DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTA

JOSE HIGINIO RUIZ PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C 18 DE FEBRERO DE 2018

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTA

JOSE HIGINIO RUIZ PEÑA

MONOGRAFIA

CON MIRAS A OBTENER EL TITULO DE:

ESPECIALISTA EN SEGURIDAD INFORMATICA

DIRECTOR

EDGAR ALONSO BOJACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTÁ D.C 18 DE FEBRERO DE 2018

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C, febrero 18 de 2018

DEDICATORIA

Dedico el cumplimiento de esta meta, en primer lugar a Dios por su orientación, por sus bendiciones y sabiduría, en segundo lugar a mi esposa Ana Rosa, a mis hijos Julián David, Ingrid Natalia y Verónica Vanessa, quienes son el soporte y mi razón de ser, quienes con su amor y apoyo incondicional me han fortalecido espiritual y anímicamente para continuar adelante en búsqueda de la consecución de esta etapa tan anhelada en mi vida y, en tercer lugar a mis padres (Q.E.P.D), personajes que siempre llevaré en mi memoria por sus consejos, por los buenos principios y valores que enfundaron en mí, por su misión cumplida en la vida y por hacer de mí una persona de bien.

AGRADECIMIENTOS

Agradezco a Dios por todas sus bendiciones y por todo lo que me ha dado en la vida, a la Cooperativa Multiactiva del Personal del SENA, COOPSENA, y en especial al Ingeniero Héctor Fabio Barón por su colaboración en el levantamiento de la información, a la Universidad Nacional Abierta y a Distancia; por la contribución educativa de los Colombianos, mediante el fortalecimiento de la investigación, la proyección social y las innovaciones metodológicas y didácticas, por fomentar el aprendizaje autónomo y colaborativo generador de la buena cultura y del espíritu emprendedor, principios que han hecho posible el desarrollo de este proyecto investigativo.

También agradezco, a los ingenieros Salomón Gonzáles y Edgar Alonso Bojacá directores del curso, por sus aportes, sugerencias y recomendaciones.

Por último, agradezco a mi familia, a mis hermanos y demás familiares quienes creyeron en mis capacidades y me alentaron para el cumplimiento de esta meta que me propuse conseguir en la vida.

CONTENIDO

pág.

