar los activos de información de acuerdo con el alcance del SGSI, sus respectivos responsables y su ubicación, para luego elaborar un inventario con dicha información.

- El Inventario se debe documentar y actualizar ante cualquier modificación de la información y los activos asociados con los medios de procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.

- Es responsabilidad de realizar y mantener actualizado el inventario de activos de información cada responsable de proceso de Suárez Padilla & Cía Ltda en compañía del Líder de Seguridad de la Información.

- La clasificación de la Información se debe tener en cuenta los criterios de la Información en los cuales se fundamenta la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad.

Definición de los Criterios de Calificación de la Información:

- Uso Público: Información que por sus características puede o debe estar a disposición de cualquier persona natural o jurídica en el Estado Colombiano. Dentro de esta clasificación se puede considerar: noticias, informes de prensa, información de rendición de cuentas, información sobre trámites, normatividad.

- Interno: Información que por sus características puede o debe estar a disposición sólo del personal interno que labora en la compañía o terceros que deben acceder a la información por tener un vínculo directo con la organización.

- Uso Confidencial: Información cuya divulgación no autorizada puede afectar considerablemente el cumplimiento de la misión de Suárez Padilla & Cía Ltda. La divulgación de esta información, requiere de la aprobación de su respectivo propietario. En el caso de terceros rige el acuerdo de confidencialidad que exista entre Suárez Padilla & Cía Ltda y el tercero.

• Los medios físicos que almacenan y transportan información deben tener un cifrado o solicitar datos de autenticación para acceder a la información.

• Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios

CONTROL DEL ACCESO

• Los privilegios de acceso a los sistemas de información, infraestructura de red, equipos de cómputo e información sensible en la organización deben estar autorizados por el responsable o dueño del proceso al que pertenece el activo de información.

• El proceso de tecnologías de la información y de acuerdo al perfil de cargo define los niveles de acceso a la red, sistema operativo, sistemas de información y servicios de TI.

• El proceso de Talento Humano deberá mantener los registros donde se autorizó a los empleados o terceros los accesos a los diferentes sistemas de información de la organización.

- Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada empleado o tercero.

- Cuando se retire o cambie de contrato cualquier empleado, el proceso de tecnologías de la información deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el empleado estaba autorizado con el previo aviso del proceso de talento humano.

- El proceso de tecnologías de la información deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los empleados al menos una vez al año, manteniendo los registros de las revisiones y hallazgos.

- Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúscula y minúscula, en lo posible utilizar caracteres especiales.

- Todos los empleados deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 4 meses.

- Los sistemas de información deberán bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación.

Los usuarios deben cumplir las siguientes características para el uso de contraseñas:

a) Mantener los datos de acceso en secreto.

b) Sean fáciles de recordar.

c) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

d) Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: Pérdida, robo o indicio de pérdida de confidencialidad.

- Si el Funcionario debe abandonar la estación de trabajo por determinado tiempo, activará protectores de pantalla, con el fin de evitar que terceros puedan ver la información o continuar con la sesión de usuario habilitada.

SEGURIDAD FÍSICA Y DEL ENTORNO

- Mantener Áreas seguras para la gestión, almacenamiento y procesamiento de información en Suárez Padilla & Cía Ltda. Las áreas deben contar con protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.

- El ingreso de terceros a la Sala de Equipos, debe estar debidamente registrado mediante una bitácora custodiada por el personal de vigilancia de la organización.

- Los privilegios de acceso físico a la Sala de Equipos deben ser eliminados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un funcionario o contratista autorizado.

- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los empleados se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

- Los empleados o terceros que presten sus servicios a Suárez Padilla & Cía Ltda, no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

- Todos los visitantes que ingresan a la organización, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones de la misma.

- La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de cada funcionario y contratista asignado, junto con una autorización del jefe inmediato.

- La documentación física generada o recibida por los empleados de la organización o contratistas debe estar ubicada en archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las directrices establecidas por el proceso documental de la organización y según la clasificación de la documentación.

Equipos Desatendidos en Áreas de Usuarios

- Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.

- Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.

- Apagar los equipos de cómputo al finalizar la jornada laboral.

SEGURIDAD DE LAS OPERACIONES

- Deben establecerse medidas de control de acceso al sistema operativo, para garantizar la autenticación de los empleados.

- Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de Suárez Padilla & Cía Ltda, la interfaz del sistema operativo debe estar configurada de tal forma que tenga solo privilegios de invitado. Todas estas labores deben ser estrictamente realizadas por el proceso de gestión de tecnologías de la información.

- Todos los usuarios con acceso a un sistema de información o a la red informática de la organización dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que ha sido asignado.

- El acceso a la información de Suárez Padilla & Cía Ltda, deberá ser otorgado sólo a Usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad.

- El escritorio virtual de cada equipo de cómputo independiente del sistema operativo que use, debe mantenerte despejado, no debe contener archivos de ningún tipo salvo los accesos directos a aplicaciones necesarias en la labor del empleado.

- Todo el personal debe bloquear el equipo de cómputo con protector de pantalla que exija la contraseña de acceso a la sesión ante la ausencia temporal del puesto de trabajo.

- Por política de Directorio Activo se debe bloquear con protector de pantalla que exija la contraseña de acceso tras 3 minutos de inactividad del equipo.

- La asignación de privilegios a las aplicaciones informáticas presentes en Suárez Padilla & Cía Ltda, debe ser solicitada por el líder de proceso y/o jefe inmediato al proceso de gestión de la información y la comunicación para su ejecución.

- A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones contra software de seguridad, mantenimiento de los equipos, administración de la red y bloqueo de puertos en la red de telecomunicaciones.

- El proceso de tecnologías de la información y la comunicación debe ser la encargado de bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad.

SEGURIDAD DE LAS COMUNICACIONES

- Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la organización.

- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la organización.

- Los contratos o acuerdos contractuales que realice Suárez Padilla & Cía Ltda, deben incluir cláusulas que especifiquen las responsabilidades sobre el adecuado tratamiento de Información, estableciendo sanciones en caso de incumplimiento, y advirtiendo sobre la responsabilidad que en materia legal implica su desconocimiento. Se debe mantener un registro por Contratista, Proveedor, Cliente y Usuario del entendimiento y seguimiento de la Política.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- Suárez Padilla & Cía Ltda, debe establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.

- La información tratada por las aplicaciones aceptadas por Suárez Padilla & Cía Ltda, debe preservar su confiabilidad desde su ingreso, transformación y entrega a las aplicaciones de la Organización.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Suárez Padilla & Cía Ltda debe asegurar que se establezcan y ejecuten procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se haga una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

- Todos los usuarios de la información de Suárez Padilla & Cía Ltda deben reportar los incidentes de seguridad que se presenten, según el procedimiento de gestión de incidentes vigente en la organización.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

- Debe evaluarse el impacto de las interrupciones que afectan la operación de los procesos críticos de la institución y definir e implementar planes de

continuidad y de recuperación ante desastres para propender por la continuidad de la misma.

- Los planes de continuidad y de recuperación deben probarse y revisarse periódicamente y mantenerlos actualizados para su mejora continua y garantizar que sean efectivos.

- Para los procesos críticos del negocio, Suárez Padilla & Cía Ltda debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de Operación.

CUMPLIMIENTO

- Suárez Padilla & Cía Ltda, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros, la privacidad, los delitos informáticos, el uso inadecuado de recursos de procesamiento, el uso de criptografía y la recolección de evidencia.

- Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la compañía deben contar con su respectiva licencia de uso.

- Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.

- La Política junto con el Sistema de Gestión de Seguridad de la Información de Suárez Padilla & Cía Ltda, debe ser auditado anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

- La información de auditoría generada por el uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el Responsable para:

 Detectar Violaciones a la Política.

 Reportar incidentes de seguridad.

 Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

• Los contratos de trabajo de empleados y los contratos de desarrollo realizados por proveedores y contratistas deben contar con cláusulas respecto a la propiedad intelectual que le pertenece a Suárez Padilla & Cía Ltda.

