SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADA AL ÁREA DE OPERACIONES DE UNA EMPRESA DE TELECOMUNICACIONES.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADA AL ÁREA DE OPERACIONES DE UNA EMPRESA DE TELECOMUNICACIONES.

DANIELA STEFANY BUITRAGO ROJAS
EDWARD LEONARDO ALVARADO ROMERO

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA
INGENIERÍA EN TELEMÁTICA

BOGOTÁ
2018

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADA AL ÁREA DE OPERACIONES DE UNA EMPRESA DE TELECOMUNICACIONES.

DANIELA STEFANY BUITRAGO ROJAS
EDWARD LEONARDO ALVARADO ROMERO

Proyecto presentado como requisito para optar al título de Ingeniería en Telemática

TUTOR:

MIGUEL ÁNGEL LEGUIZAMON PÁEZ
Ingeniero en Sistemas

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA
INGENIERÍA EN TELEMÁTICA

BOGOTÁ
2018

AGRADECIMIENTOS

Expresamos nuestros agradecimientos primero a Dios, el ser que nos da la oportunidad de vivir cada día en salud para cumplir las metas propuestas en nuestras vidas. A nuestros padres y familiares que dan la vida por ayudarnos a cumplir nuestras metas y que cada día nos dan fuerza para salir adelante y seguir luchando por nuestros ideales, a nuestros profesores por sus enseñanzas y orientación en cada etapa de nuestra carrera.

A nuestros compañeros y amigos que cada día nos apoyaron, nos motivaron y nos guiaron mostrándonos sus experiencias para así obtener mejores resultados y hacer posible este proyecto. Además un agradecimiento especial al Ingeniero
Miguel Ángel Leguizamón Páez quien con su experiencia, conocimiento y orientación nos ayudó a alcanzar los objetivos propuestos.

Agradezco primeramente a Dios por brindarme la oportunidad de lograr mis metas y de seguir formando mi camino, A mis padres por su esfuerzo y apoyo incondicional con el cual hicieron posible mi formación personal y académica, A mis hermanos quienes han estado hay siempre para apoyarme, Al profesor Miguel Ángel Leguizamón Páez quien guio este proyecto exitosamente y Finalmente a todos aquellos que de alguna manera u otra han contribuido directa o indirectamente en mi desarrollo como persona, estudiante y profesional.

Daniela

Expreso mi agradecimiento primeramente a Dios, por la vida que me dio por la familia que me brindo y por ayudarme a cumplir cada una de las metas como lo es el título universitario, a mis padres y hermanos que me apoyaron económicamente, afectivamente y moralmente en cada momento y paso de esta carrera, a cada uno de los profesores que brindaron su conocimiento, enseñanzas y orientación a un mejor camino y por ultimo un agradecimiento especial al profesor que apoyo este proyecto el Ingeniero Miguel Ángel Leguizamón quien oriento el proyecto que se llevó a cabo finalizándolo con éxito.

Leonardo

TABLA CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Las empresas de telecomunicaciones prestan diferentes servicios como lo son la telefonía, televisión de cable, internet entre otras, dichas empresas se encargan de renovar y actualizar la tecnología brindada a sus clientes, al ofrecer diferentes servicios posee gran cantidad de información la cual es vulnerable a robo, e inconsistencia en el manejo de datos de la infraestructura, En el año 2016 se evidencia durante un estudio realizado por IBM security que las empresas del sector de telecomunicaciones no cuentan con un control para la protección de la información y de los activos que interactúan con la operación, por ello se llevara a cabo el desarrollo de un manual de políticas de seguridad para vulnerabilidades y riesgos identificados, donde se definan los controles necesarios para mitigar los riesgos y vulnerabilidades ya nombrados además realizar una herramienta que permita monitorear e informar a los gerente de las áreas afectadas y al personal de calidad encargado sobre el estado de los controles definidos todo esto para el área de operaciones de las empresas de telecomunicaciones .

El proyecto mencionado se estimó con una investigación proyectiva basada en la metodología magerit y el marco de trabajo cobit para la mitigación de riesgos, vulnerabilidades y amenazas que se identificaron en el proyecto.

INTRODUCCION

En el presente documento se realizó un sistema de gestión de seguridad de la información con el objetivo de mitigar los riesgos y las vulnerabilidades que se identifican para las empresas de telecomunicaciones.
La característica principal del sistema de gestión es realizar controles que mitiguen los riesgos y vulnerabilidades que se identificaron, sin permitir fugas de información.
Para analizar esta problemática es necesario mencionar las causas. Una de ellas es el control inadecuado de la protección de la información, Donde se corre el riesgo de que la misma sea alterada, robada o interceptada ya que se no se tiene definida una manera concreta de condicionar el uso de dicha información.
La investigación de esta problemática se da debido a que se presentan inconsistencias en la información y en el control de activos en las áreas de operación de dichas empresas debido a que no se tiene un proceso definido lo cual permite alterar la integridad de la información y esto afecta la empresa en general.

En el ámbito profesional crece el interés de cómo definir el control de la protección de la información debido a los riesgos y las vulnerabilidades que se identificaron en la investigación del proyecto

El documento está conformado en ocho capítulos donde se va exponiendo cada una de las fases del proyecto, en el primer capítulo se encuentra la fase de definición, planeación y organización del proyecto, en el capítulo dos se encuentra el análisis de caso estudio, en el tercer capítulo se hace referencia al análisis de riesgos, el capítulo cuatro está compuesto de las políticas y controles de seguridad definidos en el capítulo cinco se expone el manual de políticas y controles, el capítulo seis está conformado por la definición de la metodología y el desarrollo que se llevó acabo en el prototipo, en el capítulo siete se encuentran las conclusiones y recomendaciones y por último el capítulo ocho consta de los anexos y bibliografía

CAPÍTULO I
FASE DE DEFINICIÓN, PLANEACIÓN Y ORGANIZACIÓN

1. FASE DE DEFINICIÓN, PLANEACIÓN Y ORGANIZACIÓN

1.1. TÍTULO

Sistema de gestión de seguridad de la información (SGSI) aplicada al área de operaciones de una empresa de telecomunicaciones.

1.2. PLANTEAMIENTO DEL PROBLEMA

Toda empresa del sector de las telecomunicaciones es vulnerable a los robos de información, e inconsistencias en el manejo de datos de infraestructura, filtraciones de registros, entre otros ataques ya que diariamente generan gran cantidad de información, lo cual puede afectar el área de operaciones de dichas empresas y la reputación de una organización, Esto quedó evidenciado en el estudio realizado por IBM Security en el año 2016 el cual arrojó que "las empresas del sector de la información y comunicación e instituciones gubernamentales sufrieron el mayor número de incidentes y registros atacados en 2016 (3.400 millones en el primer caso y 398 millones de registros filtrados en el caso de instituciones gubernamentales)"[1] ,Esto se debe a que no se cuenta con un control para la protección de la información y de los activos que interactúan con la operación.

Según **ESET Security Report Latinoamérica 2017 "**las empresas colombianas cada vez incrementan más el uso de la gestión de la seguridad y las prácticas más usadas son el mantenimiento de políticas de seguridad con un (74%), la realización de auditorías internas y/o externas con un (38%) y la clasificación de la información con un (31%),Si bien existe un leve incremento del 5% con respecto a 2015 en la cantidad de empresas latinoamericanas que utilizan políticas de seguridad, algunos indicadores despiertan dudas en relación a qué tan bien diseñadas se encuentran,Se consideró el tamaño de la empresa junto a las gestiones implementadas,se evidencia que el 17% de las pequeñas organizaciones, el 10% de las medianas y el 6% de las grandes no siguen ninguna de estas prácticas. Esto es muy preocupante, sobre todo cuando se debe tener en cuenta las consecuencias que puede conllevar para la protección del negocio. No obstante, estas cifras han disminuido en los últimos años, planteando un panorama esperanzador para el futuro**"**[2],Este estudio demuestra la importancia de seguir trabajando en la seguridad de la información en las compañías colombianas**.**

En vista de que no se está realizando el debido control de la información se está corriendo el riesgo de que la misma sea alterada, robada o interceptada ya que no se tiene definida una manera concreta de condicionar el uso de dicha información, lo cual representa un peligro para la empresa ya que la información tratada en el área específica es fundamental e importante para la continuidad del negocio, en la actualidad se evidencian irregularidades en el manejo de la información donde los datos proporcionados por la empresa en varias ocasiones no coincide con los que brinda la operación, destacando también que la información que maneja el área es

[1] https://colombiadigital.net/actualidad/noticias/item/9670-las-vulnerabilidades-y-filtracion-de-datos-siguen-fuera-de-control.html

[2] https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

de vital importancia ya que en ella se encuentra todos los productos a ofrecer por parte de la empresa y en caso de caer en manos equivocadas se puede filtrar la información de los clientes y los productos adquiridos, sin dejar de lado que se puede identificar las debilidades y fortalezas de la empresa en cuestiones de mercadeo.

Al haber vulnerabilidades y amenazas en la información se evidencia que no se están asegurando los principios de confidencialidad e integridad de la misma, lo cual puede ocasionar pérdida en la secuencia de procesos que internamente se llevan a cabo para un buen funcionamiento y control de activos.

1.3. FORMULACIÓN DEL PROBLEMA

¿Cómo fortalecer la seguridad de la información y de los activos en la gestión y tratamiento de los riesgos en la información tratada en las áreas de operaciones de las empresas de telecomunicaciones?

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

Elaborar un Sistema de Gestión de Seguridad de la información para el área de operaciones de empresas de telecomunicaciones.

1.4.2. OBJETIVOS ESPECÍFICOS

- Realizar el diagnóstico de la situación actual de la seguridad de la información para el caso estudio definido.
- Adelantar el análisis de riesgos usando metodologías que permitan identificar los peligros de la información para este tipo de empresas, basados en los conceptos de Magerit.
- Seleccionar políticas y controles de seguridad para el área de operaciones de empresas dedicadas al sector de las telecomunicaciones, basados en la normatividad ISO/IEC 27001.
- Desarrollar un manual basado en las políticas y controles seleccionados durante el desarrollo del caso estudio.
- Implementar un prototipo que permita presentar el trabajo desarrollado.

1.5. SOLUCIÓN TECNOLÓGICA

Como solución tecnológica para el estudio que se está llevando a cabo, se desarrollarán los eventos necesarios para implementar la infraestructura necesaria para el proyecto, teniendo en cuenta la metodología magerit y el marco de trabajo cobit para la mitigación de riesgos, vulnerabilidades y amenazas que tiene la información del estudio del proyecto que se está llevando a cabo.

Teniendo en cuenta lo ya descrito se tendrá en cuenta la norma Iso 27000 para realizar el respectivo manual de políticas de seguridad para las vulnerabilidades y

riesgos identificados donde se defina los controles necesarios para llevar a cabo la solución del proyecto, dicho manual contendrá, las políticas de seguridad del SGSI, Los controles que se deberán implementar para retroalimentar y evaluar, además de una propuesta económica que servirá como referente a la hora de implementar el SGSI .

Por último, se desarrollará un prototipo de aplicación web que permita consultar el trabajo desarrollado, el sitio web se encargará de mantener informado tanto al gerente, como al encargado del área de calidad de dichas empresas de cómo va el cumplimiento de los controles que se definieron para evaluar, esto lo hará mediante correo electrónico el cual se enviará cada vez que las estadísticas se encuentren por debajo de los umbrales establecidos. Para el desarrollo se usará el lenguaje de programación web java, el frameworkPrimeFaces y como motor de base de datos PostgreSQL, Se seleccionan estas tecnologías para el desarrollo ya que cuentan con cualidades como que son de código abierto, multiplataforma y cuentan con bastante soporte y documentación en internet, lo cual nos será de gran utilidad al momento de comenzar la etapa de desarrollo.

1.6. MARCO TEÓRICO

En vista de que la información se ha convertido en uno de los principales activos de las empresas hoy en día, se ha detectado que la seguridad de esta debe ser una de las prioridades dentro de cualquier organización y no dejando de lado otro factor importante como lo es el control de equipos en las empresas de telecomunicaciones, es por ello que en el presente proyecto se abordará esta temática para un mejor control en los activos mencionados.