INTRODUCCION 24

1. PLANTEAMIENTO DEL PROBLEMA 27

1.2 DESCRIPCIÓN DEL PROBLEMA 27

1.3 FORMULACIÓN DEL PROBLEMA.....28

2. JUSTIFICACION 29

3. OBJETIVOS 31

3.1 OBJETIVO GENERAL 31

3.2 OBJETIVOS ESPECIFICOS.....31

4. ALCANCE Y DELIMITACION.....32

5. MARCO REFERENCIAL 33

5.1 ANTECEDENTES 33

5.2 MARCO TEÓRICO 38

5.2.1 La seguridad informática 38

5.2.1.1 Seguridad física. 41

5.2.1.2 Seguridad lógica 42

5.2.2 Seguridad de la información 42

5.2.3 Infraestructura tecnológica 44

5.2.4 SGSI 47

5.2.5 Importancia de un SGSI 48

5.2.6 Componentes de un SGSI. Entre los componentes de un SGSI, tenemos: .50

5.3 ESTADO DEL ARTE 51

5.3.1 Estándares o normas utilizados para la seguridad de la información. 51

5.3.1.1 BS7799-3 51

5.3.1.2 COBIT 52

5.3.1.3 COSO 54

5.3.1.4 NIST (National Insitute of Standards and Technology) 54

5.3.1.5 Normas ISO/IEC 27000 55

5.3.2 Norma ISO/IEC 27001 57

5.3.2.1 Funcionamiento de la ISO/IEC 27001.....57

5.3.2.2 Importancia de la ISO/IEC 27001 58

5.3.3 Gestión de riesgos. Metodologías.....63

5.3.3.1 OCTAVE 64

5.3.3.2 NIST SP 800-30:.....65

5.3.3.3 MEHARI 66

5.3.3.4 ISO 27005.....66

5.3.3.5 MAGERIT.....67

5.3.3.5.1 Paso 1: inventario y valoración de activos 71

5.3.3.5.2 Paso 2: identificación y valoración de amenazas.....77

5.3.3.5.3 Paso 3: análisis de salvaguardas.....80

5.3.3.5.4 Paso 4: Impacto residual.....81

5.3.3.5.5 Paso 5: Riesgo residual 81

5.4 MARCO CONCEPTUAL 81

5.4.1 MARCO LEGAL 81

5.4.2 Ley 1273 de 2009 82

5.4.3 Ley 1341 del 30 de julio de 2009 85

5.4.4 Ley estatutaria 1581 de octubre 17 de 2012 85

5.5 MARCO CONTEXTUAL 86

5.5.1 Cooperativa Multiactiva del Personal del SENA, COOPSENA 86

5.5.2 Reseña Histórica 86

5.5.3 Misión 87

5.5.4 Visión 87

5.5.5 Política de Calidad 87

5.5.6 Organigrama institucional 88

5.5.7 Integrantes de los órganos de administración y control, periodo 2016 – 2018 89

6. MARCO METODOLOGICO 91

6.1 METODOLOGÍA DE INVESTIGACIÓN 91

6.2 METODOLOGÍA DE DESARROLLO 91

6.2.1 Investigación descriptiva 92

6.2.2 Investigación explicativa 92

7. DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN COOPSENA.....94

7.1 IMPLICACIÓN DE LOS DIRECTIVOS PARA EL DESARROLLO DEL PROYECTO.....94

7.2 ALCANCE DEL PROYECTO 94

7.3 ELECCIÓN DE LA METODOLOGÍA PARA LA GESTIÓN DE RIESGOS.....95

7.4 GESTIÓN DE RIESGOS DEL SISTEMA DE INFORMACIÓN DE COOPSENA 95

7.4.1 Inventario de activos 95

7.4.1.1 Valoración de activos 104

7.4.2 Identificación y valoración de riesgos 109

7.4.3 Gestión de riesgos 119

7.4.4 Determinación de salvaguardas.....133

7.4.4.1 Lista de chequeo.....133

7.4.4.2 Declaración de aplicabilidad 134

7.4.4.3 Plan de tratamiento de riesgos 134

7.5 POLITICAS RECOMENDADAS A IMPLEMENTAR EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA COOPSENA.....140

7.6 PLAN DE CONTINUIDAD DE NEGOCIO PARA LA COOPERATIVA MULTIACTIVA DEL PERSONAL DE SENA, COOPSENA. 145

8. CONCLUSIONES.....165

9. RECOMENDACIONES 167

9.1 PROGRAMA DE SENSIBILIZACION 168

BIBLIOGRAFIA.....170

ANEXOS.....178

LISTA DE TABLAS

pág.

Tabla 1. Niveles de la infraestructura tecnológica en una organización 45

Tabla 2. Dominios y procesos del estándar COBIT 53

Tabla 3. Clasificación de activos según MAGERIT.....72

Tabla 4. Estimación cualitativa del riesgo 76

Tabla 5. Relación entre escala cualitativa y cuantitativa.....76

Tabla 6. Criterios de valoración de activos de acuerdo al grado de la amenaza ...77

Tabla 7. Probabilidad de ocurrencia de la amenaza.....79

Tabla 8. Impacto de las amenazas sobre las dimensiones de seguridad.....79

Tabla 9. Tipos de salvaguardas.....80

Tabla 10. Estructura de la ley 1273 de 2009 83

Tabla 11. Consejo administrativo COOPSENA.....89

Tabla 12. Junta de vigilancia.....89

Tabla 13. Revisoría fiscal y gerencia 90

Tabla 14. Activos esenciales 96

Tabla 15. Archivos de datos 98

Tabla 16. Infraestructura de clave publica 99

Tabla 17. Servicios 99

Tabla 18. Aplicaciones (software) 101

Tabla 19. Equipos informáticos 101

Tabla 20. Redes de comunicaciones 102

Tabla 21. Soportes de información 103

Tabla 22. Equipamiento auxiliar 103

Tabla 23. Instalaciones 104

Tabla 24. Personal 104

Tabla 25. Criterios de valoración del nivel de criticidad de los activos 105

Tabla 26. Valoración de activos y nivel de criticidad 106

Tabla 27. Probabilidad de ocurrencia de la amenaza 109

Tabla 28. Dimensiones de seguridad según MAGERIT.....110

Tabla 29. Eficacia de controles.....110

Tabla 30. Valoración del riesgo residual.....111

Tabla 31. Valoración de riesgos y el impacto sobre los activos x cada dimensión de seguridad de acuerdo a la metodología MAGERIT.....112