8.2.2 Plan De Tratamiento De Riesgos Y Planes De Seguridad. Teniendo como base las entrevistas realizadas a los empleados que apoyan y conocen los procesos y del análisis de la información y documentación recibida, se identificaron oportunidades de mejora como parte del análisis de riegos que llevan a proponer los siguientes planes de tratamiento y de seguridad, con el fin de mejorar el Sistema de Gestión de Seguridad de la Información, así:

Tabla 19 Plan De Tratamiento De Riesgos Y Planes De Seguridad

No.	Actividad	Responsables	Fecha
1	Definir, documentar, Difundir e implementar un procedimiento de gestión de incidentes de seguridad de la información en la Empresa	Sandra Suárez, Olga Morales	23-Dic-2015
2	Revisión de Políticas de Contraseñas en Directorio Activo: Definir e implementar política de contraseñas seguras para el acceso a los sistemas de información	Sandra Suárez, Mónica Rivera	04-Dic-2015
3	Políticas de Bloqueo Automático de Equipos: Definir e implementar tiempos para el bloqueo automático de las pantallas y una política para que todos los usuarios bloqueen de forma manual al abandonar de forma permanente el lugar de trabajo.	Sandra Suárez, Mónica Rivera	04-Dic-2015
4	Procedimiento de Manejo de Dispositivos Móviles	Sandra Suárez, Olga Morales	27-Nov-2015
5	Ajustar Procedimiento de Administración de Personal	Sandra Suárez, Jackelinne Manosalva Cruz	04-Dic-2015
6	Fortalecer controles salida de equipos de la entidad	Sandra Suárez, Olga Morales	04-Dic-2015

No.	Actividad	Responsables	Fecha
7	Procedimiento de Gestión de Cambio	Sandra Suárez, Mónica Rivera	27-Nov-2015
8	Revisión y Mejoras Consola Antivirus	Sandra Suárez, Olga Morales	31-Dic-2015
9	Revisión y Mejoras Consola Filtro Contenido Web	Sandra Suárez, Fabio Parrado	31-Dic-2015
10	Revisión y Mejoras Consola Firewall	Sandra Suárez, Fabio Parrado	31-Dic-2015
11	Procedimiento de Gestión de Backups	Sandra Suárez, Olga Morales	31-Dic-2015
12	Procedimiento de Gestión de Usuarios: Definir, documentar e implementar procedimiento o política para asignación, revisión, modificación y eliminación de privilegios de acceso a los Sistemas de Información	Sandra Suárez, Mónica Rivera	04-Dic-2015
13	Revisar Acuerdos de Confidencialidad Funcionarios y Terceros	Sandra Suárez, Jackelinne Manosalva Cruz	04-Dic-2015
14	Definir, documentar, Difundir e implementar un Plan de Continuidad de Negocio para la Empresa.	Sandra Suárez, Olga Morales	27-Nov-2015
15	Definir, documentar, Difundir e implementar el procedimiento de Tratamiento de Datos Personales	Olga Morales	31-Dic-2015

Tabla 19 (Continuación)

8.2.3 Plan De Continuidad De Negocio De Suarez Padilla & Cia Ltda. Para desarrollar nuestro Plan de Continuidad y garantizar su éxito, lo primero es determinar los procesos esenciales del negocio dentro de la compañía, con el objetivo de asegurar la continuidad de la actividad en caso de contingencia.

Tabla 20 Procesos esenciales del negocio y Tiempo máximo de interrupción

Proceso	Necesidades de Recuperación (*)	Criticidad (*)
Soporte telefónico a solicitud o trámite	Día 1-7	2

Proceso	Necesidades de Recuperación (*)	Criticidad (*)
Atención personalizada Clientes	Día 1-7	2
Legalización de pólizas	Día 1-7	2
Control y verificación de pagos	Día 7–30	2
Gestión de Nómina	Día 7–30	3
Gestión de Talento Humano	Día 7–30	3

(*)Necesidad de Recuperación:
Día 0: Recuperación inmediata
Día 1-7: El proceso debe ser recuperado entre el primer y el quinto día después de un incidente.
Día 7–30: El proceso debe ser recuperado después de la primera semana y antes de un mes.
Más 30 días: El proceso pude esperar más de 30 días a ser recuperado.

(*) Rangos de Criticidad:
1 – La organización/departamento no puede funcionar sin el sistema
2 – La organización/departamento puede funcionar parcialmente sin el sistema
3 - La organización/departamento puede funcionar sin el sistema

En el caso de Suarez Padilla & Cía. Ltda, la disponibilidad de las comunicaciones y las calidades de servicio comprometidas son claves para el negocio pues preservar la confianza de los clientes es vital; una interrupción prolongada de las operaciones podría tener un impacto grave en la imagen institucional y en la confianza de los clientes. Esa desconfianza e incertidumbre impacta los procesos del negocio generando pérdidas potenciales.

Estrategia de Respaldo

Existen diferentes estrategias para mitigar el impacto de una interrupción, cada una tiene unos parámetros de tiempo, disponibilidad y costes asociados, a continuación se describe las estrategias de recuperación del negocio para la reubicación funcional que asegure la continuidad de los procesos:

Tabla 21 Estrategias de Respaldo

RECURSO CRÍTICO	OBJETIVO	ESTRATEGIAS DE RECUPERACIÓN
Personas que participan en las actividades de negocio	Mantener el conocimiento y las capacidades del personal con funciones y responsabilidades en actividades críticas	• Documentar actividades críticas • Formación • Conocimiento compartido y multidisciplinar • Separación de tareas clave
Instalaciones y Puestos de trabajo	Reducir el impacto que genera la falta de disponibilidad de las instalaciones de trabajo	• Instalaciones alternas • Teletrabajo
Tecnología	Entender el entorno tecnológico que soporta las actividades críticas y mantener la capacidad para replicarlo en caso de desastre	• Mantenimiento de la misma tecnología en diferentes ubicaciones • Copias de software crítico
Información y Documentación	Garantizar la protección y recuperación de la información vital para la organización	• Copias de seguridad • Procedimientos de recuperación

Fuente: El autor Tabla 21. (Continuación)

Tabla 22 Relación entre el Tiempo de Recuperación Objetivo y las Estrategias de Recuperación

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
MESES	Reconstrucción / Realojamiento	-
SEMANAS	Utilización de espacios propios existentes en la compañía	- - -
DIAS	Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad	- - - -

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
HORAS	Trabajo en casa Copias de software crítico Copias de seguridad	- - -
INMEDIATO	Localizaciones diversas para la misma función	- -

Fuente: El autor

Desarrollo del Plan de Continuidad

- **Organización De Los Equipos**

Comité de Crisis: Su objetivo es el de reducir al máximo el riesgo y la incertidumbre en la dirección de la situación, debe tomar las decisiones "clave" durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente.

Tabla 23 Comité de Crisis

Responsable del Comité:	Cristian Andrés Riaño: Subgerente Teléfono Móvil: XXXXXXX
Miembros del Comité:	Pedro Pablo González Santos Jefe de Oficina Comercial Teléfono Móvil: XXXXXXX
	María Victoria Martínez Jefe de Oficina Financiera Teléfono Móvil: XXXXXXX
	Jackelinne Manosalva Cruz Jefe de Oficina Recursos Humanos Teléfono Móvil: XXXXXXX

Fuente: El autor

Funciones:

- Análisis de la situación.

- Tomar la decisión de activar o no el Plan de Continuidad

- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación

- Iniciar el proceso de notificación a los empleados

Lugar de Reunión: Apartamento del Subgerente General Calle 83 # 14 36, Interior 3 Apartamento 305 Bogotá- Colombia

Equipo de Recuperación:

Su función es restablecer la infraestructura necesaria para la recuperación. Esto incluye el servidor, PC's, comunicaciones de voz y datos y cualquier otro elemento requerido para llevar a cabo la restauración de un servicio.

Suárez Padilla & Cía Ltda por el tamaño de la empresa a la fecha cuenta con un ingeniero de sistemas por contrato y un técnico, quienes deberán llevar a cabo todo el proceso de recuperación, para lo cual deberá desarrollar las siguientes actividades:

Desplazamiento del ingeniero desde la Oficina principal hacia la Calle 45 13- 27 Oficina 403 (sitio alterno). El orden de criticidad los sistemas a poner en marcha son: B.D Clientes, Nómina, contabilidad y Gestión del talento Humano, para lo cual se tomará la última copia de seguridad.

En este sitio alterno se cuenta con un servidor de aplicaciones de menores características que el de la Oficina principal y dos equipos de cómputo. La persona del equipo de logística será la encargada de proveer los recursos adicionales que se requieran con el fin de poder iniciar el restablecimiento de los servicios

Punto de Reunión: Campo de futbol Jorge Avellano. Si por motivo de la magnitud de los daños es imposible reunirse en el campo de futbol, se tomará como punto de reunión el parque principal Metrópolis, situado a 800 metros del Campo de futbol Jorge Avellano.