Para ello tomará como referencia los siguientes proyectos que abordan temáticas similares, donde presentan las amenazas internas y externas a las que se exponen este tipo de organizaciones y de la misma manera establecen las mejores prácticas para la seguridad de la información, con el fin de poder minimizarlas aplicando los controles de la norma 27000 en los diferentes dominios, a continuación se relacionan los proyectos tomados como referencia:

1.6.1. Nombre Proyecto Referencia 1

Propuesta para la Planeación e Implementación de un SGSI basado en la ISO/IEC 27001:2005 para el área de operaciones de una empresa de telecomunicaciones, Desarrollado por Héctor Fernando Vargas Montoya para la universidad de UOC (UniversitatOberta de Catalunya) en el año 2014.

1.6.1.1. Alcance

El sistema de Gestión de Seguridad de la Información – SGSI comprende los sistemas de información que apoyan a los procesos para la operación de Telecomunicaciones: Gestión logística, Ventas y PRQ, Gestión del servicio y la operación, Gestión de la relación con proveedores, Gestión de inventario y gestión de la facturación y el recaudo, dichos procesos son apoyados por los sistemas de información CRM, OSM, Facturación y portal Web para el comercio electrónico, así

mismo el SGSI también comprenderá el proceso financiero y su sistema de información ERP. Éste alcance está delimitado por la declaración de aplicabilidad y la implementación de controles se limita por el posible presupuesto aprobado.

1.6.1.2. Resumen

El presente documento corresponde al Trabajo Final del Máster – TFM del "Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones- MISTIC" de la universitatOberta de Catalunya, Universitat Rovira i Virgili y la Universitat Autónoma de Barcelona, el cual se fundamenta en la propuesta de planeación y diseño de un sistema de gestión de seguridad SGSI así como la implementación de algunos de los elementos, basado en la norma ISO/IEC 27001:2005 y su anexo la ISO 27002, dicho proyecto está enmarcado para una empresa de telecomunicaciones en Colombia y estará proyectado acorde al alcance y la declaración de aplicabilidad.

1.6.1.3. Estado del arte

"Los incidentes de seguridad siempre van a existir sin importar los controles que implementan las organizaciones. Sin embargo poder tener claro cuáles son los incidentes más comunes en la empresa, permite orientar las inversiones en seguridad hacia las brechas que mayor impacto pueden generar en caso que un incidente se materialice. El estado del arte presentado en este proyecto presenta algunas experiencias muy similares en cuanto a las actividades principales abordadas para el establecimiento de un sistema de Gestión de Seguridad de Información que aportan en gran manera al análisis y desarrollo de este proyecto y del modelo a proponer.

El SGSI sigue el proceso/ciclo de Deming (Planear-Hacer-Verificar-Actuar) y dentro de éste marco de referencia, se pretende conocer el sector de las telecomunicaciones (y sus servicios asociados) y dar una aplicabilidad de lo que es la implantación de un SGSI en pro de la protección de la información. De igual manera, en la propuesta de implementación de controles se tendrán en cuenta la normatividad y legislación actual existente en Colombia, construyendo así un sistema basado en la mejora continua.[3]

1.6.1.4. Nombre Proyecto Referencia 2

Diseño de un sistema de gestión de seguridad de la información para la corporación nacional de telecomunicaciones CNT EP, agencia doral, Desarrollado por Molina Batallas, Luis Fernando, para la Universidad De Las Américas Facultad de Ingenierías y Ciencias Agropecuarias Ingeniería en Redes y Telecomunicaciones.

[3]Héctor Fernando Vargas Montoya.Propuesta para la Planeación e Implementación de un SGSI basado en la ISO/IEC 27001:2005 para una empresa de telecomunicaciones.universidad de UOC (UniversitatOberta de Catalunya) 2014 Disponible en:
<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/35841/18/hvargasmTFM0614memoria.pdf>

1.6.1.5. Alcance

El presente proyecto consiste en el diseño de un sistema de gestión de seguridad de la información, el mismo que inicia con la selección de la agencia regional que servirá como caso de estudio, se realizará un análisis del estado actual de la seguridad de la información de la matriz seleccionada, tomando como referencia la norma NTE INEN-ISO/IEC 27001 se seleccionarán los procesos a ser aplicados considerando las principales necesidades identificadas anteriormente, finalmente se demostrara y evaluará la funcionalidad y viabilidad del sistema de gestión propuesto para verificar si este es adaptable al requerimiento de la empresa que es disponer de mayor seguridad en la información que la misma maneja. Consecuentemente la implementación y la mejora del mismo está sujeto al criterio de la empresa, por lo tanto, esto está fuera del alcance del presente proyecto.

1.6.1.6. Introducción

Los términos y definiciones que a continuación se detallarán se toman en base al requerimiento y objetivos del actual proyecto, en nuestro caso se busca diseñar un sistema de gestión de la seguridad de la información por lo que el marco teórico tiene fundamentos en base a la norma aplicada en el proyecto que es la INEN-ISO/IEC 27001:2012, esta norma detalla los fundamentos teóricos necesarios para comprender la administración de un sistema de seguridad de la información.

1.6.1.7. Justificación

Actualmente varias entidades públicas a nivel nacional han estado expuestas ataques graves de extracción de la información, dando como resultado serios perjuicios para las entidades. El motivo principal es la falta de políticas, normas y controles para la protección de la información vital. Por lo tanto el presente proyecto busca diseñar un sistema de gestión de seguridad de la información, tomando en cuenta los problemas anteriormente mencionados y el estado actual de seguridad de las entidades públicas, teniendo un lineamiento base para que otras instituciones utilicen esta gestión para mejorar su seguridad institucional.[4]

Además de los proyectos ya mencionados, se deben considerar algunos conceptos relacionados con la seguridad de la información, esto con el fin de tener un soporte teórico, que permita sustentar y dar respuesta a los requerimientos del proyecto.

1.6.2. Seguridad de la información

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de

[4] http://dspace.udla.edu.ec/bitstream/33000/6052/1/UDLA-EC-TIRT-2016-22.pdf

información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen.[5]

1.6.3. Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información ISO 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.

Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Entre dichos términos existen pequeñas diferencias, dichas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración.

La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

- Electrónicos
- En papel
- Audio y vídeo, etc.

Los gobiernos, las instituciones financieras, los hospitales y las organizaciones privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, etc. La mayor parte de esta información es reunida, tratada, almacenada y puesta a disposición de las personas que deseen revisarla.

Si se da el caso de que información confidencial de la organización, de sus clientes, de sus decisiones, de sus cuentas, etc. caen en manos de la competencia, esta se hará pública de una forma no autorizada y esto puede suponer graves consecuencias, ya que se perderá credibilidad de los clientes, se perderán posible negocios, se puede enfrentar a demandas e incluso puede causar la quiebra de la organización.

Es por todo esto que se convierte en una necesidad proteger la información confidencial, ya que es un requisito del negocio, y en muchos casos se convierte en algo ético y una obligación legal.

Para una persona normal, la Seguridad de la Información puede provocar un efecto muy significativo ya que puede tener diferentes consecuencias la violación de su privacidad dependiendo de la cultura del mismo.

[5] https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

La Seguridad de la Información ha crecido mucho en estos últimos tiempos, además ha evolucionado considerablemente. Se ha convertido en una carrera acreditada mundialmente. Dentro del éste área se ofrecen muchas especializaciones que se pueden incluir al realizar la auditoría del Sistema de Gestión de Seguridad de la Información ISO-27001, como pueden ser:

- Planificación de la continuidad de negocio
- Ciencia forense digital
- Administración de Sistemas de Gestión de Seguridad

Realizar correctamente la Gestión de la Seguridad de la Información quiere establecer y mantener los programas, los controles y las políticas de seguridad que tienen la obligación de conservar la confidencialidad, la integridad y la disponibilidad de la información de la empresa.

- **Confidencialidad**: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
- **Integridad:** es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
- **Disponibilidad**: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.[6]

1.6.4. SGSI

El SGSI (Sistema de Gestión de Seguridad de la Información) es el principal concepto sobre el que se conforma la norma ISO 27001.

La gestión de la Seguridad de la Información se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa.

1.6.4.1. ¿Qué es un SGSI?

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System.

Se puede entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

[6] http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

1.6.4.2. Fundamentos:

Para garantizar que el Sistema de Gestión de Seguridad de la Información gestionado de forma correcta se tiene que identificar el ciclo de vida y los aspectos relevantes adoptados para garantizar su:

- Confidencialidad: la información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizados.
- Integridad: mantener de forma completa y exacta la información y los métodos de proceso.
- Disponibilidad: acceder y utilizar la información y los sistemas de tratamiento de la misma parte de los individuos, entidades o proceso autorizados cuando lo requieran.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un SGSI.

1.6.4.3. Utilización

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa. La confidencialidad, integridad y disponibilidad de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurarse de que haya beneficios económicos.

Las empresas y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas que aprovechan cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques, espionajes, vandalismo, etc. Los virus informáticos o los ataques son ejemplos muy comunes y conocidos, pero también se deben asumir los riesgos de sufrir incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente desde dentro de la propia empresa o los que son provocados de forma accidental por catástrofes naturales.

El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El nivel de seguridad que se alcanza gracias a los medios técnicos es limitado e insuficiente por sí mismo. Durante la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la gerencia al frente, tomando en consideración a los clientes y a los proveedores de la organización.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Para entender que es SGSI, ayuda a establecer la política de seguridad y los procedimientos en relación a los objetivos de negocio de la empresa, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

1.6.4.4. Beneficios

- Establecer una metodología de Gestión de la Seguridad estructurada y clara.
- Reducir el riesgo de pérdida, robo o corrupción de la información sensible.
- Los clientes tienen acceso a la información mediante medidas de seguridad.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los clientes y los socios de la organización.
- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la organización a nivel internacional mejora.
- Aumenta la confianza y las reglas claras para las personas de la empresa.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

La documentación mínima que se debe tener en cuenta a la hora de implementar un SGSI:

- Política y objetivos de seguridad.
- El alcance del SGSI.
- Los procedimientos y los controles que apoyan al SGSI.
- Describir toda la metodología a la hora de realizar una evaluación de riesgo.
- Generar un informe después de realizar la evaluación de riesgo.
- Realizar un plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Declaración de aplicabilidad.
- Procedimiento de gestión de toda la documentación del SGSI.[7]

1.6.5. METODOLOGÍA PDCA – CICLO DEMING

La metodología PDCA o **ciclo Planificación – Ejecución – Evaluación – Actuación** o **secuencia Planificación – Ejecución – Evaluación – Actuación** (en inglés ,**PDCA** , de ***Plan-Do-Check-Act***) es una secuencia cíclica de actuaciones

[7] http://www.pmg-ssi.com/2015/07/que-es-sgsi/

que se hacen a lo largo del ciclo de vida de un servicio o producto para planificar su calidad, en particular en la mejora continua.

1.6.5.1. ETAPAS

Como su nombre indica, consiste en cuatro etapas que hay que hacer de forma sucesiva y en un cierto orden, por lo que cada una de ellas tiene una anterior y una posterior. Este ciclo no se acaba sino que hay que seguir indefinidamente. Las actuaciones son las següentes: [1]

- **P** (de *Plan* ,**Planificación**): Incluye, entre otras actividades, la definición de objetivos y de medidas para alcanzarlos, la definición y asignación de personas responsables , y la definición de los medios, recursos económicos y materiales necesarios. [1]
- **D** (de *Do* ,**Ejecución**): Es poner en práctica lo escogido a **P** . Incluye la formación, educación y entrenamiento del personal escogido en **P** .[1]
- **C** (de *Check* ,**Evaluación**): Comparación, análisis y evaluación de los resultados reales obtenidos en **D** con los esperados a **P**. hay que insistir en que los resultados finales no son suficientes y que se han de comparar los datos que sean necesarios en cada una de las etapas, movimientos y en cada uno de los elementos definidos en **P** , que deben aportar toda la información necesaria. [1]
- **A** (de *Act* ,**Actuación**): Si los elementos definidos en **P** no son lo suficientemente buenos o son insuficientes, habrá que modificarlos para la próxima vez. La fase de actuación es necesaria para corregir los aspectos negativos obtenidos en **C** y puede implicar la modificación de **P** . En cualquier caso, lo que se haya aprendido a **A** debe utilizarse con las conclusiones e informaciones previas que ya teníamos, para empezar de nuevo, a continuación, un **P** , y renovar así el ciclo. Es muy importante no detenerse en **A** ni quedarse con el antiguo **P** , sino empezar verdaderamente un nuevo ciclo constantemente.