Tabla 32. Matriz de gestión de riesgos (empresa COOPSENA).....120

Tabla 33. Análisis de riesgo promedio.....132

Tabla 34. Declaración de aplicabilidad (SOA) 136

Tabla 35. Plan de tratamiento de riesgos (PTR).....138

Tabla 36. Principales actividades y roles del comité del PCN 148

Tabla 37. Descripción de procesos críticos en COOPSENA 151

Tabla 38. Componentes informáticos de los procesos críticos en COOPSENA..152

Tabla 39. Parámetros del análisis de impacto del negocio.....153

Tabla 40. Recursos para la continuidad de los procesos críticos 155

Tabla 41. Tipos de pruebas del plan de continuidad del negocio 162

LISTA DE FIGURAS

pág.

Figura 1. Relación entre los riesgos, vulnerabilidades, amenazas, controles y activos 49

Figura 2. Relación entre componentes y principios de COSO 54

Figura 3. Modelo PHVA 60

Figura 4. Elementos del análisis de riesgos potenciales.....68

Figura 5. MAR – Método de Análisis de Riesgos.....69

Figura 6. Organigrama institucional COOPSENA 88

Figura 7. Análisis cuantitativo de los riesgos 119

Figura 8. Árbol de llamadas 157

Figura 9. Secuencia de actividades en caso de una interrupción del SI 158

ANEXOS

pág.

Anexo A. Dominios y controles de la ISO/IEC 27001:2013 178

Anexo B. Lista de chequeo 180

Anexo C. Resumen Analítico Especializado (RAE) 198

Anexo D. Carta de aceptación de COOPSENA para el desarrollo del proyecto ..204

GLOSARIO

ACTIVO INFORMÁTICO: es todo dispositivo o componente funcional de un sistema de información que es esencial para los procesos corporativos y objetivos de negocio. Comprende: recursos humanos, información, comunicaciones, recursos físicos (hardware), recursos lógicos (software) y servicios.

ACUERDO RECÍPROCO: Acción contractual entre dos empresas u organizaciones con la particularidad de poseer operaciones técnico- funcionales semejantes de tal manera, que permitan a la una o a la otra, recuperar sus procesos críticos mediante la prestación de recursos e instalaciones.

ALTERNATIVA DE RECUPERACIÓN: Proceso diseñado con el fin de dar solución a una parálisis de actividades como consecuencia de un desastre.

AMENAZA: es el origen eventual de un incidente con la capacidad de exponer, alterar o destruir los datos de un sistema informático.

ANÁLISIS DE RIESGOS: es la metodología utilizada a través de la cual se establecen una serie de pasos con el fin determinar cómo es el sistema de información, cuánto vale, cómo está protegido, cuáles son las falencias de seguridad y proporcionar un modelo más seguro en términos de activos, amenazas y salvaguardas, que permita satisfacer las necesidades detectadas por el análisis de riesgos.

CAUSA: es el origen de producción de un riesgo

CENTRO REPLICADO: sitio alternativo de solución que requiere una alta inversión económica por parte de una organización para adaptarlo a sus propias necesidades

con el fin de ser utilizado como espacio de recuperación rápida de sus procesos ante la interrupción generada por desastre.

CERTIFICACIÓN: es la garantía que permite asegurar que los procedimientos de un sistema de información en materia de seguridad, se están realizando conforme a las leyes y normativas actuales.

CONFIANZA: es la seguridad que se tiene en que un sistema informático va a funcionar en la forma como se desea.

CONTINGENCIA: circunstancia no deseada que pone en riesgo la continuidad de procesos de una organización.

CICLO DE DEMING: estrategia implementada por la norma ISO/IEC 27001, que consiste en un ciclo en espiral de mejora continua (PHVA), para garantizar la calidad de un SGSI, implantado en una organización.

CONTROLES: es el conjunto de acciones, registros, documentos, procedimientos, medidas técnicas y buenas prácticas a adoptar que permiten garantizar que todo aspecto valorado en el análisis de riesgos, queda cubierto y disponible para procesos de auditoria.