Integrantes del equipo:

Francisco Antonio Buendía
Ingeniero de Sistemas
Teléfono Móvil: XXXXXXX
Teléfono Casa: XXXXXXX

Carlos Alberto Ramírez
Técnico en Sistemas
Teléfono Móvil: XXXXXXX
Teléfono Casa: XXXXXXX

Equipo Logístico: Este equipo es el responsable de llevar a cabo toda la logística necesaria en el marco de la recuperación, tales como transporte de material, suministros de oficina, personas y comida, al lugar de recuperación si así se requiere. Este equipo está compuesto por el personal de la Oficina de Recursos Humanos

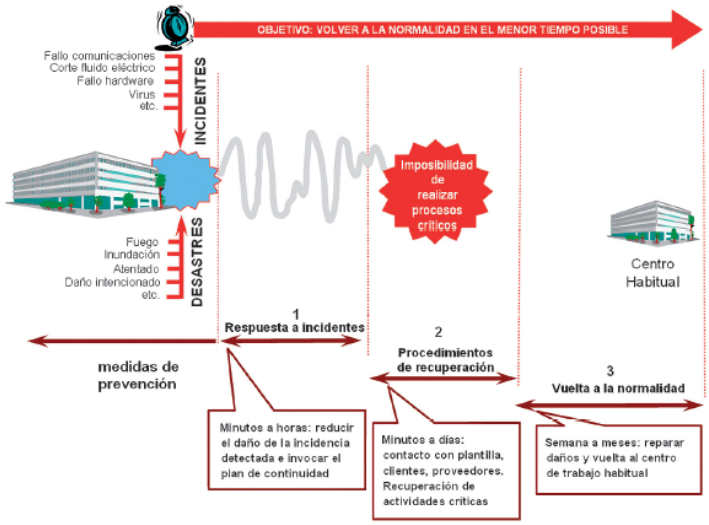
Integrantes del equipo:

Luis Alfonso Plazas
Técnico Administrativo
Teléfono Móvil: XXXXXXX
Teléfono Casa: XXXXXXX

Carolina Chica Tovas
Secretaria
Teléfono Móvil: XXXXXXX
Teléfono Casa: XXXXXX

- **Desarrollo De Procedimientos**

Figura 9 Etapas de una recuperación de desastres.



Fuente: http://en.calameo.com/read/001441005dcf633ec43ac pag.56

a. **Fase De Alerta.** Cualquier empleado que haya detectado una situación de contingencia o un incidente (fuego, inundación, virus, etc.), debe dar aviso con el máximo posible de detalle de manera inmediata al Jefe o superior jerárquico, éste a su vez da aviso a la persona de contacto del Comité de Crisis (Jefe de Recursos Humanos); una vez que el miembro del Comité de Crisis es informado del incidente, procederá a analizar y evaluar la incidencia, estimando los tiempos de interrupción y los servicios afectados, para luego con la recopilación de la mayor información posible convocar el equipo del Comité con el fin de evaluar la situación. Los incidentes que así lo requieran por estar incursos en la comisión de un delito, serán puestos en conocimiento de las autoridades correspondientes, a fin de contar con la asesoría de policía judicial, para el manejo de la evidencia digital y su posible judicialización.

Notificación: Cualquier empleado que haya detectado una situación de contingencia o un incidente (fuego, inundación, virus, etc.), debe dar aviso con el máximo posible de detalle de manera inmediata al Jefe o superior jerárquico, éste a su vez da aviso a la persona de contacto del Comité de Crisis (Jefe de Recursos Humanos); una vez que el miembro del Comité de Crisis es informado del incidente, procederá a analizar y evaluar la incidencia, estimando los tiempos de interrupción y los servicios afectados, para luego con la recopilación de la mayor información posible convocar el equipo del Comité con el fin de evaluar la situación.

Evaluación: El Comité analizará la situación y deberá tomar la decisión de activar o no el Plan de Continuidad. En caso de que la decisión sea no activar el Plan de

Continuidad porque la gravedad del incidente no lo requiere, se requerirá gestionar el incidente para que no aumente su gravedad.

Ejecución del Plan: Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, deberá comunicarse con los responsables de los equipos de recuperación y logística informando el inicio de las actividades del Plan para que inicien los procedimientos de actuación de cada uno de ellos.

b. **Fase De Transición.** Puesto en marcha el Plan, se deberá acudir a la oficina alterna (Calle 45 13- 27 Oficina 403). El equipo logístico deberá iniciar con el traslado de personas a la oficina alterna y del material requerido (Copias de software crítico, Copias de seguridad, material de oficina, documentación, etc.), para poner en marcha dicha oficina y así dar inicio a la intervención del equipo de recuperación, con el fin de establecer la infraestructura necesaria, tanto de software como de comunicaciones, etc.

Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como oficina alterna o cualquier otro designado por el Comité de Dirección de Crisis.

c. **Fase De Recuperación.** Establecidas las bases para dar inicio a la recuperación, se iniciará con la carga de datos y a la restauración de los servicios críticos, comprobando su funcionamiento con el fin de reanudar el negocio con las máximas garantías de éxito.

d. **Fase De Vuelta A La Normalidad.** Luego de haber solucionado la contingencia y haberse recuperado las actividades críticas de la empresa, se deben establecer los mecanismos necesarios para volver a la normalidad del "día a día" de las actividades. Se debe llevar a cabo un análisis de impacto con el fin de valorar de forma detallada los daños presentados (equipos, instalaciones averiadas, etc.), para así definir la estrategia de vuelta a la normalidad, dichas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

- **Generación De Informes Y Evaluación.** Cuando se determina el fin del incidente y se ha vuelto a la normalidad, se requiere que cada equipo realice un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc., y así las directivas podrán valorar la funcionalidad del Plan o si se presentaron fallos corregirlos.

➢ **Fin De La Contingencia.** Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre horas, días o meses, lo realmente importante es que durante el transcurso de este tiempo de vuelta a la normalidad, el servicio a los clientes y empleados sea prestado y que la incidencia afecte lo menos posible al negocio.

➢ **Plan De Mantenimiento Y Mejora Del Plan De Continuidad (BCP).** El Plan de Mantenimiento es un seguimiento de la eficacia y los resultados del BCP a lo largo del tiempo. No se trata de la realización puntual y periódica de una serie de procedimientos sino que es un proceso cíclico de mejora y revisión del BCP según los cambios tecnológicos, de personal o de funciones críticas.

El Plan de Mantenimiento debe llevarse a cabo especialmente en dos circunstancias del ciclo de vida del BCP:

▪ ***Errores localizados en el BCP durante la fase de pruebas:*** Si en el informe realizado posteriormente a la fase de pruebas se encuentran fallos en los procedimientos, en la coordinación del equipo de recuperación o en los tiempos de respuesta ante las situaciones de desastre, se deben analizar estos fallos para hacer las correspondientes modificaciones sobre el BCP.

▪ ***Cambios en el entorno del BCP:*** Si se producen cambios que afectan al modo de recuperación ante desastres, se deben hacer las correcciones necesarias en el BCP para adaptarse a las nuevas situaciones. Estos cambios pueden ser:

✓ Renovaciones tecnológicas: Cambios evolutivos en las tecnologías utilizadas en los procesos de negocio. Estos cambios requieren un cambio en las respuestas a las situaciones de desastre.

✓ Cambios estructurales en la organización: Si se producen modificaciones que afectan a la organización estructural de la empresa, como nuevos departamentos, nuevos perfiles de empleados o nuevas áreas de negocio se debe actualizar el BCP para asignar o desasignar tareas en función de la nuevas jerarquías implantadas en la organización.

✓ Contratos con los proveedores: Si cambian los proveedores que van a dar soporte técnico a los sistemas de información, o bien cambian los contratos de

soporte, se deben corregir los procedimientos de recuperación para adaptarse a las nuevas condiciones.

- **Desarrollar Programas De Entrenamiento Y Concientización.** En esta etapa, el objetivo principal será desarrollar un programa orientado a crear y mantener conciencia en el negocio, además de mejorar las habilidades requeridas para desarrollar e implementar los planes de recuperación. Para lograr esto deberá:

- Definir los objetivos de entrenamiento y concientización.

- Desarrollar y ejecutar programas variados de entrenamiento.

- Desarrollar programas de concientización.

- Identificar otras oportunidades de educación.

8.2.4 Procedimiento De Revisión De La Dirección. Sin el apoyo de la alta dirección de la empresa, la implementación de una política de seguridad fracasaría de manera inminente ya que es imprescindible que los directivos proporcionen los medios y el apoyo para llevar a cabo cualquier tipo de cambio en la cultura de la seguridad en la entidad.

Es por esto que la alta dirección deberá participar en la toma de decisiones relacionadas con la seguridad de la información y posterior a esto ejercer un seguimiento de los procedimientos y controles o mecanismos implementados para así garantizar el buen funcionamiento del Sistema de Gestión de Seguridad de la Información “SGSI”.