1.6.6. PASOS DEL CICLO PDCA

1.6.6.1. PLAN

Establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los proyectados (objetivos o metas). Para determinar el resultado de la confianza, la integridad y exactitud de la especificación es también una parte de la mejora a mejorar. Cuándo puede comenzar a pequeña escala para probar los posibles efectos.

1.6.6.2. DESARROLLAR

Implementar el plan, ejecutar el proceso, hacer el producto. Recopilar datos para el mapeo y análisis de los próximos pasos “salida” y “set”. Por lo que este paso genera mucho cuidado porque no puede ser la causa raíz.

1.6.6.3. CHECK/EVALUACIÓN

Los resultados del estudio (medidos y recopilados en el paso anterior “Reproducir”) y compararlo con los resultados esperados (objetivos establecidos en el “plan” paso) para determinar cualquier diferencia.

Búsqueda de desviaciones sobre todo en la aplicación del plan y también mira la adecuación y el alcance del plan permite la ejecución de la etapa siguiente, es decir, “ACT”.

Gráficos de datos pueden hacer esto mucho más fácil ver tendencias a lo largo de varios ciclos PDCA y así convertir los datos recogidos en información. La información es lo que necesita para el siguiente paso “Ajuste”.

1.6.6.4. EL APALANCAMIENTO/SET/LEY

Tomar acciones correctivas sobre las diferencias entre los datos reales y previstas. Analizar las diferencias para determinar sus causas. Determinar dónde para aplicar los cambios que incluyen la mejora del proceso o producto.

Cuando un pase a través de estos cuatro pasos no dan lugar a la necesidad de alguna mejora, el método al que se aplica PDCA puede ser refinado con mayor detalle en la siguiente iteración del ciclo, o la atención debe ser colocado en una forma diferente en cualquier etapa del proceso.

El plan de PDCA cuando se aplica con el Sistema de Gestión de Calidad puede implementar acciones para lograr la mejora continua, garantizar el funcionamiento y el control de los procesos de producción.

En el Sistema de Gestión de Calidad que podemos encontrar los no – conformidades en los procesos, para tratar de no – plan de cumplimiento utilizó el PDCA .Acción para eliminar una no identificado en consecuencia.

Plan de acción correctiva de acción para eliminar la causa de una no – existente de línea, para eliminar o reducir la posibilidad de que vuelva a producirse el no.

Cumplimiento de medidas preventivas plan de acción para eliminar la causa de una no conformidad potencial, para eliminar o reducir la posibilidad de este no – plan de acción de mejora del cumplimiento de acción para implementar mejoras en los procesos continuos. La apertura de un plan de acción PDCA.

El plan de medidas preventivas o correctivas o de mejora están abiertos a considerar la determinación de las causas y las acciones propuestas, con la supervisión de análisis crítico siempre que haya.[8]

[8] http://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/

1.6.7. COBIT

Su sigla en ingles se refiere a Control ObjectivesforInformation and RelatedTechnology y es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992.

Cobit es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. Cobit permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Cobit enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de Cobit.

El propósito de Cobit es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan. Cobit permite entender cómo dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. Cobit suministra las herramientas para supervisar todas las actividades relacionadas con IT.

1.6.7.1. Qué ventajas ofrece Cobit:

- Cobit es un marco de referencia aceptado mundialmente de gobierno IT basado en estándares y mejores prácticas de la industria. Una vez implementado, es posible asegurarse de que IT se encuentra efectivamente alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas.
- Suministra un lenguaje común que le permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales.
- Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de IT. El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada.
- Ayuda a los ejecutivos a entender y gestionar las inversiones en IT a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que IT entregara los beneficios esperados.

La diferencia entre compañías que gestionan adecuadamente sus recursos IT y las que no es enorme. Cobit permite el desarrollo de políticas claras y buenas prácticas para la gestión de IT. Su marco de referencia permite gestionar los riesgos de IT y asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Al ser Cobit reconocida y aceptada internacionalmente como una herramienta de gestión, su implementación es un indicativo de la seriedad de una organización. Ayuda a Empresas y profesionales de IT a demostrar su competitividad ante las demás compañías. Así como existen procesos genéricos de muchos tipos de negocios, existen estándares y buenas prácticas específicos para IT que deben

seguirse por las compañías cuando se soportan en IT, en donde Cobit agrupa tales estándares y entrega un marco de referencia para su implementación y gestión.

Una vez se identifican e implementan los principios relevantes de Cobit para una compañía, se obtiene plena confianza en que todos los recursos de sistemas están siendo gestionados efectivamente.

1.6.7.2. Qué resultados se obtienen al implementar Cobit?

- El ciclo de vida de costos de IT será más transparente y predecible.
- IT entregará información de mayor calidad y en menor tiempo.
- IT brindará servicios con mayor calidad y todos los proyectos apoyados en IT serán más exitosos.
- Los requerimientos de seguridad y privacidad serán más fácilmente identificados, y su implementación podrá ser más fácilmente monitoreada.
- Todos los riesgos asociados a IT serán gestionados con mayor efectividad.
- El cumplimiento de regulaciones relacionadas a IT serán una práctica normal dentro de su gestión.

El marco de referencia Cobit en su versión 4 (a Julio de 2010), incluye lo siguiente:

- Marco de referencia: explica cómo Cobit organiza la Gestión de IT, los objetivos de control y buenas prácticas del negocio por dominios y procesos de IT, relacionándolos directamente con los requerimientos del negocio. Este marco de referencia contiene un total de 34 niveles de objetivos de control, uno por cada proceso de IT, agrupados en cuatro dominios: Planeamiento y Organización, Adquisición e Implementación, Desarrollo y Soporte y Monitoreo y Evaluación (*Que tal la coincidencia con el ciclo PHVA de las Normas ISO?*)
- Descripción de procesos: Incluida para cada uno de los 34 procesos de IT, cubriendo todas las áreas y responsabilidades de IT de principio a fin.
- Objetivos de Control: Suministra objetivos de gestión basados en las mejores prácticas para los procesos de IT.
- Directrices de Gestión: Incluye herramientas para ayudar a asignar responsabilidades y medir desempeños.
- Modelos de madurez: proporciona perfiles de los procesos de IT describiendo para cada uno de ellos un estados actual y uno futuro.

1.6.7.3.Cobit 5:

Programado para salir en el 2011, Cobit 5 consolidara los marcos de referencia de Cobit 4.1, Val IT 2.0 (inversiones en TI) y riesgos en IT, aprovechando también el modelo de negocio de Seguridad de la Información (IMC) y ITAF.[9]

[9] http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

1.6.8. ISO/IEC 27001

1.6.8.1. Origen de la norma

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1 (JointTechnicalCommittee 1). 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 como norma internacional requiere la aprobación de, por lo menos, el 75% de los organismos nacionales que emiten su voto. La Norma Internacional ISO/IEC 27002 fue preparada inicialmente por el Instituto de Normas Británico (como BS 7799), y adoptada bajo la supervisión del subcomité de técnicos de seguridad del comité técnico ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales miembros de ISO e IEC. Una vez que fue publicada la Norma ISO/IEC 17799-1 (actualmente se corresponde con la Norma ISO/IEC 27002), Reino Unido (BSI) y España (AENOR) elevaron al comité internacional sus normas nacionales sobre las especificaciones de los sistemas de gestión de la seguridad de la información (SGSI), BS 7799-2 y UNE 71502 respectivamente, siendo estas normas el origen de lo que finalmente acabo publicándose como norma internacional ISO/IEC 27001 en el año 2005, que fue adoptada como norma española UNE-ISO/IEC 27001 en el año 2007, tras un periodo de convivencia con la norma anteriormente mencionada. Actualmente, tanto la norma ISO/IEC 27001 como la ISO/IEC 27002 están en proceso de revisión internacional, y se espera que se publiquen las nuevas versiones a lo largo del año 2013. Como se ha comentado anteriormente, este estándar internacional adopta también el modelo Plan-Do-Check-Act (PDCA), es decir, se basa en un ciclo de mejora continua que consiste en planificar, desarrollar, comprobar y actuar en consecuencia con lo que se haya detectado al efectuar las comprobaciones. De esta manera se conseguirá ir refinando la gestión, haciéndola más eficaz y efectiva.

1.6.8.2. Objeto y campo de aplicación de la norma

La Norma ISO/IEC 27001, como el resto de las normas aplicables a los sistemas de gestión, está pensada para que se emplee en todo tipo de organizaciones (empresas privadas y públicas, entidades sin ánimo de lucro, etc.), sin importar el tamaño o la actividad. Esta norma especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de

la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis. Puede ejecutarse con una herramienta comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno. Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente. [10]

1.6.9. MAGERIT

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

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

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

MAGERIT persigue los siguientes objetivos:Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.6.10. JAVA

Java es un lenguaje de programación con el que podemos realizar cualquier tipo de programa. En la actualidad es un lenguaje muy extendido y cada vez cobra más

10

https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1502520656&Signature=RrgRD0Fjfpbb3AxncrC3U4I5oXI%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22994_1.pdf

importancia tanto en el ámbito de Internet como en la informática en general. Está desarrollado por la compañía Sun Microsystems con gran dedicación y siempre enfocado a cubrir las necesidades tecnológicas más punteras.

Una de las principales características por las que Java se ha hecho muy famoso es que es un lenguaje independiente de la plataforma. Eso quiere decir que si se desarrolla un programa en Java podrá funcionar en cualquier ordenador del mercado. Es una ventaja significativa para los desarrolladores de software, pues antes tenían que hacer un programa para cada sistema operativo, por ejemplo Windows, Linux, Apple, etc. Esto lo consigue porque se ha creado una Máquina de Java para cada sistema que hace de puente entre el sistema operativo y el programa de Java y posibilita que este último se entienda perfectamente.

La independencia de plataforma es una de las razones por las que Java es interesante para Internet, ya que muchas personas deben tener acceso con ordenadores distintos. Pero no se queda ahí, Java está desarrollándose incluso para distintos tipos de dispositivos además del ordenador como móviles, agendas y en general para cualquier cosa que se le ocurra a la industria.[11]

1.6.10.1. PRIMEFACES

PrimeFaces es una librería de componentes visuales open source desarrollada y mantenida por Prime Technology, una compañía Turca de IT especializada en consultoría ágil, JSF, Java EE y Outsourcing. El proyecto es liderado por ÇağatayÇivici, un miembro del "JSF ExpertGroup" (y forofo del Barça). Las principales características de Primefaces son:

- soporte nativo de Ajax, incluyendo Push/Comet.
- kit para crear aplicaciones web para móviles.
- es compatible con otras librerías de componentes, como JBossRichFaces.
- uso de javascript no intrusivo (no aparece en línea dentro de los elementos, sino dentro de un bloque <script>).
- es un proyecto open source, activo y bastante estable entre versiones.