DENEGACIÓN DE SERVICIO (DoS): es una modalidad de ataque en el que un delincuente intenta deshabilitar un recurso o un servicio al que quieren acceder los usuarios autorizados del sistema de información.

DESASTRE: suceso no premeditado, cuyo impacto produce durante un determinado periodo de tiempo, la interrupción total o parcial de las operaciones de un negocio, además de generar incertidumbre organizacional.

GESTIÓN DE RIESGOS: es una secuencia de actividades que permiten establecer estrategias de identificación, evaluación, manejo y reducción de efectos negativos que los riegos pueden llegar a ocasionar en un sistema informático. Incluye por lo tanto, el análisis y el tratamiento de riesgos.

IMPACTO: medida del daño que podría ocurrir en un activo informático, como consecuencia de una amenaza.

INCIDENTE: evento inesperado que un determinado momento, puede alterar o interrumpir una operación de un sistema, disminuyendo la calidad del servicio o actividad productiva dependientes del mismo.

INCIDENCIA: influencia de riesgos en un sistema de información, cuyo efecto podría causar alteraciones en el mismo.

INTERRUPCIÓN: suspensión total o parcial de uno o más procesos productivos del negocio durante un determinado período de tiempo.

INGENIERÍA SOCIAL: Método utilizado por los atacantes para engañar a los usuarios de un sistema de información, para que realicen una acción que normalmente, producirá consecuencias negativas, como la descarga de malware o la divulgación de información empresarial o personal.

MTD: **Tiempo Máximo Permitido de Recuperación** o (Maximum Tolerable Downtime): es el periodo de tiempo establecido para que un proceso crítico organizativo pueda permanecer interrumpido antes de producirse una situación desastrosa para la organización.

NIVEL DE CRITICIDAD: Valor cualitativo que determina la trascendencia de un sistema en relación con un servicio, recurso o proceso, cuyo funcionamiento debe

ser constante o estar disponible operativamente, en el tiempo mínimo posible después de la ocurrencia de un incidente ya sea de tipo físico, natural o humano.

PLAN DE CONTINUIDAD DEL NEGOCIO: Es el conjunto de etapas que de manera sucesiva se desarrollan como objeto de prevención de las interrupciones de un sistema que pueda afectar el normal desempeño de las actividades del Negocio.

PROBABILIDAD DE OCURRENCIA: variable cuantitativa y cualitativa que permite medir el grado de materialización de una amenaza sobre un activo informático.

RIESGO: probabilidad de que uno o más activos informáticos, reciban la acción de una amenaza, la cual puede causar daños significativos a una organización.

RPO: Punto de Recuperación Objetivo o (Recovery Point Objective); es el volumen de información máximo tolerable que una organización puede llegar a perder ante el impacto de una contingencia o desastre.

RTO: **Tiempo de Recuperación Objetivo** o (Recovery Time Objective): es el tiempo establecido durante el cual un proceso puede estar interrumpido para poderse recuperar, dado una contingencia o desastre.

SALVAGUARDAS: son los medios o recursos tecnológicos que debidamente implementados, reducen los riesgos sobre un sistema.

SITIO ALTERNATIVO SUBCONTRATADO A TERCEROS: acuerdo o contrato que una empresa establece con otras empresas especializadas con ciertos recursos y espacios alternativos que son utilizados de manera temporal para la recuperación de procesos críticos ante la eventualidad de un desastre.

TELETRABAJO: modalidad moderna de desempeño de una determinada función que es permitida mediante el uso de medios teleinformáticos, desde lugares externos al centro de actividades normales de una organización.

VIRUS INFORMÁTICO: es una aplicación informáticas que tienen como objetivo alterar, interrumpir o modificar el funcionamiento de un sistema de información y en muchas ocasiones, la pérdida o destrucción de la información.

VULNERABILIDAD: es la debilidad que presentan los activos de información o sus medidas de seguridad, facilitando el impacto de una amenaza potencial.

RESUMEN

Este proyecto de titulación, presenta una descripción detallada de lo que es un Sistema de Gestión de Seguridad de la Información; especifica para que sirve, cuáles son sus objetivos, cuáles son sus ventajas, cuáles son sus componentes y cuáles son las metodologías más influyentes para logra una buena y económica implementación.