8.2.4 Procedimiento de revisión por parte de la dirección

a) En un periodo no mayor a un año la dirección llevará a cabo una verificación del cumplimiento de todos los estándares, normas y procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información “SGSI”. La persona encargada de llevar a cabo esta revisión será el Oficial de Seguridad.

b) El análisis de la situación se llevará a cabo sobre las siguientes áreas/controles:

- Comprobación del conocimiento de las normas por parte de las personas que acceden a los sistemas de información de la entidad.

- Control, revisión y evaluación de registros de usuarios, registros de incidencias de seguridad, control de inventario de activos, etc.

- Control de autorizaciones de delegación de funciones concernientes con la seguridad.

- Vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo Previa

c) Luego de realizado este análisis, el Oficial de Seguridad preparará un informe ejecutivo sobre los hallazgos, incidencias y deficiencias encontradas, sus posibles soluciones y propuestas de mejora.

d) Teniendo en cuenta los resultados de los informes de auditoría interna y el informe del análisis presentado por el Oficial de seguridad, la dirección actualizará los documentos del SGSI, modificando procedimientos y controles que afecten la seguridad de la información, si fuese necesario.

e) La dirección revisará los resultados de las auditorías internas anuales y hará un seguimiento semestral de las acciones correctivas. Igualmente deberá acudir a auditorías externas con una frecuencia de tres (3) años, haciendo un seguimiento de las acciones por lo menos anualmente.

f) Por lo menos anualmente la dirección solicitará un resumen de los indicadores de seguridad con el fin de ser analizados por el comité de seguridad.

8.2.5 Recomendaciones Acordes A Estandar Iso 27002. **RL**: Requerimiento Legal, **OC**: Obligaciones Contractuales, **RN/MP**: Requerimientos del negocio/Mejores Prácticas, **RER**: Resultados Evaluación de Riesgos (Ver Tabla 24. **Recomendaciones Acordes A Estándar ISO 27002)**

9. POLÍTICAS RECOMENDADAS EN LA ORGANIZACIÓN

Las siguientes son las políticas que se recomienda implementar en la empresa Suárez Padilla & Cia Ltda:

ALCANCE

Esta política es de aplicación para todas las áreas que hacen parte de la empresa Suárez Padilla & Cia Ltda, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la empresa a través de contratos o acuerdos con terceros y a todo el personal de la entidad, cualquiera sea su situación contractual, la dependencia en la cual se encuentre prestando sus servicios y el nivel de las tareas que desempeñe.

Acuerdos de confidencialidad

Todos los funcionarios de Suárez Padilla & Cia Ltda y/o terceros deben aceptar los acuerdos de confidencialidad, donde cada funcionario individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; cualquier violación a lo establecido en este parágrafo será considerado como un “incidente de seguridad”.

Uso adecuado de los activos

El acceso a los documentos físicos y digitales estará determinado por la competencia del área específica y los permisos y niveles de acceso de los funcionarios y/o contratistas, serán determinadas por los Jefes de Área o Dependencia, quien comunicará a la persona encargada de la administración de los recursos informáticos el listado con los funcionarios y sus privilegios con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la empresa.

Acceso a Internet

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea tales como Facebook, MSN Messenger, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de Suárez Padilla & Cía Ltda.

- El intercambio no autorizado de información de propiedad de Suárez Padilla & Cía Ltda, de sus clientes y/o de sus funcionarios, con terceros.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

b) Todos los usuarios son responsables de dar un uso adecuado a este recurso y en ningún momento pueden usarlo para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

c) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Suárez Padilla & Cía Ltda.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados a funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware, cambios de configuración del equipo cómputo de Suárez Padilla & Cía Ltda, es

responsabilidad de la persona encargada de la administración de los recursos informáticos y por tanto es el único autorizado para realizar estas labores.

b) La sincronización de dispositivos móviles, sobre los que se puedan realizar intercambios de información con cualquier recurso de la empresa, deberán estar autorizados de forma explícita por la dependencia respectiva, en conjunto con la persona encargada de la administración de los recursos informáticos y podrá llevarse a cabo únicamente en dispositivos provistos por la entidad, para tal fin.

Capacitación y educación en seguridad de la información

Todo empleado de la empresa al momento de ingresar a la misma debe contar con la inducción y actualización periódica en materia de la política, normas y procedimientos consignados en el Manual de Políticas de Seguridad de la Información; esta tarea deberá desarrollarse por la Oficina de Recursos Humanos, donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

Control de acceso físico

a) Se debe tener acceso controlado y restringido al cuarto de servidores y de comunicaciones.

b) Se deberán elaborar y mantener las normas, controles y registros de acceso a dicha área.

Protección y ubicación de los equipos

a) Los equipos que hacen parte de la infraestructura tecnológica de Suárez Padilla & Cia Ltda, así como estaciones de trabajo, deben estar ubicados y protegidos adecuadamente, para lo cual deben adoptase los controles necesarios con el fin de mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

b) Los funcionarios y/o contratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de Suárez Padilla & Cia Ltda no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

Protección contra software malicioso

a) Todos los sistemas informáticos deben ser protegidos por software antivirus con capacidad de actualización automática.

b) El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Copias de respaldo

a) Suárez Padilla & Cia Ltda debe asegurar que la información con cierto nivel de clasificación, contenida en la plataforma tecnológica de la empresa, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

b) Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

c) Los medios magnéticos que contienen la información crítica deberá ser almacenados en un sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Control de acceso lógico

a) Todos los usuarios de equipos de cómputo son responsables de la confidencialidad del identificador de usuario y el password de su equipo.

b) Todos los usuarios deberán autenticarse con los mecanismos de control de acceso lógico antes de tener acceso a los recursos de la Infraestructura tecnológica de la empresa.

c) El identificador de usuario dentro de la red es único y personalizado, por lo tanto el usuario es responsable de todas las actividades realizadas con su identificador de usuario

Gestión de contraseñas de usuario

a) Es obligación del usuario cambiar la clave por defecto asignada por la persona encargada de la administración de los recursos informáticos

b) Cuando un usuario olvide, bloquee o extravíe su password deberá solicitar a la persona encargada de la administración de los recursos informáticos para que ella realice la acción que le permita ingresar un nuevo password, y al momento de recibirlo deberá personalizar uno nuevo.

c) Está prohibido mantener ayudas escritas o impresas referentes al password en lugares donde personas no autorizadas pueden descubrirlos.

d) La revelación del password o contraseña a terceros responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

e) Los usuarios deberán observar las siguientes guías para la construcción de su contraseña:

- La contraseña estará compuesta de caracteres alfanuméricos de mínimo siete (8) caracteres y máximo 12 (doce) y deberán estar constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

- No deben estar relacionados con nombre del empleado, fechas de nacimiento, lugar o cargo o estado dentro del trabajo.

- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días.

Escritorio y pantalla limpia

a) Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo y se podrá desbloquear sólo con la contraseña del usuario.

b) Al finalizar las actividades diarias, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

c) Se establecerá una política de protector de pantalla a nivel de directorio activo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Reporte e investigación de incidentes de seguridad de la información

a) Los empleados y/o contratistas de la empresa Suarez Padilla & Cía Ltda debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la persona encargada de la administración de los recursos informáticos.

b) Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, se deberá informar al encargado de la administración de los recursos informáticos tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Tabla 24 Recomendaciones Acordes A Estándar ISO 27002

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Políticas de Seguridad de la Información	**A.5.1**	**Política de 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 los reglamentos y las leyes pertinentes.					
	A.5.1.1	Políticas de Seguridad de la Información.			X	X	Es importante que el documento sea: Aprobado, divulgado e implementado al interior de la organización.
	A.5.1.2	Revisión de las Política de Seguridad de la Información.				X	Documentar política de revisión, actualización y divulgación de las políticas de seguridad de la información en la organización.
Organización de la Seguridad de la Información	**A.6.1**	**Organización Interna.**					
		Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.					
	A.6.1.1	Roles y responsabilidades para la seguridad de la Información.			X		Definir los roles y responsabilidades de seguridad de la información al interior de la organización.
	A.6.1.2	Separación de deberes.			X		Definir los deberes en seguridad de la información de los empleados de la entidad.
	A.6.1.3	Contacto con las Autoridades.				X	Adicionar el contacto con las autoridades en Colombia en el procedimiento de Gestión de Incidentes.