Algunos inconvenientes podrían ser:

- para utilizar el soporte de Ajax tenemos que indicarlo explícitamente, por medio de atributos específicos de cada componente.
- no podemos utilizar el soporte de Ajax de JSF 2 (mediante <f:ajax>) con los componentes de Primefaces.[12]

[11] https://docs.google.com/document/d/1Sv0I1iGAr85ysjfLlW07m-PZ5vXN1NEzqBaY14w0bWQ/edit#
[12] https://www.adictosaltrabajo.com/tutoriales/introduccion-primefaces/

1.6.11. POSTGRESQL

PostgreSQL es un potente sistema de base de datos objeto-relacional de código abierto. Cuenta con más de 15 años de desarrollo activo y una arquitectura probada que se ha ganado una sólida reputación de fiabilidad e integridad de datos. Se ejecuta en los principales sistemas operativos que existen en la actualidad como:

- Linux
- UNIX (AIX, BSD, HP-UX, SGI IRIX, Mac OS X, Solaris, Tru64)
- Windows

Es totalmente compatible con ACID, tiene soporte completo para claves foráneas, uniones, vistas, disparadores y procedimientos almacenados (en varios lenguajes). Incluye la mayoría de los tipos de datos del SQL 2008, incluyendo INTEGER, numérico, BOOLEAN, CHAR, VARCHAR, DATE, INTERVAL, y TIMESTAMP. También soporta almacenamiento de objetos binarios grandes, como imágenes, sonidos o vídeo. Cuenta con interfaces nativas de programación para C / C + +, Java,.Net, Perl, Python, Ruby, Tcl, ODBC, entre otros, y la documentación que actualmente existe es realmente excepcional.
Una base de datos de clase empresarial, PostgreSQL cuenta con características avanzadas tales como Multi-Version Control de concurrencia (MVCC), puntos en tiempo de recuperación, tablespaces, replicación asincrónica, transacciones anidadas (savepoints), respaldos online/hot, un sofisticado queryplanner/optimizer. Soporta el conjunto de caracteres internacional, codificaciones de caracteres multibyte, Unicode, mayúsculas y minúsculas.
Es altamente escalable, tanto en la enorme cantidad de datos que puede manejar y en el número de usuarios concurrentes que puede administrar. Hay sistemas activos en PostgreSQL en entornos de producción que manejan más de 4 terabytes de datos. Algunos límites y características generales que se incluyen en PostgreSQL son:

Tamaño máximo de la Base de datos	Ilimitado
Tamaño máximo de la tablas	32 TB
Tamaño máximo de la fila	1.6 TB
Tamaño máximo para cada campo	1 GB
Máximo de filas por tabla	Ilimitado
Máximo de columnas por tabla	250-1600 dependiendo del tipo de columna

Máximo de índices por tabla	Ilimitado

1.6.11.1. Altamente personalizable

En PostgreSQL puedes escribir procedimientos almacenados en más de una docena de lenguajes como:

- Java
- Perl
- Python
- Ruby
- Tcl
- C / C ++
- PL / pgSQL (que es similar a PL / SQL de Oracle)

Incluye una biblioteca de funciones estándar con cientos de funciones integradas que van desde las operaciones matemáticas básicas, operaciones con strings para criptografía y compatibilidad con Oracle. Los disparadores (triggers) y procedimientos almacenados pueden ser escritos en C y se cargan en la base de datos como una biblioteca, lo cual permite una gran flexibilidad y ampliación de sus capacidades. Del mismo modo, PostgreSQL incluye un framework que permite a los desarrolladores definir y crear sus propios tipos de datos personalizados. Como resultado, una gran cantidad de tipos de datos avanzados se han creado que van desde los geométricos y espaciales para direcciones de red, incluso para los tipos de datos ISBN / ISSN (International Standard Book Number / Número Internacional Normalizado de Publicaciones Seriadas), los cuales pueden ser opcionalmente agregados al sistema.
Así como hay muchos lenguajes de procedimientos soportados en PostgreSQL, también existen muchas librerias de interfaces, lo que permite que varios lenguajes sean tanto compilados e interpretados a la interfaz con PostgreSQL. Hay interfaces para Java (JDBC), ODBC, Perl, Python, Ruby, C, C + +, PHP, Lisp, Scheme, y Qt sólo por mencionar algunos.
Lo mejor de todo, el código fuente de PostgreSQL está disponible bajo una licencia de código abierto: la licencia de PostgreSQL. Esta licencia le da la libertad para usar, modificar y distribuir PostgreSQL en cualquier forma que guste ya sea de código abierto o cerrado. Como tal, PostgreSQL no es sólo un sistema de base de datos de gran alcance capaz de usarse en las empresas, es todo una plataforma de desarrollo sobre la cual puedes desarrollar todo tipo de software que requieren un RDBMS de grandes capacidades.[13]

[13] https://microbuffer.wordpress.com/2011/05/04/que-es-postgresql/

1.6.12. METODOLOGÍAS DE DESARROLLO DE SOFTWARE

1.6.12.1. SCRUM

Es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado posible de un proyecto. Estas prácticas se apoyan unas a otras y su selección tiene origen en un estudio de la manera de trabajar de equipos altamente productivos.

En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales.

Scrum también se utiliza para resolver situaciones en que no se está entregando al cliente lo que necesita, cuando las entregas se alargan demasiado, los costes se disparan o la calidad no es aceptable, cuando se necesita capacidad de reacción ante la competencia, cuando la moral de los equipos es baja y la rotación alta, cuando es necesario identificar y solucionar ineficiencias sistemáticamente o cuando se quiere trabajar utilizando un proceso especializado en el desarrollo de producto.[14]

1.6.12.2. EL PROCESO

En primer lugar se define el ProductBacklog, lo que nos permitirá realizar nuestros Sprints más adelante.

- **ProductBacklog**: Es una **"wishlist" sobre las funcionalidades del producto**. Es elaborado por el ProductOwner y las funciones están priorizadas según lo que es más y menos importante para el negocio. El objetivo es que el ProductOwner responda la pregunta **"¿Qué hay que hacer?"**.
- **Sprint Backlog:** Es un subconjunto de ítemes del ProductBacklog, que son seleccionados por el equipo para realizar durante el Sprint sobre el que se va a trabajar**.** El **equipo establece la duración de cada Sprint.**
- **Sprint Planning Meeting:** Esta reunión se hace al comienzo de cada**Sprint**ysedefine cómo se va a enfocar el proyecto que viene del ProductBacklog las etapas y los plazos. **Cada Sprint está compuesto por diferentes features**. Por ejemplo, decidimos que los features del primer Sprint son: diseño del logo, definición colores y contenido multimedia.
- **DailyScrum o Stand-up Meeting:** Es una **reunión breve** que se realiza a diario mientras dura el periodo de Sprint. Se responden individualmente tres preguntas: **¿Qué hice ayer?, ¿Qué voy a hacer hoy?, ¿Qué ayuda**

[14] https://proyectosagiles.org/que-es-scrum/

necesito? El Scrum Master debe tratar de solucionar los problemas u obstáculos que se presenten.

- **Sprint Review**: Se revisa el **sprint terminado**, y ya debería haber un avance claro y tangible para presentárselo al cliente.
- **Sprint Retrospective: El equipo** revisa los **objetivos cumplidos** del Sprint terminado. Se anota lo bueno y lo malo, para no volver a repetir los errores. Esta etapa sirve para implementar mejoras desde el punto de vista del proceso del desarrollo.

Figura 1. El proceso Scrum

1.6.12.3. PARTICIPANTES

- ProductOwner: Habla por el cliente, y asegura que el equipo cumpla las expectativas. Es “el jefe” responsable del proyecto.
- Scrum Master: Lidera las reuniones y ayuda al equipo si es que tienen problemas. Además, minimiza los obstáculos para cumplir el objetivo del Sprint, es un “facilitador” pero no es un gestor.
- ScrumTeam: Son los encargados de desarrollar y cumplir lo que les asigna el ProductOwner.
- Cliente: Recibe el producto y puede influir en el proceso, entregando sus ideas o comentarios respecto al desarrollo.[15]

[15] http://www.i2btech.com/blog-i2b/tech-deployment/para-que-sirve-el-scrum-en-la-metogologia-agil/

1.7. METODOLOGÍA

Para el desarrollo de este proyecto se utilizara el ciclo Deming o también nombrado ciclo PHVA(Planear ,hacer, verificar y actuar), complementandolo con la metodología Magerit para el análisis y la gestión de riesgos y por último se va a utilizar el marco de trabajo Cobit para establecer las políticas de seguridad y el seguimiento que se va a llevar a cabo de las mismas.

Ciclo Deming: ya que es considerada una de las principales herramientas para implementar una mejora continua en cualquier proyecto, además está metodología permitirá diseñar una arquitectura para la creación del sistema de gestión de seguridad de la información (SGSI),además de esto permite aplicar a cualquiera de los sistemas de gestión
considerados, ya sea ISO 9001, ISO 14001 o OHSAS 18001, ya que en cierta medida todos y cada uno de los procesos de gestión de los servicios deben adoptar y reproducir, esta estructura para asegurar que cada una de estas fases se encuentra correctamente documentada.

1.7.1. PLANIFICACIÓN

Durante esta etapa se realizará el levantamiento información donde se identifiquen los procesos que se manejan en el área de operaciones para que posteriormente se pueda hacer el análisis y la evaluación de riesgos, teniendo en cuenta el impacto de cada uno de estos y las consecuencias que podría generar, con el objetivo de poder definir la manera en que se debe tratar cada uno.

1.7.2. HACER

Durante esta etapa y con la información obtenida en la fase anterior se lleva a cabo el plan de acción del tratamiento que se le va dar a cada uno de los riesgos, que se identificaron durante la etapa anterior para la mitigación de los mismos.

1.7.3. VERIFICAR

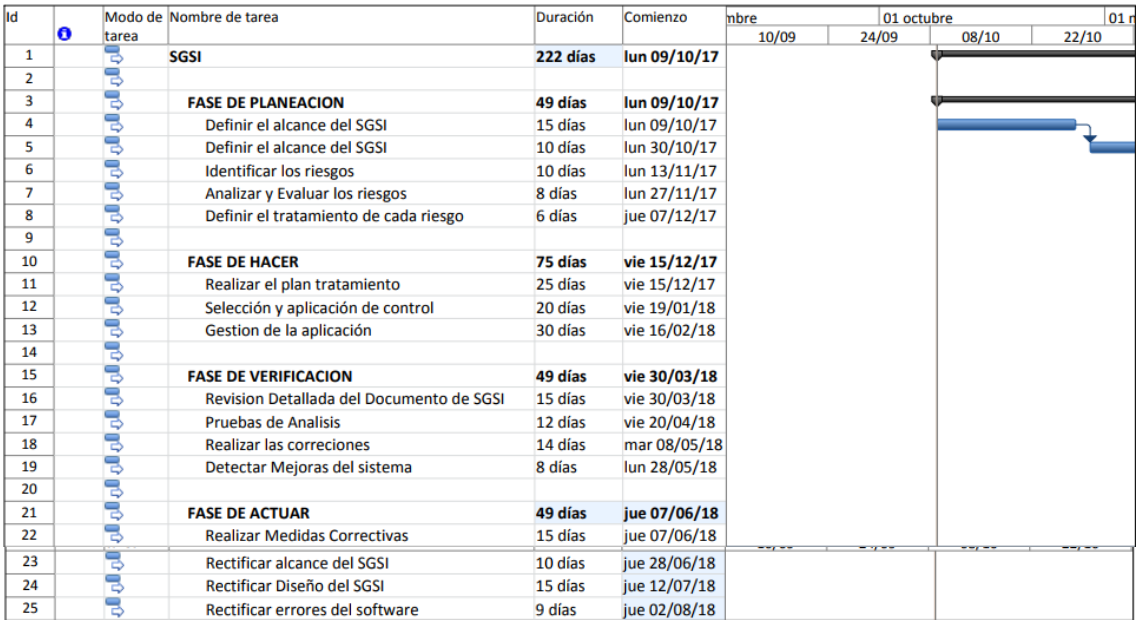
Durante esta etapa se hará una revisión de los controles implementados para cada uno de los riesgos identificados, mediante algunas pruebas, para así poder detectar las mejoras que necesite el sistema y poder hacer las respectivas correcciones.

1.7.4. ACTUAR

Durante esta etapa se ratifica el alcance del sgsi y su diseño en cada uno de los controles de los riesgos identificados, mediante la aplicación de medidas correctivas, donde se pueda dar utilización de nuevos controles, la modificación de los ya existentes o la eliminación de los que puedan ser obsoletos.