Su desarrollo está basado en la investigación realizada a la infraestructura tecnológica de COOPSENA, con el fin de analizar la situación actual de la entidad desde la perspectiva de los procedimientos que se llevan a cabo con relación a la seguridad de la información, para ello, nos hemos valido de recursos como la observación, la entrevista y el análisis de documentos, así como la información obtenida de la norma ISO/IEC 27001:2013, elegida para el diseño y desarrollo de proyecto en mención.

Para la etapa de planificación, que hace parte del modelo Deming integrado en la norma mencionada anteriormente, se ha elegido utilizar la metodología MAGERIT como herramienta para el proceso de gestión de riesgos, la cual ha permitido realizar las actividades de desarrollo de una forma más sistemática, gracias a las etapas en que se encuentra estructurada.

- Identificación y valoración de los activos corporativos.
- Identificación y valoración de amenazas
- Determinación de salvaguardas, proceso apoyado por técnicas como las listas de chequeo y la declaración de aplicabilidad (SOA).
- Impacto residual
- Riesgo residual

Palabras clave: SGSI, Estándar, Arquetipo, Infraestructura tecnológica, Gestión de riesgos, Degradación, Impacto residual, Riesgo residual, Declaración de aplicabilidad.

INTRODUCCION

En el actual globalizado mundo moderno, en donde el nivel de competencia entre las empresas u organizaciones cada día es mayor, en donde aparecen nuevos desafíos que crean la necesidad de buscar estrategias que permitan obtener cierta ventaja de sostenimiento en el mercado para lo cual, necesariamente, deben valerse de las tecnologías informáticas dado que son el eje de todas las operaciones empresariales y sociales, gracias a sus beneficios y potencialidades como lo son: la facilidad de manejo de enormes volúmenes de información, la automatización, la realidad virtual, la comunicación instantánea, la inteligencia artificial, la mecatrónica, el comercio electrónico y otra serie de recursos como el E-learning y las páginas sociales, entre otros.

Si bien es cierto, que todos estos cambios han contribuido a novedosos modos de vida, nuevas formas y prácticas de hacer negocio, novedosos conceptos administrativos, etc. También han contribuido a la generación de nuevos problemas que han repercutido seriamente en los ámbitos sociales y aún más, en el clima, la cultura y los entornos organizacionales debido al desorientado y mal uso de los recursos informáticos que ha acuñado nuevos términos al diccionario informático como secuestro de datos, robo de identidad, robo de información, hackers, crackers, pirata cibernético, virus informáticos, crimen cibernético, entre otros. Estos elementos conforman una realidad cuya frecuencia comienza a generar un obstáculo de altas proporciones para el cumplimiento de objetivos empresariales y, por ende, para el desarrollo social.

Ese tipo de factores y situaciones se han convertido en uno de los temas de gran interés para los profesionales, investigadores y desarrolladores de técnicas y mecanismos relacionados a la seguridad informática, debido al alto grado de complejidad y complicación que representan para proteger la información, para que las empresas puedan cumplir con los objetivos para los cuales fueron creadas.

Por tal razón, para que las organizaciones puedan operar eficiente y eficazmente, se han creado una serie de modelos y estándares internacionales a través de los cuales, estas deben demostrar que ejecutan acciones competentes y efectivas para salvaguardar los recursos informáticos y los datos que gestionan como recursos críticos a los cuales hay que brindarles una protección adecuada. Para eso, se debe hacer una buena gestión de riesgos, analizar y ordenar adecuadamente los activos informáticos con los que cuenta la organización, establecer adecuados procedimientos de seguridad y contar con los controles y mecanismos necesarios que permitan alcanzar los objetivos de las decisiones tomadas.

Estas acciones, son las que conforman un Sistema de Gestión de Seguridad de la Información (en adelante identificado como SGSI), que, en sí, es una metodología orientada a disminuir los riesgos y el impacto que estos puedan ocasionar contra la integridad, confidencialidad, disponibilidad y la autenticidad de la información, y cuya implementación no requiere grandes inversiones. Una de dichas metodologías, es la que está reglamentada bajo el estándar ISO/IEC 270001.