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Organización de la Seguridad de la Información	A.6.1.4	Contacto con Grupos de Interés Especiales.			X		Realizar contactos con grupos de investigación, páginas de información, para mantener actualizada la organización en seguridad de la información
	A.6.1.5	Seguridad de la Información en la gestión de proyectos.			X	X	Definir políticas, normas o estándares de seguridad en los nuevos proyectos de la organización.
	A.6.2	**Dispositivos móviles y teletrabajo.**					
		Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.					
	A.6.2.1	Política para dispositivos móviles.			X		Definir política de acceso a áreas seguras de los dispositivos móviles.
	A.6.2.2	Teletrabajo.			X		Si se contempla por parte de la organización aprobar el teletrabajo, se deben establecer políticas de acceso remoto a los servidores o aplicaciones de la organización el cual debe ser por un canal seguro (Cifrado) y tener un listado de que empleado y contratistas estarán autorizados.
Seguridad de los Recursos Humanos	**A.7,1**	**Antes de asumir el empleo**					
		Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos e los roles para los que se consideran.					
	A.7.1.1	Selección.		X	X		Control adecuado con posibilidades de mejora

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de los Recursos Humanos	A.7.1.2	Términos y condiciones de empleo.	X	X			Control adecuado con posibilidades de mejora
	A.7.2	**Durante la ejecución del empleo.**					
		Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.					
	A.7.2.1	Responsabilidades de la dirección.			X	X	Incluir en el contrato laboral, la aceptación por parte de los empleados o contratistas el cumplimiento de las Políticas de Seguridad de la Información establecidas en la organización.
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.			X	X	Definir un plan de capacitaciones a los empleados y contratistas en temas de seguridad de la información, y realizar sensibilizaciones al interior de la organización del SGSI.
	A.7.2.3	Proceso disciplinario.			X	X	Integrar en un documento de "PROCEDIMIENTO FUNCIONES DISCIPLINARIAS" el incumplimiento de los procedimientos, normas o políticas de seguridad de la información en la organización.
	A.7.3	**Terminación y cambio de empleo.**					
		Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.					

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de los Recursos Humanos	A.7.3.1	Terminación o Cambio de responsabilidades de empleo.			X		Incluir en el documento: PROCEDIMIENTO ADMINISTRACIÓN DE PERSONAL" o definir uno nuevo, donde se indique las actividades en el momento de la terminación laboral o cambios en la contratación de los empleados o contratistas de la organización.
Gestión de activos	**8.1**	**Responsabilidad por los activos.**					
		Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.					
	A.8.1.1	Inventario de activos.			X	X	Se debe realizar un instructivo para el mantenimiento y actualización del inventario de activos.
	A.8.1.2	Propiedad de los activos.					Control adecuado con posibilidades de mejora
	A.8.1.3	Uso aceptable de los activos.				X	Aunque se cuenta con política de uso aceptable de los activos no ha sido aprobada ni divulgada a los empleados o contratistas.
	A.8.1.4	Devolución de Activos.			X		Verificar que el control se esté aplicando en la organización por parte de los procesos involucrados.
	8.2	**Clasificación de la información.**					

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Gestión de activos		**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.**					
	A.8.2.1	Clasificación de la información.			X		No existe un proceso formal donde se determine la clasificación de la información de la organización.
	A.8.2.2	Etiquetado de la información.			X	X	La documentación de la organización debe contar con etiquetado según los niveles de clasificación definidos y establecidos por la organización.
	A.8.2.3	Manejo de activos.			X	X	El manejo de la información deberá estar definido en el proceso o procedimiento de clasificación de la información y dependerá de su nivel de clasificación.
	8.3	**Manejo de medios.**					
		Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.					
	A.8.3.1	Gestión de medios removibles.				X	Definir política, procedimiento o estándar para la compra, manejo o eliminación de medios removibles en la organización.
	A.8.3.2	Disposición de los medios.				X	
	A.8.3.3	Transferencia de medios físicos.					Definir política o estándar para el transporte de medios físicos que transporten información.
	A.9.1	**Control de acceso.**					

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Control de acceso		**Limitar el acceso a información y a instalaciones de procesamiento de información.**					
	A.9.1.1	Política de control de acceso.			X		Realizar aprobación y divulgación de las políticas de Seguridad de la Información
	A.9.1.2	Acceso a redes y servicios de red.					
	A.9.2	**Gestión de acceso de usuarios.**					
		Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.					
	9.2.1	Registro y cancelación del registro de usuarios.				X	Sugerencia: Definir el proceso de creación y cancelación de usuarios, para tener control de los usuarios que acceden a las aplicaciones.
	9.2.2	Suministro de acceso de usuarios.				X	Con el proceso o procedimiento que se defina en la creación y cancelación de usuarios es importante definir los diferentes niveles de privilegios que pueden asignar a los sistemas de información.
	9.2.3	Gestión de derechos de acceso privilegiado.				X	
	9.2.4	Gestión de información de autenticación secreta de usuarios.				X	Definir en el proceso o procedimiento de creación y cancelación de usuarios los lineamientos de asignación de nombre de usuario y estructura de contraseñas seguras para el acceso por parte de los usuarios de cada sistema de información.
	9.2.5	Revisión de los derechos de acceso de usuarios.				X	La eliminación de los derechos de acceso se realiza de acuerdo con la aplicación del procedimiento de

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Control de acceso	9.2.6	Retiro o ajuste de los derechos de acceso.					"administración de personal". Importante mencionar en el documento una frecuencia de revisión de privilegios de los sistemas de información.
	A.9.3	**Responsabilidad de los usuarios.**					
		Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
	A.9.3.1	Uso de información de autenticación secreta.				X	Control adecuado con posibilidades de mejora
	A.9.4	**Control de acceso a sistemas y aplicaciones.**					
		Evitar el acceso no autorizado a sistemas y aplicaciones.					
	A.9.4.1	Restricción de acceso a la información.			X		De acuerdo con la asignación de privilegios a los sistemas de información se debe restringir el acceso a la información según el nivel de clasificación que se tenga.
	A.9.4.2	Procedimiento de ingreso seguro.			X	X	Definir un procedimiento de ingreso seguro a los equipos de cómputo de la organización.
	A.9.4.3	Sistemas de gestión de contraseñas.			X	X	Se asigna una contraseña genérica de Directorio Activo y no se forza para que el usuario la cambie en el siguiente logon, se deben integrar todos los sistemas para que autentiquen con el Directorio Activo.

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Control de acceso	A.9.4.4	Uso de programas utilitarios privilegiados.			X	X	No se puede controlar de manera centralizada qué programas puede o no ejecutar el usuario
	A.9.4.5	Control de acceso a códigos fuente de programas.					Definir un lugar de almacenamiento de los códigos fuentes de las aplicaciones de la organización donde solo tenga acceso el personal autorizado para su consulta.
Criptografía	**A.10.1**	**Controles Criptográficos.**					
		Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.					
	A.10.1.1	Políticas sobre el uso de controles criptográficos.			X		Definir, documentar e implementar políticas de controles criptográficos
	A.10.1.2	Gestión de llaves.			X		Se debe desarrollar un procedimiento de gestión centralizada de las llaves y certificados digitales.
Seguridad física y del entorno	**A.11.1**	**Áreas seguras.**					
		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.					
	A.11.1.1	Perímetros de seguridad física.			X		Control adecuado con posibilidades de mejora
	A.11.1.2	Controles de accesos físicos.			X		Control adecuado con posibilidades de mejora

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad física y del entorno	A.11.1.3	Seguridad de oficinas, recintos e instalaciones.			X		Control adecuado con posibilidades de mejora
	A.11.1.4	Protección contra amenazas externas y ambientales.			X		Control adecuado con posibilidades de mejora
	A.11.1.5	Trabajo en áreas seguras.					Definir áreas seguras en la organización donde el control de acceso y el acceso con equipos electrónicos sean restringidos.
	A.11.1.6	Áreas de despacho y carga.			X		
	A.11.2	**Equipos.**					
		Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.					
	A.11.2.1	Ubicación y protección de los equipos.			X		Se debe fortalecer el control de salida de equipos y sensibilizar a los usuarios en la protección física de los mismos, ya que en las pruebas de Ingeniería Social realizadas se evidenciaron muchos equipos portátiles sin protección
	A.11.2.2	Servicio de suministro.			X		Control adecuado con posibilidades de mejora
	A.11.2.3	Seguridad de cableado.			X		Control adecuado con posibilidades de mejora

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad física y del entorno	A.11.2.4	Mantenimiento de equipos.			X		Control adecuado con posibilidades de mejora
	A.11.2.5	Retiro de activos.				X	Definir un procedimiento o política que indique el método de retiro de los activos.
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.			X		Definir un procedimiento o política que indique el método para garantizar la seguridad de los equipos fuera de las instalaciones.
	A.11.2.7	Disposición segura o reutilización de equipos.					Definir e implementar un procedimiento o política en la organización para una segura reutilización o eliminación de los equipos de cómputo.
	A.11.2.8	Equipos de usuario desatendido.			X		Control adecuado con posibilidades de mejora
	A.11.2.9	Política de escritorio limpio y pantalla despejada.				X	Definir e implementar política para escritorio virtual y físico limpio, donde no se permita el almacenamiento o permanencia de información confidencial.
	A.12.1	**Procedimientos operacionales y responsabilidades.**					
		Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.					