1.8. CRONOGRAMA

Figura 2. Cronograma



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		**SGSI**	**222 días**	**lun 09/10/17**
2				
3		**FASE DE PLANEACION**	**49 días**	**lun 09/10/17**
4		Definir el alcance del SGSI	15 días	lun 09/10/17
5		Definir el alcance del SGSI	10 días	lun 30/10/17
6		Identificar los riesgos	10 días	lun 13/11/17
7		Analizar y Evaluar los riesgos	8 días	lun 27/11/17
8		Definir el tratamiento de cada riesgo	6 días	jue 07/12/17
9				
10		**FASE DE HACER**	**75 días**	**vie 15/12/17**
11		Realizar el plan tratamiento	25 días	vie 15/12/17
12		Selección y aplicación de control	20 días	vie 19/01/18
13		Gestion de la aplicación	30 días	vie 16/02/18
14				
15		**FASE DE VERIFICACION**	**49 días**	**vie 30/03/18**
16		Revision Detallada del Documento de SGSI	15 días	vie 30/03/18
17		Pruebas de Analisis	12 días	vie 20/04/18
18		Realizar las correciones	14 días	mar 08/05/18
19		Detectar Mejoras del sistema	8 días	lun 28/05/18
20				
21		**FASE DE ACTUAR**	**49 días**	**jue 07/06/18**
22		Realizar Medidas Correctivas	15 días	jue 07/06/18
23		Rectificar alcance del SGSI	10 días	jue 28/06/18
24		Rectificar Diseño del SGSI	15 días	jue 12/07/18
25		Rectificar errores del software	9 días	jue 02/08/18

Fuente:Autores

1.9. FACTIBILIDAD ECONÓMICA

A Continuación se describe la factibilidad económica del proyecto ,lo que se necesita son mínimo dos equipos de trabajo, papelería para realizar el modelado del proyecto, acceso a Internet y asesorías de los tutores del proyecto.

En las siguientes tablas se presentarán la factibilidad económica, identificando los costos de papelería, hardware, software y recursos humanos necesarios para la realización del proyecto que se propone.

Se dividió en tres aspectos:

- recursos humanos
- recursos técnicos
- otros recursos

La distinción de los recursos humanos se presenta en la **Tabla 1**, Aquí se presenta las asesorías que se tendrán y los gastos de los analistas.

Tabla 1 Factibilidad Económica Recursos Humanos

Tipo	Descripción	Valor-Hora	Cantidad	Total
Tutor	Asesorías para la realización del proyecto, referente a la metodología.	$ 40.000	200	$ 8.000.000
Analistas	Dos analistas que realicen el SGSI.	$ 30.000	8 horas semanales	$ 7.680.000
Total Recursos Humanos				$ 15.680.000

Fuente:Autores

En la **Tabla 2** se presentarán los gastos de los recursos técnicos, que se presentarán en el desarrollo del proyecto.

Tabla 2 FactibilidadEconómicaRecursosTécnicos

Recurso	Descripción	Valor Unitario	Cantidad	Total
Computadores	Equipos de escritorio para la realización del documento SGSI.	$ 2.000.000	2	$ 4.000.000
Total Recursos Técnicos				$ 4.000.000

Fuente:Autores

En la **Tabla 3** se muestran los gastos adicionales, que serán solventados por desarrolladores del proyecto.

Tabla 3 FactibilidadEconómicaCosto Total

Recurso	Valor
Total Recursos Humanos	$15.680.000
Total Recursos Técnicos	$4.000.000
Total Otros recursos	$200.000
SUB TOTAL	$19.880.000
Costos imprevistos (20%) del total del costo del proyecto.	$3.976.000
TOTAL COSTO	$23.856.000

Fuente:Autores

CAPÍTULO II
ANALISIS CASO DE ESTUDIO

2. ANÁLISIS CASO DE ESTUDIO

2.1. CASO DE ESTUDIO

El caso de estudio fue desarrollado en una empresa de telecomunicaciones ubicada en la ciudad de Bogotá, más específicamente para el área de operaciones, el nombre de dicha empresa no se relaciona en este documento por políticas de confidencialidad, por lo tanto al momento de hacer referencia a ella se identificara como “la empresa” , está área no tiene definido un plan de seguridad que permita mitigar los riesgos en cuanto a la seguridad de la información, por tal motivo es muy vulnerable a la pérdida, alteración e inconsistencia de información, ya que la seguridad que se maneja es muy baja y tanto personal interno como externo tiene acceso a la misma sin ningún control.

El área ya mencionada de la empresa cuenta con un cuarto donde se encuentran alojados los servidores, dicho lugar está a la vista de todo el personal e incluso de los individuos externos que ingresen al área, lo cual quiere decir que equipos que se encargan de prestar el servicio de almacenar bases de datos, servidores web y toda la información están al alcance de cualquier persona además de toda la configuración de la red tanto física como lógica.

En cuanto a los equipos de trabajo que se le asignan a cada usuario, estos cuentan con su debido control de acceso puesto que al ingreso se les proporciona un usuario y contraseña, los cuales deben ser los mismos para acceder a los diferentes servicios del área como son repositorios, bases de datos, servidores de aplicaciones entre otros ,pero a pesar de que se realiza este proceso en muchas ocasiones los accesos no son otorgados a tiempo o simplemente nunca se hace y por tal motivo los usuarios deben compartir sus datos de acceso, razón por la cual en caso de una indebida manipulación de la información no se puede saber a ciencia cierta quién fue, por lo que toda el área podría estar accediendo a alguno de los servicios con los mismos datos de acceso.

2.2 INFORMACIÓN TÉCNICA

A continuación, se describe el área sobre la que se ha realizado el caso de estudio en cuanto a su información técnica, en detalle su estado actual**:**

2.2.1 Plataforma Tecnológica

- Servidores de Base de Datos Oracle 10g y 11g
- Sistemas Operativos: Windows 7, Windows 8, Ubuntu
- Tecnologías de desarrollo :java,php,Sharepoint

2.2.2 Caracterización de la infraestructura actual

La compañía cuenta con una red de 13 servidores que permiten el almacenamiento y procesamiento de la información, su distribución es de la siguiente manera:

Tabla 4 Caracterización de la Infraestructura Actual

SERVIDORES	**CANTIDAD**
Base de datos	5
Aplicaciones	4
Almacenamiento	4
Total	13

Fuente:Autores

La infraestructura de cableado estructurado categoría 5 y cuenta con el siguiente canal de internet: Proveedor Claro, 50 Megas de bajada y 9 Megas de subida.

2.3 Matriz DOFA

Está herramienta permite trabajar con toda la información que se posee del área de operaciones que fue la tomada en el caso estudio,mediante la implementación de dicha herramienta se determinara cuales son Debilidades internas, Oportunidades externas, Fortalezas internas y Amenazas externas.

Tabla 5 Matriz DOFA

	DEBILIDADES	**FORTALEZAS**
MATRIZ DOFA	● Falta de políticas de seguridad bien definidas. ● El desarrollo del SGSI sea muy detallado. ● Desconocimiento de la metodología.	● Reducción de riesgos que afecten la seguridad,disponibilidad y confidencialidad de la información. ● Reduce el tiempo de interrupción del servicio y mejora el grado de satisfacción de los clientes. ● Optimización de la seguridad de la información.
OPORTUNIDADES	**ESTRATEGIAS(DO)**	**ESTRATEGIAS(FO)**
● Definición de políticas de Seguridad de Información,estableciendo controles y normas para el manejo de seguridad. ● Certificación ISO 27001. ● Aumentar la confianza en el área.	● Buscar asesoría profesional con el fin de cumplir los requisitos, para la certificación ISO 27001. ● Capacitar a los empleados en cuanto a la metodología Magerit para fomentar la seguridad en los procesos del área.	● Fortalecer los procesos del área para aumentar la calidad del producto ayudados de una gestión fuerte de PQR. ● Aprovechar la mejora de la seguridad de la información, para aumentar la confianza en el área por parte de la compañía, mediante la entrega de mejores resultados.
AMENAZAS	**ESTRATEGIAS(DA)**	**ESTRATEGIAS(FA)**
● Falta de compromiso en la implementación del SGSI.	● Poner en marcha una campaña a nivel del área que concientice al	● Realizar capacitaciones a todo el personal para mejorar la

● Dificultad a la hora de poner en práctica esos conocimientos. ● Disponer de personal no calificado.	personal en cuanto a la importancia de la implementación del sgsi.	calidad de los resultados entregados por el área.

Fuente:Autores

2.4. Declaración de Aplicabilidad

Este es un documento que refleja el perfil de seguridad de una empresa, aquí se declaran los controles que son relevantes para el SGSI del área de operaciones y aplicables al mismo.

La presente declaración de aplicabilidad tomará lugar siempre y cuando el área cuente con las sub áreas establecidas a continuación, para un buen desempeño en los controles y su implementación.

Sub áreas a tener en cuenta:

- Soporte y monitoreo
- Instalación y mantenimiento
- Infraestructura
- Desarrollo
- Calidad

Ver anexo A. - “Declaración de Aplicabilidad” Se encuentra en la carpeta Anexos del CD.

2.5. Alcance del SGSI dentro del Caso Estudio

Para la implementación de la norma, se ha identificado la actividad principal del área de operaciones, la cual es transformar la materia prima en un producto elaborado, con un valor agregado que en el inicio del proceso no tenía. Por ello, se ha determinado que el dominio a seguir de la norma ISO/IEC 27001:2013 es el 14: Adquisición, desarrollo y mantenimiento de sistemas.

2.6. Metodología a Usar

La metodología que predetermina el enfoque del análisis y los criterios de gestión de riesgos en el SGSI es Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y la norma ISO/IEC 27005:2008.

2.6.1. Magerit

Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[16].

Magerit persigue los siguientes objetivos:

Directos

- concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos

- preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Etapas de la metodología magerit

- **Toma de datos y procesos de información:** va de la mano con el alcance definido para el SGSI, y se deben tener en cuenta los procesos que lleva a cabo la organización y analizar los riesgos que puedan interferir en los procesos críticos; también se debe precisar a qué nivel de detalle se debe llegar.

- **Establecimiento de parámetros:** se deben identificar los parámetros que se utilizarán durante todo el proceso de análisis de riesgos, los cuales son:

  - Valor de los activo
  - Vulnerabilidad
  - Impacto
  - Efectividad del control de seguridad:

- **Análisis de activos:** identificar cuáles son los activos que posee la empresa y que necesita para llevar a cabo sus actividades; debe ir acorde con el alcance definido. Los activos se pueden clasificar en: físicos, lógicos, de

[16] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

personal, de entorno e infraestructura, intangibles. Se efectuará su valoración de acuerdo a los parámetros descritos anteriormente.

- **Análisis de amenazas:** amenazas son aquellas situaciones que podrían llegar a darse en una organización y que resultan en un problema de seguridad. Se clasifican en:

  - Accidentes
  - Errores
  - Amenazas intencionales presenciales
  - Amenazas intencionales remotas

- **Establecimiento de vulnerabilidades:** vulnerabilidades son aquellos agujeros que se tienen en la seguridad de una empresa y que permiten que una amenaza pueda dañar un activo. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas.

- **Establecimiento de impactos:** los impactos son las consecuencias que provoca en la empresa el hecho de que cierta amenaza, aprovechando una vulnerabilidad, afecte un activo. Al analizar los impactos, se deben tener en cuenta los siguientes aspectos: el resultado de la agresión de una amenaza sobre un activo, el efecto sobre cada activo, el valor económico de las pérdidas producidas en cada activo, las pérdidas cuantitativas o cualitativas.

- **Análisis de riesgo intrínseco:** el riesgo intrínseco en la metodología utilizada, se toma como el riesgo en la situación actual de la empresa que se analiza. De acuerdo a esto, con los valores analizados en los puntos descritos anteriormente, sólo es necesario multiplicar los valores así: Riesgo = Valor del activo × Vulnerabilidad × Impacto

- **Influencia de salvaguardas:** las salvaguardas son los controles de seguridad, para este análisis se clasifican en dos tipos: preventivas (reducen las vulnerabilidades) y correctivas (reducen el impacto de las amenazas). En esta fase se trata de encontrar las soluciones de seguridad que existan en el mercado de ambos tipos.