Por todo lo anterior, las organizaciones públicas y privadas hoy más que nunca, deben integrar en sus políticas de gestión de la calidad, un plan orientado a la protección de sus activos informáticos, lo cual implica que deben conocer y aprender a poner en práctica la conceptualización, las técnicas, herramientas, métodos, normas y decretos de ley que las obliga a la revisión y hacer buen uso de la información contenida en sus sistemas informáticos.

De manera que, su recurso humano debe estar debidamente capacitado y estar al día con los cambios tecnológicos para aplicar de manera exitosa los procedimientos relacionados al manejo y seguridad de los elementos informáticos que estén bajo su responsabilidad, pues, como bien lo dice Lizarazo Rueda: “La falta de formación en el uso apropiado de las herramientas informáticas, ha puesto de manifiesto una de las debilidades más grandes en cuanto a la preservación de la seguridad de la

información se trata, ya que el primer paso utilizado por los atacantes para obtener acceso indebido a la información es a través de un usuario inexperto en el uso de las TIC" [1].

La capacitación del recurso humano es fundamental para enfrentar los desafíos que imponen las amenazas como los hackers, los virus y los riesgos ambientales; a través de los métodos de control de acceso, monitoreo, sistemas de autenticación y demás controles de prevención y protección, así como el cumplimiento y aceptación de las directrices que conforman un plan de seguridad informática para generar un clima laboral favorable que facilite la gestión del anulamiento o disminución de los riesgos de ataques informáticos que puedan impactar la continuidad de un negocio.

En definitiva, las empresas necesariamente, deben proteger su información si quieren mantener vigente su competencia y liderazgo en el mercado, y para lograrlo se recomienda diseñar e implementar un SGSI.

[1] LIZARAZO RUEDA, Javier Enrique. El ser humano: Factor clave en la seguridad de la información. {En línea}. Septiembre de 2012. {Consultado el 9 de octubre de 2016}. Disponible en: http://docplayer.es/1146750-El-ser-humano-factor-clave-en-la-seguridad-de-la-informacion.html

1. PLANTEAMIENTO DEL PROBLEMA

1.2 DESCRIPCIÓN DEL PROBLEMA

Debido a la evolución de las Tecnologías de la Información y las Comunicaciones, que converge en modernas y nuevas aplicaciones, revolucionarios avances tecnológicos y mejoramiento continuo en las funciones y propiedades de los mismos, ha conllevado también a la generación continua de riesgos, vulnerabilidades y amenazas que pueden comprometer seriamente, los sistemas informáticos y; por consiguiente, la continuidad operativa de un negocio.

Estas amenazas pueden ser externas como el phisching, hacking, cracking, virus, etc. e internas como las malas prácticas o infidelidad de los usuarios del sistema de información y las que son causadas por las fallas del sistema y el medio ambiente.

Ante esta situación, para que un negocio pueda operar con eficiencia y rentabilidad, debe proteger su información, acción que en la actualidad, ya no es simplemente una necesidad sino un requisito que las organizaciones deben cumplir, ante el surgimiento y actualización constante de estándares, leyes y normativas que son avalados por la comunidad internacional, y para el caso de Colombia, por el congreso de la república y el ministerio de comunicaciones.

Es por esto, que las organizaciones deben implementar metodologías a través de las cuales puedan gestionar los riesgos y detectar las vulnerabilidades o puntos débiles causantes del alto porcentaje de concreción de amenazas sobre un sistema informático y establecer adecuados controles de seguridad que les permita proteger la información; el activo más importante para sus gestiones empresariales.

De ahí, la iniciativa de este proyecto investigativo para ponerlo a disposición de la institución COOPSENA, con el fin de reducir los posibles riesgos presentes, brindar una mejor protección a su infraestructura informática y poder cumplir con sus responsabilidades jurídicas y económicas.

Los procedimientos y técnicas contemplados en este proyecto para diseñar un SGSI, se fundamentan en la norma ISO/IEC 27001:2013 y en la metodología MAGERIT 3.0 para la gestión de riesgos.