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de las operaciones	A.12.1.1	Procedimiento de operación documentados.			X		Control adecuado con posibilidades de mejora
	A.12.1.2	Gestión de cambios.					Definir e implementar un procedimiento de Gestión de Cambios.
	A.12.1.3	Gestión de capacidad.			X		Realizar seguimiento y análisis a los resultados de la medición, mantener actas o informes de las actividades de la medición.
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.			X		Definir e implementar los ambientes de desarrollo, pruebas y operación.
	A.12.2	**Protección contra códigos maliciosos.**					
		Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.					
	A.12.2.1	Controles contra códigos maliciosos			X		Realizar seguimiento y análisis desde una consola centralizada del antivirus y eventos o incidentes que se presenten en el firewall.
	A.12.3	**Copias de respaldo.**					
		Proteger contra la pérdida de datos.					
		Respaldo de la información.			X		Realizar y verificar la copia de seguridad del servidor de la organización. Realizar verificación periódica de las copias de respaldo de los discos compartidos para revisar su confiabilidad.

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de las operaciones	**A.12.4**	**Registro y seguimiento.**					
		Registro de eventos y generar evidencia.					
	A.12.4.1	Registro de eventos.			X		Determinar un canal para reporte de eventos de seguridad, y generación automática de los eventos que se presenten en los sistemas de información.
	A.12.4.2	Protección de la información de registro.			X		Garantizar un almacenamiento seguro de los eventos de seguridad que se presenten en la organización.
	A.12.4.3	Registros del administrador y operador.			X		Verificar el registro de actividades en los sistemas de información y garantizar un almacenamiento seguro.
	A.12.4.4	Sincronización de relojes.			X		Control adecuado con posibilidades de mejora
	A.12.5	**Control de software operacional.**					
		Asegurarse de la integridad de los sistemas operacionales.					
	A.12.5.1	Instalación de software en sistemas operativos.			X		
	A.12.6	**Gestión de la vulnerabilidad técnica.**					
		Prevenir el aprovechamiento de las vulnerabilidades técnicas.					
	A.12.6.1	Gestión de las vulnerabilidades técnicas.				X	Definir un procedimiento para la gestión de las vulnerabilidades técnicas donde se incluya su reporte, tratamiento y mejora.

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de las operaciones	A.12.6.2	Restricción sobre la instalación de software.			X		Control adecuado con posibilidades de mejora
	A.12.7	**Consideraciones sobre auditorías de sistemas de información.**					
		Minimizar el impacto de las actividades de auditoría sobre los sistemas					
	A.12.7.1	Controles de auditorías de sistemas de información.			X		Se debe implementar un mecanismo de monitoreo de logs y correlación de eventos de la plataforma más crítica
Seguridad de las comunicaciones	**A.13.1**	**Gestión de la seguridad de las redes.**					
		Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.					
	A.13.1.1	Controles de redes.			X		Se recomienda implementar una solución (Ej.: NAC - Control de Acceso a la Red) que permita controlar los equipos de funcionaros y de terceros que conectan a la red corporativa.
	A.13.1.2	Seguridad de los servicios de red.			X		Se deben documentar todos los servicios de red, implementando los controles de seguridad que apliquen en cada caso.
	A.13.1.3	Separación en las redes.			X		Cuando se dé la ampliación de la planta de personal se debe implementar una adecuada segmentación de redes

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Seguridad de las comunicaciones	**A.13.2**	**Transferencia de información.**					
		Mantener la seguridad de la información transferida dentro de una organización y con cualquier organización externa.					
	A.13.2.1	Políticas y procedimientos de transferencia de información.			X		Definir e implementar políticas de transferencia de información en la organización.
	A.13.2.2	Acuerdos sobre transferencia de información.			X		
	A.13.2.3	Mensajería electrónica.			X	X	Verificar que el cifrado de correo electrónico se encuentre activado.
	A.13.2.4	Acuerdos de confidencialidad o de no divulgación.			X	X	Definir acuerdo de confidencialidad con los empleados y contratistas de la organización.
Adquisición, desarrollo y mantenimiento de sistemas	**A.14.1**	**Requisitos de seguridad de los sistemas de información.**					
		Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.					
	A.14.1.1	Análisis y especificaciones de requisitos de seguridad de la información.			X		Definir política para que en todos los proyectos de la organización se tenga en cuenta requisitos de seguridad de la información.
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.			X	X	Se debe asegurar el FTP que está expuesto con acceso anónimo

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Adquisición, desarrollo y mantenimiento de sistemas	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.			X		
	A.14.2	**Seguridad en los procesos de desarrollo y de soporte.**					
		Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
	A.14.2.1	Política de desarrollo seguro.			X		Definir, divulgar e implementar política de desarrollos seguro en los sistemas de información de la organización.
	A.14.2.2	Procedimientos de control de cambios en sistemas.			X		Definir, divulgar e implementar procedimiento de control de cambios en los sistemas de información e infraestructura tecnológica.
	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.			X		Definir, divulgar e implementar procedimiento, formato o lista de chequeo cuando se realicen cambios en la plataforma tecnológica.
	A.14.2.4	Restricción en los cambios a los paquetes de software.			X		Definir, divulgar e implementar política para la restricción a los paquetes de software.
	A.14.2.5	Principios de construcción de los sistemas seguros.			X		Se deben desarrollar estándares de seguridad de desarrollo de software
	A.14.2.6	Ambiente de desarrollo seguro.			X		Definir los controles de seguridad con los debe contar el ambiente de desarrollo

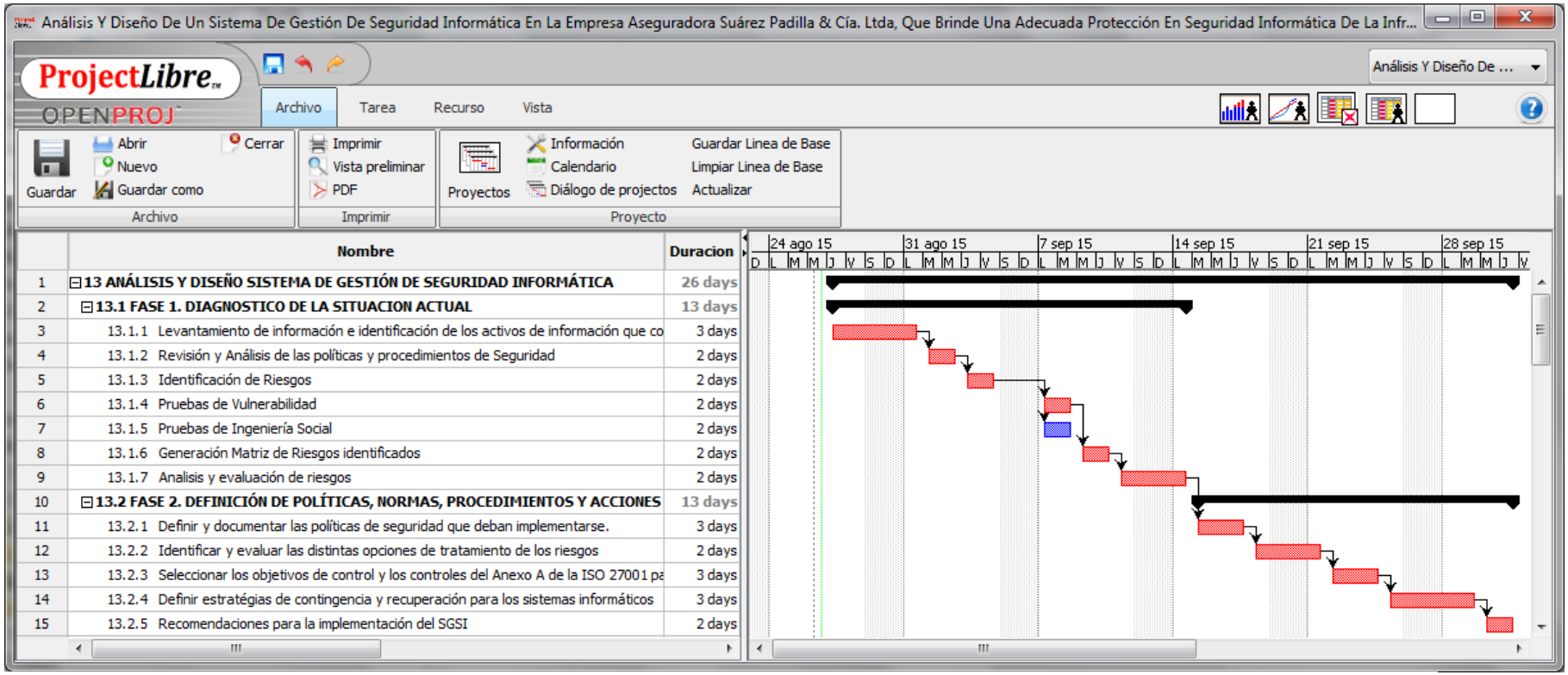
CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Adquisición, desarrollo y mantenimiento de sistemas	A.14.2.7	Desarrollo contratado externamente.			X		Control adecuado con posibilidades de mejora
	A.14.2.8	Pruebas de seguridad de sistemas.			X		Definir un plan de pruebas de seguridad a los actuales y a los nuevos desarrollos de la organización, junto con una política que contenga criterios de aceptación de los sistemas.
	A.14.2.9	Prueba de aceptación de sistemas.			X		
	A.14.3	**Datos de pruebas.**					
		Asegurar la protección de los datos usados para pruebas.					
	A.14.3.1	Protección de datos de prueba.			X		Se debe definir una política que contenga el uso y manejo adecuado para la protección de los datos usados para pruebas
Relaciones con los proveedores	**A.15.1**	**Seguridad de la información en las relaciones con los proveedores.**					
		Asegurar la protección de los activos de la organización que sean accesibles a Los proveedores.					
	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.			X		Definir, divulgar e implementar política de seguridad de la información donde contemple tener seguridad en la relación con los proveedores
	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.			X		Control adecuado con posibilidades de mejora