- **Análisis de riesgos efectivo:** se estudia cómo se reducen los riesgos con cada una de las salvaguardas identificadas en la fase anterior, es decir, se calcula el riesgo efectivo que tendría la empresa para cada una de las amenazas identificadas. Este cálculo se realiza de la siguiente manera:

Riesgo efectivo = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

- **Evaluación de riesgos:** consiste en la toma de decisiones por parte de la empresa sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquella. Las organizaciones deben pretender disminuir todos los riesgos que han

detectado hasta situarlos por debajo del denominado "umbral de riesgos" y que represente un menor costo.[17]

2.6.2 Terminología

Modelo de valor
Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos
Relación de las amenazas a que están expuestos los activos.

Declaración de aplicabilidad
Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Evaluación de salvaguardas
Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo
Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias
Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

Cumplimiento de normativa
Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

Plan de seguridad
Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

2.6.3 Norma ISO/IEC 27005

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de

[17] http://metodologia-magerit.blogspot.com.co/

riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.

ISO 27005 sustituyó a la Gestión de la Información y Comunicaciones Tecnología de Seguridad, la norma ISO / IEC TR 13335-3:1998 y la norma ISO / IEC TR 13335-4:2000.

2.6.4 Secciones de contenido

Se trata de un estándar que cuenta con una parte principal concentrada en 24 páginas, también cuenta con anexos en los que se incluye ejemplos y más información de interés para los usuarios.

En estos anexos podemos encontrar tabulados amenazas, vulnerabilidades e impactos, lo que puede resultar útil para abordar los riesgos relacionados con los activos de la información en evaluación.[18]

- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.
- Descripción del proceso de ISRM.
- Establecimiento Contexto.
- Información sobre la evaluación de riesgos de seguridad (ISRA).
- Tratamiento de Riesgos Seguridad de la Información.
- Admisión de Riesgos Seguridad de la información.
- Comunicación de riesgos de seguridad de información.
- Información de seguridad Seguimiento de Riesgos y Revisión.
- Anexo A: Definición del alcance del proceso.
- Anexo B: Valoración de activos y evaluación de impacto.
- Anexo C: Ejemplos de amenazas típicas.
- Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
- Enfoques ISRA: Anexo E.

[18] http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

2.7 Tipos de Activos

Magerit clasifica los activos de la siguiente manera:

- Activo de información
- Software
- Hardware
- Infraestructura
- Servicios
- Recurso humano

2.8 Codificación o etiquetación de los Activos

Para el caso de estudio se etiquetara los activos de la siguiente manera**:**

Tabla 6 Codificación o Etiquetación de los Activos

ACTIVO	**ETIQUETA**
Activo de Información	ACI - ###
Software	SOF - ###
Hardware	HAR - ###
Infraestructura	INF - ###
Servicios	SER - ###
Recursos Humanos	RH - ###

Fuente:Autores

2.9 Criterios de Valoración de Activos

Para la valoración de los activos se tendrán en cuenta las siguientes dimensiones:

Tabla 7 Dimensiones de Valoración

CRITERIO	**DIMENSIÓN**
Disponibilidad	D
Integridad de los datos	I
Confidencialidad de la información	C

Fuente:Autores

Conforme al criterio de evaluación presentada por Magerit,las dimensiones se valoran de la siguiente manera:

Tabla 8 Criterios de Valoración de Activos

CRITERIO	VALOR	NIVEL
Daño extremadamente grave	Extremo	10
Daño muy grave	Muy Alto	9
Daño grave	Alto	6-8
Daño importante	Medio	3-5
Daño menor	Bajo	1-2
Irrelevante a efectos prácticos	Despreciable	0

Fuente:Autores

Estos criterios de valoración dados por la metodología solo se tendrán en cuenta para las dimensiones de disponibilidad (D) e integridad (I),para la dimensión de confidencialidad se manejaran otros criterios de acuerdo al tipo de información, los cuales se relacionan a continuación:

Tabla 9 Criterios de Valoración de Activos II

CRITERIO	NIVEL
Restringido	8-10
Uso Interno	4-7
Pública	0-3

Fuente:Autores

Restringido

Hace referencia a la información propia del área, que no puede ser divulgada entre las diferentes áreas de la organización y mucho menos externos a la misma ejemplo de está accesos de los servidores.

Uso Interno

Hace referencia a la información que circula al interior de la compañía, ejemplo de está políticas internas de la misma.

Pública

Hace referencia a la información que puede ser vista tanto por el personal interno como por cualquier persona externa de la compañía, ejemplo de está la página web de la misma.

2.10. Tipos de Impacto y Riesgo (Amenazas)

Magerit clasifica las amenazas en cuatro grupos como los mencionado a continuación:

- Errores y fallos no Intencionados
- Ataques Intencionados
- De Origen Industrial
- Desastres Naturales

Cada amenaza se presenta en un cuadro como el relacionado a continuación:

Tabla 10 ModeloDescripciónAmenaza

(Código) Descripción de lo que puede pasar		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Que se puede ver afectados por este tipo de amenaza.	De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenada de más a menos relevante.	valor del impacto de acuerdo al criterio
DESCRIPCIÓN		
lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.		

Fuente:Autores

Ver Anexo B. – “Amenaza de Acuerdo a la Metodología Magerit”

2.11. Criterios de Valoración de Probabilidad del Riesgo

La probabilidad de que el riesgo se repita o sea frecuente se valorará de la siguiente manera:

Tabla 11 Criterios de Valoración Probabilidad de Riesgo

VALOR	NIVEL
Siempre	5
Casi Siempre	4
A Menudo	3
Algunas Veces	2
Casi Nunca	1

Fuente:Autores

2.12. Criterios de Valoración de Impacto

La valoración de impacto del riesgo en el activo de la información, se realizará de la siguiente manera:

Tabla 12 Criterios de Valoración de Impacto

CRITERIO	VALOR	NIVEL
Amenaza y/o impacto extremadamente grave	Muy Alto	5
Amenaza y/o impacto muy grave	Alto	4
Amenaza y/o impacto grave	Medio	3
Amenaza y/o impacto importante	Bajo	2
Amenaza y/o impacto menor	Muy Bajo	1

Fuente:Autores

2.13. Criterios de Valoración del Riesgo

Para realizar la valoración del riesgo, se tiene en cuenta la valoración de probabilidad y la valoración de impacto dada a cada activo, esta valoración se comporta de la siguiente manera:

Tabla 13 Criterios de Valoración del Riesgo

VALOR	NIVEL
Muy Alto	17 – 25
Alto	10 – 16
Medio	5 – 9
Bajo	2 – 4

Muy Bajo	1

Fuente:Autores

2.14. Criterios de Calificación del Control

La calificación del control, se realizará de la siguiente manera:

Tabla 14 Criterios de Calificación del Control

VALOR	**NIVEL**
Control Adecuado	10
Control Importante	9
Control Parcialmente Adecuado	6-8
Control Menor	3-5
Control Inadecuado	1-2

Fuente:Autores

2.15. Criterios de Valoración de Vulnerabilidades

Se pretende analizar e identificar las vulnerabilidades que pueda tener el caso de estudio presentado a valoración de la vulnerabilidad se realiza teniendo en cuenta los siguientes niveles de valoración:

- **Alta:** es grave debido al aprovechamiento de una amenaza para realizar daño.
- **Media:** es importante pero tiene poca probabilidad de ser aprovechada por una amenaza
- **Baja:** no es aprovechada, ya que no existe amenaza alguna para materializarse en ella.

CAPÍTULO III
ANÁLISIS DE RIESGOS

3. ANÁLISIS DE RIESGOS

3.1. Caracterización de Activos

3.1.1. Identificación de Activos

Los activos con los cuales cuenta el área, para el desarrollo de su trabajo son los siguientes:

3.1.1.1. Datos/Información

Los Datos e información que se deben tener en cuenta son:

- Documentos Internos
- Manuales de Usuario
- Manuales Técnicos
- Manuales de Instalación
- Base de Datos
- Contratos
- Entregables (CD/DVD)
- Material Físico (Impreso)
- Información Disco Portables
- Información en Carpetas compartidas en Red

3.1.1.2. Software/Aplicaciones Informáticas

El software o aplicaciones que se tienen en cuenta son:

- Desarrollos a medida y/o propios del área
- Servidores Aplicaciones/Contenedores
- Sistemas Operativos
- Antivirus
- Navegadores
- Office
- Motor Base de Datos
- Licencias
- Desarrollo - IDE

3.1.1.3. Equipamiento Informático (Hardware)

En el equipamiento de hardware se encuentra los siguientes:

- Servidores

- Portátiles
- Routers
- Teléfonos
- Modems
- CD/DVD
- Discos Portables
- Dispositivos Móviles
- Equipos Multifuncional
- Cámaras de Seguridad
- Lector Huella Dactilar

3.1.1.4. Servicios

Los servicios a tener en cuenta son:

- Internet
- Red Inalámbrica
- Telefonía
- Fluido Eléctrico
- Almacenamiento de Información

3.1.1.5. Infraestructura

La infraestructura con que el área cuenta es:

- Planta de la Organización
- Canalización de red Eléctrica
- Instalación de red de Eléctrica
- Canalización de red Datos
- Instalación de red de Datos

3.1.1.6. Personal

El personal del área que se tiene en cuenta es:

- Usuarios Internos
- Analistas
- QA
- Funcionales
- Desarrolladores
- Clientes
- Proveedores

3.1.2. Etiquetado de Activos

De acuerdo al tipo de activo, se ha etiquetado los activos identificados de la siguiente manera:

Tabla 15 Etiquetado de Activos

TIPO ACTIVO	NOMBRE	CÓDIGO
Información	Documentos Internos	INF_01
	Manuales de Usuario	INF_02
	Manuales Técnicos	INF_03
	Manuales de Instalación	INF_04
	Base de Datos	INF_05
	Contratos	INF_06
	Entregables (CD/DVD)	INF_07
	Material Físico (Impreso)	INF_08
	Información Disco Portables	INF_09
	Información en Carpetas compartidas en Red	INF_010
Software	Desarrollos a medida y/o propios del área	SOF_01
	Servidores Aplicaciones/Contenedores	SOF_02
	Sistemas Operativos	SOF_03
	Antivirus	SOF_04
	Navegadores	SOF_05
	Office	SOF_06

	Motor Base de Datos	SOF_07
	Licencias	SOF_08
	Desarrollo - IDE	SOF_09
Hardware	Servidores	HAR_01
	Portátiles	HAR_02
	Routers	HAR_03
	Teléfonos	HAR_04
	Modems	HAR_05
	CD/DVD	HAR_06
	Discos Portables	HAR_07
	Dispositivos Móviles	HAR_08
	Equipos Multifuncional	HAR_09
	Cámaras de Seguridad	HAR_010
	Lector Huella Dactilar	HAR_011
Servicios	Internet	SER_01
	Red Inalámbrica	SER_02
	Telefonía	SER_03
	Fluido Eléctrico	SER_04
	Almacenamiento de Información	SER_05
	Planta de la Organización	INF_01
	Canalización de red Eléctrica	INF_02

Infraestructura	Instalación de red de Eléctrica	INF_03
	Canalización de red Datos	INF_04
	Instalación de red de Datos	INF_05
Personal	Usuarios Internos	PER_01
	Analistas	PER_02
	QA	PER_03
	Funcionales	PER_04
	Desarrolladores	PER_05
	Clientes	PER_06
	Proveedores	PER_07

Fuente:Autores

3.1.3. Valoración de Activos

Una vez identificados todos los activos, se procede a hacer su valoración, esto hace referencia al valor que se asigna a cada activo de acuerdo al grado de importancia, además resguardando la disponibilidad, integridad y confidencialidad de cada uno de ellos.

A continuación se realizará la valoración correspondiente a cada activo de acuerdo al criterio de valoración de cada una de las siguientes dimensiones.