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
	A.15.1.3	Cadena de suministro de tecnología de información y comunicación.			X		Control adecuado con posibilidades de mejora
	A.15.2	**Gestión de la prestación de servicios de proveedores.**					
		Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.					
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.			X		Se debe validar la viabilidad de programar una auditoria para las empresas que le prestan servicios a la organización.
	A.15.2.2	Gestión de cambios en los servicios de los proveedores.			X		Se debe validar el proceso de gestión de cambio de los proveedores
Gestión de incidentes de seguridad de la información	**A.16.1**	**Gestión de incidentes y mejoras en la seguridad de la información.**					
		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.					
	A.16.1.1	Responsabilidades y procedimientos.			X	X	Definir, divulgar e implementar procedimiento de gestión de incidentes de seguridad de la información.
	A.16.1.2	Reporte de eventos de seguridad de la información.			X	X	
	A.16.1.3	Reporte de debilidades de seguridad de la información.			X	X	
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.			X	X	
	A.16.1.5	Respuesta a incidentes de seguridad de la información.			X	X	

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.			X	X	
	A.16.1.7	Recolección de evidencia.			X	X	
Aspectos de seguridad de la información de la gestión de continuidad de negocio	**A.17.1**	**Continuidad de seguridad de la información.**					
		La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					
	A,17.1.1	Planificación de la continuidad de la seguridad de la información.			X	X	Aprobar, divulgar, implementar y probar en plan de continuidad del negocio.
	A,17.1.2	Implementación de la continuidad de la seguridad de la información.			X	X	
	A,17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.			X	X	
	A.17.2	**Redundancias.**					
		Asegurar la disponibilidad de instalaciones de procesamiento de información.					
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.			X	X	Control adecuado con posibilidades de mejora
Cumplimiento	**A.18.1**	**Cumplimiento de requisitos legales y contractuales.**					
		Evitar el incumplimiento de las obligaciones legales, estatutarias, de					
	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.					Control adecuado con posibilidades de mejora

CONTROLES ISO 27002			Selección Controles y Razón				Recomendación
			RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**					
Cumplimiento	A.18.1.2	Derechos de propiedad intelectual.					Control adecuado con posibilidades de mejora
	A.18.1.3	Protección de registros.			X		Se debe fortalecer los controles de acceso a la información
	A.18.1.4	Privacidad y protección de información de datos personales.	X		X	X	Se debe documentar e implementar controles sobre los datos personales que se manipulan en la organización
	A.18.1.5	Reglamentación de controles criptográficos.			X		Definir, divulgar e implementar política de controles criptográficos.
	A.18.2	**Revisiones de seguridad de la información.**					
		Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.					
	A.18.2.1	Revisión independiente de la seguridad de la información.			X		Se deben aprobar, dar o a conocer y entender las políticas de seguridad de la información
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad.			X	X	Se deben implementar mecanismos que permitan medir el cumplimiento de las políticas de seguridad
	A.18.2.3	Revisión del cumplimiento.			X	X	Se deben implementar mecanismos que permitan medir el cumplimiento de las políticas de seguridad

CRONOGRAMA


Análisis Y Diseño De Un Sistema De Gestión De Seguridad Informática En La Empresa Aseguradora Suárez Padilla & Cía. Ltda, Que Brinde Una Adecuada Protección En Seguridad Informática De La Infr...
ProjectLibre
OPENPROJ
Archivo
Tarea
Recurso
Vista
Análisis Y Diseño De ...
Abrir
Nuevo
Guardar como
Cerrar
Guardar
Archivo
Imprimir
Vista preliminar
PDF
Imprimir
Proyectos
Información
Calendario
Diálogo de proyectos
Guardar Linea de Base
Limpiar Linea de Base
Actualizar
Proyecto
Nombre
Duracion
1 13 ANÁLISIS Y DISEÑO SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA 26 days
2 13.1 FASE 1. DIAGNOSTICO DE LA SITUACION ACTUAL 13 days
3 13.1.1 Levantamiento de información e identificación de los activos de información que co 3 days
4 13.1.2 Revisión y Análisis de las políticas y procedimientos de Seguridad 2 days
5 13.1.3 Identificación de Riesgos 2 days
6 13.1.4 Pruebas de Vulnerabilidad 2 days
7 13.1.5 Pruebas de Ingeniería Social 2 days
8 13.1.6 Generación Matriz de Riesgos identificados 2 days
9 13.1.7 Analisis y evaluación de riesgos 2 days
10 13.2 FASE 2. DEFINICIÓN DE POLÍTICAS, NORMAS, PROCEDIMIENTOS Y ACCIONES 13 days
11 13.2.1 Definir y documentar las políticas de seguridad que deban implementarse. 3 days
12 13.2.2 Identificar y evaluar las distintas opciones de tratamiento de los riesgos 2 days
13 13.2.3 Seleccionar los objetivos de control y los controles del Anexo A de la ISO 27001 pa 3 days
14 13.2.4 Definir estratégias de contingencia y recuperación para los sistemas informáticos 3 days
15 13.2.5 Recomendaciones para la implementación del SGSI 2 days
24 ago 15
31 ago 15
7 sep 15
14 sep 15
21 sep 15
28 sep 15

10. CONCLUSIONES

Como se ha evidenciado a lo largo de este trabajo, es claro e innegable que la "información y los datos" son el activo más importante de una organización, es por ello que partiendo de dicha premisa para una Pyme como Suárez Padilla & Cía. Ltda es importante poder contar con un Sistema de Gestión de Seguridad de la Información (SGSI) enfocado en las necesidades del negocio y basado en estándares y buenas prácticas como lo es la norma ISO/IEC 27001:2013.

✓ La falta de políticas, controles y normativas de seguridad pueden ocasionar consecuencias graves en el cumplimiento de los objetivos organizacionales.

✓ Para asegurar el éxito y la madurez del SGSI es de vital importancia contar con el apoyo incondicional de la alta Dirección para la aprobación de la documentación generada, la divulgación y su aplicación por parte de los funcionarios y contratistas.

✓ Se debe atacar en el menor tiempo posible los incidentes se seguridad materializados y que aún no reciben tratamiento formal mediante el diseño e implementación de un "procedimiento de gestión de incidentes" para el tratamiento correcto de los mismos y que ayude a crear cultura para documentar todo lo que sucede respecto a la seguridad que facilite la identificación de las vulnerabilidades en seguridad de la información.

✓ La implementación de un SGSI en la empresa Suárez Padilla y Cía. Ltda, brindará seguridad efectiva en los sistemas de información e incrementará la confianza de sus clientes mejorando su imagen ante ellos generando solidez de la misma.

11. RECOMENDACIONES

Es imprescindible que la Alta Dirección apruebe, dé a conocer y entender las políticas de seguridad de la información a toda la organización.