Disponibilidad [D]
Integridad de los datos [I]
Confidencialidad [C]

Ver Anexo C. – “Valoración de Activos” Se encuentra en la carpeta Anexos del CD.

3.2. Caracterización de Amenazas

3.2.1. Identificación de Amenazas por tipo de Activo

Amenazas son aquellas situaciones que podrían llegar a darse en una organización y que resultan en un problema de seguridad, por lo tanto en este punto se detallan las principales amenazas sobre cada uno de los activos.

Antes de identificar las amenazas para cada activo identificado del caso estudio, se realizó una lista de las posibles amenazas por tipo de activo, todo esto en base en el anexo C “Ejemplo de amenazas comunes” de la norma
ISO/IEC 27005:2008 con su respectiva descripción.

Ver Anexo D. – “Identificación de Amenazas por tipo de Activo” Se encuentra en la carpeta de Anexos del CD.

3.2.2. Valoración de Vulnerabilidad por Amenazas de tipo de Activo

Se realiza una identificación y valoración de vulnerabilidad identificada en cada una de las amenazas por tipo de activo identificado anteriormente, todo esto en base del anexo D “Vulnerabilidades y Métodos para la Evaluación de la Vulnerabilidad” de la norma ISO/IEC 27005:2008

Ver Anexo E. - “Identificación de Vulnerabilidades por Amenaza de Tipo de
Activo” Se encuentra en la carpeta Anexos del CD.

3.2.3. Identificación de Amenazas

De acuerdo a la identificación de amenazas por cada tipo de activo anteriormente realizada, se presenta a continuación el catálogo de amenazas sobre los activos de la organización, teniendo en cuenta su valor hallado en la valoración de activos este entre “Extremo, Muy Alto y Alto”.

Ver Anexo F. – “Identificación de Amenazas” Se encuentra en la carpeta Anexos del CD.

3.2.4. Identificación de Vulnerabilidades

Vulnerabilidades son aquellos agujeros que se tienen en la seguridad de una empresa y que permiten que una amenaza pueda dañar un activo. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas.

De acuerdo a la identificación de amenazas sobre los activos de laorganización, se presenta a continuación el catálogo de vulnerabilidades por cada amenaza identificada.
Ver Anexo G. – “Identificación de Vulnerabilidades” Se encuentra en la carpeta Anexos del CD.

3.2.5. Relación entre Impacto, Probabilidad y Riesgo

Este análisis de riesgo se hace con el fin de aclarar la relación existente entre elriesgo, la probabilidad de que ocurra y el impacto que puede tener en cada unode los activos identificados anteriormente.

Matriz de Riesgo

En la siguiente figura se evidencia la Matriz de Riesgo de los activos identificados enel caso estudio, sin tener en cuenta los controles que se hagan en el casoestudio.

Figura 3. Riesgos Inherentes

		Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
Probabilidad	Siempre	0	0	0	0	0
	Casi Siempre	0	0	0	0	0
	A Menudo	0	0	0	0	0
	Algunas Veces	0	0	0	0	0
	Casi Nunca	0	0	0	0	0

Fuente:Autores

En la siguiente figura se evidencia la Matriz de Riesgo de los activos identificados en el caso estudio, teniendo en cuenta los controles que se hagan en el caso estudio.

Figura 4. Riesgos Residuales

		Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
Probabilidad	Siempre	0	0	0	0	0
	Casi Siempre	0	0	0	0	0
	A Menudo	0	0	0	0	0
	Algunas Veces	0	0	0	0	0
	Casi Nunca	0	0	0	0	0

Este documento refleja las decisiones por parte del área sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquella. Las organizaciones deben pretender disminuir todos los riesgos que han detectado hasta situarlos por debajo del denominado "umbral de riesgos" y que represente un menor costo, para ver el análisis de riesgo en detalle de cada activo y su procedimiento:

Ver Anexo H. – “Análisis de Riesgos” Se encuentra en la carpeta de Anexos del CD.

CAPÍTULO IV
POLÍTICAS Y CONTROLES DE SEGURIDAD

4. POLÍTICAS Y CONTROLES DE SEGURIDAD

4.1. Procedimientos y Controles

Teniendo en cuenta el análisis de riesgo generado para la implementación del Sistema de Gestión de Seguridad de la Información en el caso estudio se procedió a definir una serie de controles asociados a cada objetivo de control teniendo en cuenta la norma ISO 27002:2005, en donde se identifican cuáles de ellos aplican a las amenazas identificadas por cada activo.

El plan de mitigación de riesgos es un documento en el cual se detalla cada control, se identificó cada uno de los riesgos, se define la prioridad en la que se debe realizar el plan de tratamiento, se le asignó un código y un responsable de acuerdo al área en la que se identifica el riesgo, para observar de una manera más específica el plan de mitigación de riesgos:

Ver Anexo I. – "Plan de Mitigación de Riesgos" el cual se encuentra en la carpeta de Anexos del CD.

4.2. Políticas de Seguridad

Teniendo en cuenta el análisis de riesgos se definen una serie de normas y/o buenas prácticas con el fin de estandarizar los procesos del área y así mismo gestionar y proteger los distintos activos de la misma.

Con el fin de poder detallar este proceso se elaboró un documento, el cual contiene un riesgo, el respectivo control que sirve para mitigarlo y una breve descripción que indica en que consiste el control, para ver los controles aplicados a cada riesgo:

Ver Anexo J. – "Riesgos y Control" Se encuentra en la carpeta Anexos del CD.

CAPÍTULO V
MANUAL DE POLÍTICAS Y CONTROLES

5. MANUAL DE POLÍTICAS Y CONTROLES

5.1. Manual de Políticas y Controles

Teniendo en cuenta las políticas de seguridad y los controles se definió un manual que busca orientar a los usuarios internos en cuanto al debido proceso que deben llevar en cualquier eventualidad de riesgo.

Para ver el manual de políticas y controles:

Ver Anexo K. – “Manual de Políticas y Controles” Se encuentra en la carpeta Anexos del CD.

CAPÌTULO VI
PROTOTIPO

6. PROTOTIPO

6.1. Introducción

Este capítulo describe la implementación de la metodología de trabajo scrum, para el desarrollo del prototipo diseñado a partir del SGSI desarrollado a lo largo de este trabajo.

Incluye junto con la descripción de este ciclo de vida iterativo e incremental para el proyecto, los artefactos o documentos con los que se gestionan las tareas de adquisición y suministro: requisitos, monitorización y seguimiento del avance, así como las responsabilidades y compromisos de los participantes en el proyecto.

6.2. Personas y Roles del proyecto

Tabla 16 Personas y Roles del Proyecto

PERSONA	CONTACTO	ROL
Edward Leonardo Alvarado Romero	leotkd24@gmail.com	Scrum Master
Daniela Stefany Buitrago Rojas	dsbuitragor@gmail.com	Equipo de trabajo

Fuente:Autores

6.3. Artefactos

6.3.1. Historias de Usuario

Tabla 17Historias de Usuario

ID HISTORIA DE USUARIO	TIPO DE USUARIO	TAREA	OBJETIVO
H1	usuario,usuario administrador	Login	ingresar al sistema.
H2	usuario,usuario administrador	Recuperar contraseña	Restablecer contraseña en caso de olvido.
H3	usuario administrador	Registro de usuarios	Registrar la información de los usuarios en el sistema.
H4	usuario administrador	Editar Usuarios	Modificar la información de los usuarios en el sistema.
H5	usuario administrador	Eliminar Usuarios	Eliminar usuarios del sistema

H6	usuario administrador	Registro ítem del plan de mitigación de riesgos	Registrar la información del plan a seguir para cada uno de los riesgos.
H7	usuario administrador	Editar ítem del plan de mitigación de riesgos	Editar la información del plan a seguir para cada uno de los riesgos.
H8	usuario administrador	Eliminar ítem del plan de mitigación de riesgos	Eliminar la información del plan a seguir para cada uno de los riesgos.
H9	Usuario	Editar estado de un ítem del plan de mitigación de riesgos	Editar el estado del plan a seguir,según el riesgo asignado.
H10	usuario,usuario administrador	Visualizar documento	Acceder al manual de políticas y controles.
H11	usuario administrador	Cargar documento	Cargar manual de políticas y controles al sistema.
H12	usuario administrador	Configuración hora tarea programada	Configurar a qué hora desea que se corra la tarea programada, encargada de enviar correo cuando uno de los ítems del plan de mitigación de riesgos no se encuentre finalizado.
H13	usuario,usuario administrador	Cerrar sesión	Finalizar la sesión del usuario.

Fuente:Autores

6.3.2. productbacklog

Tabla 18product backlog

BACKLOG ID	ID HISTORIA DE USUARIO	ESTIMACIÓN	PRIORIDAD
B1	H1	9	Muy Alta
B2	H2	5	Alta
B3	H3	9	Muy Alta
B4	H4	5	Alta
B5	H5	5	Alta

B6	H6	9	Muy Alta
B7	H7	5	Alta
B8	H8	5	Alta
B9	H9	9	Muy Alta
B10	H10	3	Media
B11	H11	3	Media
B12	H12	9	Muy Alta
B13	H13	3	Media

Fuente:Autores

6.3.3. Sprint Backlog

Cada uno de los Sprint cuenta con una duración de una semana, a continuación se detalla el Sprint Backlog de los realizados.

6.3.3.1. Sprint 1

Tabla 18 Sprint 1

BACKLOG ID	ESTADO
B1	Terminado
B2	Terminado
B13	Terminado

Fuente:Autores

6.3.3.2. Sprint 2

Tabla 19Sprint 2

BACKLOG ID	ESTADO
B3	Terminado
B4	Terminado
B5	Terminado

Fuente:Autores

6.3.3.3. Sprint 3

Tabla 20Sprint 3

BACKLOG ID	ESTADO
B6	Terminado
B7	Terminado
B8	Terminado
B9	Terminado

Fuente:Autores

6.3.3.4. Sprint 4

Tabla21 Sprint 4

BACKLOG ID	ESTADO
B10	Terminado
B11	Terminado
B12	Terminado

Fuente:Autores

6.4. Manual de Usuario

Con base en el producto final desarrollado se elaboró un manual de usuario, el cual tiene como objetivo instruir a los diferentes tipos de usuario en el uso del sistema y la solución de los problemas que puedan suceder en la operación.

Para ver el manual de Usuario:

Ver Anexo L. – “Manual Usuario”

6.5. Manual del Sistema

También se elaboró un manual del sistema el cual va dirigido a la dirección IT,al administrador del sistema y a otros desarrolladores de software para que puedan darle mantenimiento en caso de ser requerido, este también puede ser utilizado por el departamento de sistemas para el caso de una auditoría.

Para ver el manual del Sistema:

Ver Anexo M. – “Manual del Sistema”

CAPÌTULO VII
CONCLUSIONES

7. CONCLUSIONES

- En la elaboración del proyecto se pudo determinar la importancia de la implementación del SGSI en el área de operaciones de las empresas prestadoras de servicios de telecomunicaciones, debido a que por su gran extensión no se tiene el control necesario para dar la seguridad a la información, la cual es uno de los principales activos de la misma y por lo tanto vital para la continuidad del negocio.

- Durante la etapa del diagnóstico actual del área se encontraron muchas falencias en cuanto a la seguridad de la información, esto permite concluir que a pesar de que este tipo de empresas trabajan netamente para el sector IT aún les falta mucho en este camino y que es vital que empiecen a concientizar a sus empleados de la importancia de definir políticas de seguridad y de que estas sean cumplidas al pie de la letra.

- El uso de la metodología Magerit para la gestión de riesgos informáticos, permite canalizar los riesgos que tienen las empresas de telecomunicaciones en los procesos de control de equipos e inventario, además durante análisis de gestión de riesgos a través de la metodología magerit se puede identificar la norma que se va a llevar a cabo para realizar el SGSI propuesto.

- Mediante el proceso de la selección de políticas y controles de seguridad para el área de operaciones de empresas dedicadas al sector de las telecomunicaciones, se pudo ver la importancia de la aplicación de la norma ISO/IEC 27001, la cual es una gran herramienta de ayuda para lograr mejorar la seguridad de la información en cualquier área de cualquier compañía.

- La fabricación del manual de políticas y controles, permitió establecer una guía a seguir para la seguridad de la información, que cualquier área de operaciones de una empresa dedicada al sector de las telecomunicaciones puede aplicar y con ella mitigar los riesgos que pueda correr su información.

- La implementación del prototipo demuestra como una herramienta tecnológica puede ayudar en los procesos de seguridad de la información que lleve a cabo cualquier compañía, para este caso en específico es una herramienta de mucha ayuda para el área de operaciones de las empresas de telecomunicaciones.

7.1 RECOMENDACIONES

- Implementar el proyecto general en todas las áreas de las empresas de telecomunicaciones.

- Ampliar el desarrollo implementado en el proyecto adicionando un módulo de gestor documental que permita manejar toda la documentación del proceso sistema de gestión de seguridad (SGSI)

- Actualizar el proyecto general de acuerdo a la actualización de las metodologías y normas utilizadas

- Se recomienda para la implementación del sistema de gestión de seguridad de la información en las demás áreas de la empresa, acudir al conocimiento de la Universidad Distrital en este tipo de proyectos

CAPÌTULO VIII
ANEXOS

8. ANEXOS

8.1. Anexo B Amenaza de Acuerdo a la Metodología Magerit

Tabla 22 AMZ01- AccidenteImportante

AMZ01- Accidente Importante		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Alto
DESCRIPCIÓN		
Consiste en un daño a nivel físico o electrónico que perjudica el funcionamiento del hardware.		

Fuente:Autores

Tabla 23 AMZ02- Daño por Agua

AMZ02- Daño por Agua		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Posibilidad de que el agua acabe con los recursos del sistema, generada por alguna fuga de agua interna o la rotura de la tubería de agua.		

Fuente:Autores

Tabla 24 AMZ03- Daño por Fuego

AMZ03- Daño por Fuego		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Posibilidad de que el fuego acabe con los recursos del sistema, generadas por materiales inflamables o problemas eléctricos.		

Fuente:Autores

Tabla 25 AMZ04-Falla del Equipo

AMZ04-Falla del Equipo		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad.	Alto
DESCRIPCIÓN		
Se refiere algún daño físico del activo.		

Fuente:Autores

Tabla 26 AMZ05-Hurto de Equipo

AMZ05-Hurto de Equipo		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad Confidencialidad	Muy Alto
DESCRIPCIÓN		
La sustracción de equipamiento provocando directamente la carencia de un medio para prestar el servicio, es decir una indisponibilidad		

Fuente:Autores

Tabla 27 AMZ06-Impulsos Electromagnéticos

AMZ06-Impulsos Electromagnéticos		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Alto
DESCRIPCIÓN		
Alteración de la alimentación eléctrica		

Fuente:Autores

Tabla 28 AMZ07- Mal Funcionamiento del Equipo

AMZ07- Mal Funcionamiento del Equipo		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Se refiere algún daño físico o lógico del activo.		

Fuente:Autores

Tabla 29 AMZ08- Manipulación con Hardware

AMZ08- Manipulación con Hardware		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Confidencialidad Disponibilidad	Muy Alto
DESCRIPCIÓN		
Alteración intencionada del funcionamiento del hardware, persiguiendo un beneficio.		

Fuente:Autores

Tabla30 AMZ09-Manipulación del Sistema

AMZ09-Manipulación del Sistema		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Confidencialidad Disponibilidad	Muy Alto
DESCRIPCIÓN		
Alteración intencionada del funcionamiento del hardware, persiguiendo un beneficio.		

Fuente:Autores

Tabla 31 AMZ10- Pérdida de Suministro de Energía

AMZ10- Pérdida de Suministro de Energía		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Cese de la alimentación eléctrica		

Fuente:Autores

Tabla 32 AMZ11- Polvo, Corrosión, Congelamiento

AMZ11- Polvo, Corrosión, Congelamiento		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Alto
DESCRIPCIÓN		
Suciedad en los dispositivos que genere un mal funcionamiento.		

Fuente:Autores

Tabla 33 AMZ12- Uso no Autorizado del Equipo

AMZ12- Uso no Autorizado del Equipo		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware	Disponibilidad	Alto
DESCRIPCIÓN		
Utilización de los recursos para fines no previstos.		

Fuente:Autores

Tabla 34 AMZ13- Código mal Intencionado

AMZ13- Código mal Intencionado		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información	Integridad Disponibilidad	Muy Alto
DESCRIPCIÓN		
Consiste en alguna instalación de software para alterar y/o eliminar la información.		

Fuente:Autores

Tabla 35 AMZ14-Intrusión, Accesos Forzados al Sistema

AMZ14- Intrusión, Accesos Forzados al Sistema		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información	Integridad Confidencialidad	Muy Alto
DESCRIPCIÓN		
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello.		

Fuente:Autores

Tabla 36 AMZ15- Procesamiento Ilegal de los Datos

AMZ15- Procesamiento Ilegal de los Datos		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información	Integridad	Muy Alto
DESCRIPCIÓN		
Datos mal usados que ocasiona problemas legales severos		

Fuente:Autores

Tabla 37 AMZ16-Recuperación de Medios Reciclados o Desechados

AMZ16- Recuperación de Medios Reciclados o Desechados		
TIPO DE ACTIVOS	DIMENSIONES	VALOR DE IMPACTO
Información	Confidencialidad	Muy Alto
DESCRIPCIÓN		
Uso de elementos desechados para otro fin.		

Fuente:Autores

Tabla 38 AMZ17-Saturación del Sistema de Información

AMZ17- Saturación del Sistema de Información		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Carencia de recursos suficientes provocando la caída del sistema.		

Fuente:Autores

Tabla 39 AMZ18-Incumplimiento en la Disponibilidad del Personal

AMZ18- Incumplimiento en la Disponibilidad del Personal		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Personas	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Ausencia deliberada del puesto de trabajo		

Fuente:Autores

Tabla 40 AMZ19- Acceso no Autorizado al Sistema

AMZ19- Acceso no Autorizado al Sistema		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Confidencialidad Disponibilidad Integridad	Muy Alto
DESCRIPCIÓN		
Consiste en tener acceso a información del sistema para ser modificada, borrada o inutilizar sin autorización datos o información del sistema		

Fuente:Autores

Tabla 41 AMZ20-Ataques contra el Sistema

AMZ20-Ataques contra el Sistema		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Disponibilidad Confidencialidad Integridad	Muy Alto
DESCRIPCIÓN		
Consiste en tener acceso a información del sistema para ser modificada, borrada o inutilizar sin autorización datos o información del sistema		

Fuente:Autores

Tabla 42 AMZ21-Copia Fraudulenta del Software

AMZ21-Copia Fraudulenta del Software		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Integridad Disponibilidad Confidencialidad	Alto
DESCRIPCIÓN		
Consiste en la instalación de software pirata.		

Fuente:Autores

Tabla 43 AMZ22- Error en el Sistema

AMZ22- Error en el Sistema		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Daños en el sistema que pueden ocurrir generando indisponibilidad del activo.		

Fuente:Autores

Tabla 44 AMZ23- Incumplimiento en el Mantenimiento del Sistema deInformación

AMZ23- Incumplimiento en el Mantenimiento del Sistema de Información		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Integridad Disponibilidad	Alto
DESCRIPCIÓN		
Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.		

Fuente:Autores

Tabla 45 AMZ24- Mal Funcionamiento del Software

AMZ24- Mal Funcionamiento del Software		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Disponibilidad	Muy Alto
DESCRIPCIÓN		
Error o fallo en un programa desencadenando un resultado indeseado.		

Fuente:Autores

Tabla 46 AMZ25- Uso de Software Falso o Copiado

AMZ25- Uso de Software Falso o Copiado		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software	Disponibilidad Integridad Confidencialidad	Alto
DESCRIPCIÓN		
Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.		

Fuente:Autores

Tabla 47 AMZ26- Destrucción del Equipo o de los Medios

AMZ26- Destrucción del Equipo o de los Medios		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware Información	Disponibilidad	Alto
DESCRIPCIÓN		
Eliminación total del activo.		

Fuente:Autores

Tabla 48 AMZ27- Corrupción de los Datos

AMZ27- Corrupción de los Datos		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Software Información	Integridad	Alto
DESCRIPCIÓN		
Errores que se producen durante el diligenciamiento de documentos o formularios de aplicaciones.		

Fuente:Autores

Tabla 49 AMZ28- Error en el Uso

AMZ28- Error en el Uso		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Hardware Información Software	Disponibilidad Integridad Confidencialidad	Alto
DESCRIPCIÓN		
Equivocaciones del personal cuando usa el activo.		

Fuente:Autores

Tabla 50 AMZ29- Hurto de Información

AMZ29- Hurto de Información		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información Software	Disponibilidad Confidencialidad	Muy Alto
DESCRIPCIÓN		
La sustracción de información provocando la carencia de datos importantes para la continuidad de algún proceso de la organización.		

Fuente:Autores

Tabla 51 AMZ30- Ingreso de Datos Falsos o Corruptos

AMZ30- Ingreso de Datos Falsos o Corruptos		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Información Software	Integridad	Muy Alto
DESCRIPCIÓN		
Errores que se producen durante el diligenciamiento de documentos o formularios de aplicaciones.		

Fuente:Autores

Tabla 52 AMZ31- Suplantación de Identidad

AMZ31- Suplantación de Identidad		
TIPO DE ACTIVOS	**DIMENSIONES**	**VALOR DE IMPACTO**
Personas Información	Confidencialidad Integridad	Muy Alto
DESCRIPCIÓN		
Hacerse pasar por un usuario no autorizado, disfrutando de los privilegios de este para un fin en especial.		

Fuente:Autores

8.2. BIBLIOGRAFÍA

- ATEHORTÚA, Federico Alonso. BUSTAMANTE, Ramón Elías. VALENCIA DE LOS RIOS, Jorge Alberto. Sistema de Gestión Integral. Una sola gestión, un solo equipo. 1era edición. Universidad de Antioquia: Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC. 2009. 232 Pág. ISBN: 9789587141580
- SGSI Empresa de telecomunicaciones [en línea]<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/35841/18/hvargasmTFM0614memoria.pdf>[Citado en 22 de Agosto de 2017]
- SGSI [en línea]<http://www.pmg-ssi.com/2015/07/que-es-sgsi/ >[Citado en 22 de Agosto de 2017]
- Ciclo Deming [en línea] <http://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/>
  [Citado en 30 de Agosto de 2017]
- Cobit [en línea]
  <http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html (2017)>[Citado en 12 de Agosto de 2017]
- Norma Iso27001 [en línea]
  <https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1502520656&Signature=RrgRD0Fjfpbb3AxncrC3U4I5oXI%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22994_1.pdf>[Citado en 27 de Agosto de 2017]
- Magerit [en línea]
  <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WY6ZQVEjHIU>[Citado en 27 de Agosto de 2017]
- java [en línea]<https://docs.google.com/document/d/1Sv0I1iGAr85ysjfLlW07m-PZ5vXN1NEzqBaY14w0bWQ/edit#> [Citado en 01 de Octubre de 2017]
- PrimeFaces [en línea]<https://www.adictosaltrabajo.com/tutoriales/introduccion-primefaces/> [Citado en 01 de Octubre de 2017]
- PostgreSql [en línea]<https://microbuffer.wordpress.com/2011/05/04/que-es-postgresql/> [Citado en 01 de Octubre de 2017]
- AREITIO BERTOLIN, Javier. Seguridad de la información. Redes, informática y sistemas de información. Edición 2008. Madrid (España): Paraninfo. 2008. 592 pág. ISBN 13: 9788497325028,ISBN 10: 8497325028.
- Scrum [en línea]<https://proyectosagiles.org/que-es-scrum/> [Citado en 10 de Octubre de 2017]
- Proceso [en línea]<http://www.i2btech.com/blog-i2b/tech-deployment/para-que-sirve-el-scrum-en-la-metogologia-agil/> [Citado en 10 de Octubre de 2017]