Realizar capacitaciones y sensibilizaciones a todos los empleados de Suárez Padilla & Cía. Ltda en seguridad de la Información para mitigar riesgos de ataques de tipo ingeniería social

BIBLIOGRAFÍA

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD-AEC. La gestión de la seguridad en la empresa. En Revista Calidad. [En línea], (Junio 2006). p.12. [Consultado 26 de noviembre, 2014]. Disponible en internet: www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

CAMELO, Leonardo. Seguridad de la Información en Colombia. Experiencia personal: dificultades en la implementación de un SGSI. [En línea].2010. [Consultado 26 de diciembre, 2014]. Disponible en Internet: (seguridadinformacioncolombia.blogspot.com.co/2010/02/experiencia-personal-dificultades-en-la.html)

CAMELO, Leonardo. Seguridad de la Información en Colombia. Marco Normativo (Normas y políticas) de un SGSI. [En línea]. 2010. [Consultado 14 de diciembre, 2014]. Disponible en Internet: (seguridadinformacioncolombia.blogspot.com.co/2010/03/marco-normativo-normas-y-politicas-de.html).

CAO, Javier. Medición de un SGSI: diseñando el cuadro de mandos. [En línea]. {12 de enero de 2011}. Disponible en Internet: (www.securityartwork.es/2011/01/12/medicion-de-un-sgsi-disenando-el-cuadro-de-mandos/)

CAO, Javier. Sistemas de Gestión Seguridad de la Información. Los malos 3, Los buenos 0. [En línea]. 2014. [Consultado 13 de diciembre, 2014]. Disponible en Internet: (sgsi-iso27001.blogspot.com.co/2014/06/ciberseguridad-minuto-y-resultado-los.html)

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria de 2012. (17 octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. [En línea]. Bogotá D.C.: Alcaldía de Bogotá. 2012. [Consultado el 23 de mayo, 2015]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

COMUNIDAD INTERNACIONAL DE IMPLANTADORES DE ISO27000 DE ISO27001SECURITY.COM. Consejos de implantación y métricas de ISO/IEC 27001 y 27002. Traducido por www.iso27000.es. [En línea] Versión 1, 16 p. 2007. [Consultado 26 de enero, 2014]. Disponible en Internet: (www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf)

CORLETTI, A. Análisis de ISO-27001:2005. [En línea], (abril 2006). [Consultado 06 de mayo de 2015]. Disponible en Internet: www.criptored.upm.es/guiateoria/gt_m292g.htm

DE LA CRUZ, César y VASQUEZ, Juan. Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT. Chiclayo: Universidad Católica Santo Toribio De Mogrovejo. [En línea], 2008, 160 p. Tesis de Grado Ingeniero De Sistemas y Computación. [Consultado 16 de diciembre, 2014]. Disponible en Internet: (cip.org.pe/imagenes/temp/tesis/42464064.doc)

DE LA CUESTA, Oscar. Herramientas para la implantación de un SGSI. [En línea]. 2015. [Consultado 16 de enero, 2015] Disponible en Internet: (www.palentino.es/blog/herramientas-para-la-implantacion-de-un-sgsi/)

ICONTEC “estándar Internacional ISO/IEC 27005:2008 Information Technology – Security techniques – Specification for an Information Security Managment System”

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS y CERTIFICACIÓN. Trabajos escritos: presentaciones y referencias bibliográficas. NTC 1486. Sexta actualización. Santafé de Bogotá, D.C.: ICONTEC, 2008

ISOTOOLS EXCELLENCE. SGSI. La norma ISO 27001:2013 ¿Cuál es su estructura? [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/)

ISOTOOLS EXCELLENCE. SGSI. Los pilares del SGSI. [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/07/pilares-sgsi/)

ISOTOOLS EXCELLENCE. SGSI. Por qué implantar un SGSI basado en la norma ISO 27001. [En línea]. 2015. [Consultado 18 de junio, 2015]. Disponible en Internet: (www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/)

GUTIÉRREZ, Camilo. Lo que no debes pasar por alto para gestionar la seguridad de la información. En: Revista.Seguridad. [En línea]. no.22 (ago-sep.2014). p.04-06. [Consultado 26 de enero, 2015]. Disponible en Internet: (revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Num22.pdf)

MENDOZA, Miguel y LORENZANA, Pablo. Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I. En: Revista.Seguridad. [En línea]. no.16, (Ene-Feb 2013). p. 13-17. . [Consultado 17 de diciembre, 2014]. Disponible en Internet: (revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Seguridad_Num16_0.pdf)

MERCHAN, R. Gestión De Proyectos De Seguridad De La Información. [En línea]. (s.f.) [15 de abril de 2015]. Disponible en internet: www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_Jornada_Gerencia/gestiondeproyectosdeseguridad.pdf

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. Políticas Generales de Seguridad de la Información. [En línea]. Ver.1. 9p. Bogotá, 2014. [Consultado 14 de junio, 2015]. Disponible en internet: (https://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/Politica_de_seguridad__definitiva___pdf.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. [En línea].Versión 2.0.2. 49p.Bogotá, 2011. [Consultado 15 de diciembre, 2014]. Disponible en Internet: (css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf)

PACHECO, Federico. La importancia de un SGSI. Welivesecurity en Español. [En línea].2010. [Consultado 14 de diciembre, 2014]. Disponible en Internet: (www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/)

PORTAL ISO 27001 EN ESPAÑOL. Origen serie 27K. [En línea]. [Consultado 28 de noviembre, 2014]. Disponible en internet: www.iso27000.es/iso27000.html

PORTAL ISO 27001 EN ESPAÑOL. Serie 27000.Evolución [en línea]. [Consultado 29 de noviembre, 2014]. Disponible en internet: www.iso27000.es/iso27000.html

SALCEDO, Robin. Plan de Implementación del SGSI basado en la Norma ISO 27001:2013. Memoria Trabajo Final Máster MISTIC. Barcelona: Universidad Oberte Catalunya. [En línea].2014. 43 p. [Consultado 13 de enero, 2015]. Disponible en Internet: (openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf)

ANEXOS

Anexo A Controles ISO 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Anexo B Lista de Chequeo

Elemento	Criterio / elementos	cumple SI/NO	Argumento
Título	Abarca el qué, el cómo y el dónde del tema de investigación de forma clara y concisa	SI	
	Mayúscula sostenida, en negrilla, sin punto al final	SI	
Delimitación del tema de estudio	Verificar limitaciones de tipo temporal, económico o de complejidad	SI	
	Pertinencia y relevancia del tema de estudio en el área en el que se desarrolla	SI	
	La realización de la investigación no implica riesgos para la seguridad del investigador, o el investigador es plenamente consciente de ellos y decide asumirlos	SI	Todo el desarrollo del trabajo se realiza en las instalaciónes de entidad.
Disponibilidad de la información	Es posible encontrar la suficiente información y asesoría respecto al tema en cuestión	SI	La seguridad informática es un tema que esta voga en las organizaciones, por lo tanto la documentación es amplia
Redacción	Adecuación textual	SI	
	Coherencia textual	SI	
	Cohesión textual	SI	
	Corrección gramatical	SI	
Ortografía	No se presentan errores ortográficos	SI	
Formulación del problema	Se hace una formulación clara y sin ambigüedades	SI	
	Evidencia la relación entre variables en un contexto temporal y espacial	SI	
Justificación	Argumenta las razones por las cuales se escogió el tema de estudio y evidencia su importancia	SI	
	Describe y argumenta claramente los beneficios al realizar el proyecto	SI	
	Grado de innovación del proyecto, su valor científico, académico o técnico.	SI	
Objetivo general	El objetivo general es coherente con la pregunta de investigación	SI	
Objetivos específicos	Representan metas parciales que llevan al cumplimiento del objetivo general	SI	
	Son realistas, no deben ser muy difíciles de cumplir.	SI	
	Redactados en orden cronológico (orden de cumplimiento)	SI	
Marco referencial	Marco teórico	SI	
	Marco contextual	SI	
	Marco legal	SI	Implicito en el marco teórico
	Otros marcos de referencia (si es necesario)	SI	
Diseño metodológico prelimina	Tipo de investigación	SI	
	Población, muestra, variables	SI	
	Técnicas de recolección de información	SI	
Recursos	Talento Humano	SI	
	Materiales y equipos	SI	
	Análisis de costos	NA	
	Fuentes de financiación	NA	
	Relación costo - beneficio	NA	
Cronograma	Establece los plazos de ejecución de las fases y actividades más relevantes del proyecto.	SI	
Bibliografía	Cantidad, calidad y relevancia de las fuentes	SI	
	Normatividad APA o ICONTEC	SI	
	Organizada en orden alfabético	SI	
	Funcionalidad de los enlaces, si los hay.	SI	
glosario (* opcional)	Si es necesario, se sugiere incluir un glosario con mínimo 10 términos relacionados con el tema de estudio		