1.3 FORMULACIÓN DEL PROBLEMA

Debido a la ausencia de adecuados mecanismos para la protección de la información y al poco conocimiento que en materia de seguridad informática, tienen la mayor parte de las personas y en especial, dirigentes de muchas empresas, se hace necesario el conocimiento sobre la implementación de un SGSI, que genere conciencia y compresión del valor que posee la información, de la dificultad que implica recuperarla si esta se daña o se pierde, de la necesidad de asignar un presupuesto para evitar una acción de esta naturaleza y especialmente, que exija que absolutamente todos los usuarios de un sistema informático, están en la obligación de hacer un buen uso y proteger la información que estos utilizan para que la empresa pueda operar rentable y eficientemente.

De acuerdo a estos criterios se origina la siguiente pregunta:

¿Cómo puede favorecer a la Cooperativa Multiactiva del Personal del SENA en Bogotá, si esta cuenta con las políticas, procedimientos y técnicas adecuadas para proteger su sistema informático?

2. JUSTIFICACION

Cuando una organización cumple sus objetivos de manera eficaz, es una organización que tiende a fortalecerse con calidad, con posibilidades de maximizar sus resultados de forma cualitativa y mensurable, logrando la satisfacción de las necesidades de sus consumidores, clientes y usuarios; por lo tanto, adquiere ventaja competitiva en el mercado.

Desafortunadamente, el mismo desarrollo de las tecnologías ha facilitado el acceso de individuos inescrupulosos a los sistemas de información de muchas organizaciones, quienes con sofisticadas técnicas y algunas veces, con pocos conocimientos, han causado daños de gran magnitud como inestabilidad o discontinuidad de las operaciones, secuestro o pérdida de datos, bloqueo de comunicaciones, robo de contraseñas, etc. Generando altas pérdidas económicas e impactando negativamente la buena imagen corporativa conseguida por parte de las mismas.

No hay que desconocer también, los graves perjuicios a los que se ven sometidos los sistemas informáticos por parte de los riesgos ambientales como: incendios, terremotos, vendavales, inundaciones y los causados por la indebida manipulación de los dispositivos de información por parte de los usuarios del sistema, quienes, actuando de buena fe o de mala intención, ponen en riesgo la continuidad operativa de una empresa.

Por eso, un eficiente SGSI, conformado por políticas, procedimientos y mecanismos que permitan salvaguardar la información y mantener la confidencialidad, integridad, disponibilidad, autenticidad, autorización y el no repudio de la misma, es lo que necesita una organización con un direccionamiento estratégico como el de COOPSENA, para llevar a cabo sus operaciones de manera continua, a pesar de

las anomalías, fallas técnicas o eventos naturales fortuitos que puedan presentarse en un momento dado.

En este contexto, un SGSI, asume un papel muy importante porque a través de sus mecanismos, establece el uso apropiado de la información y de los dispositivos tecnológicos que la almacenan y la procesan para la toma de decisiones, elemento clave para el desempeño, funcionamiento y competitividad de un negocio que depende precisamente, de la calidad de los datos que genera y gestiona.

Por todo lo anterior, una empresa por más pequeñas que sea, requiere de medidas y herramientas de control que permitan conocer, gestionar y contrarrestar los riesgos y las amenazas informáticas de manera óptima y económica, brindando los niveles de seguridad apropiados para proteger y cumplir con los objetivos del negocio.

Esa es precisamente, la razón de ser de un SGSI cuyos beneficios se fundamentan en la reducción de riesgos, racionalización de recursos, mejora continua de procedimientos, garantía del cumplimiento de la legislación vigente, concienciación de usuarios, y la certificación del SGSI como elemento que garantiza protección optima de la información, mejoramiento de imagen y mejores niveles de competencia de la organización.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO/IEC 27001:2013 en COOPSENA, de tal manera que permita mejorar los niveles de seguridad de su sistema informático.

3.2 OBJETIVOS ESPECIFICOS

- Realizar el levantamiento de la información del estado actual del sistema informático corporativo, las metodologías de la gestión de riesgos, la legislación y normatividad, y los controles que conforman un SGSI.

- Definir la metodología a utilizar para la gestión de riesgos con el fin de identificar las vulnerabilidades y amenazas de seguridad que se presentan en los activos informáticos de la Cooperativa.

- Establecer los controles apropiados y proponer la implementación planificada.

- Contribuir con conocimientos y buenas prácticas al fortalecimiento de la seguridad de la información en los funcionarios de la organización

4. ALCANCE Y DELIMITACION

El entorno de aplicación de este proyecto investigativo es amplio, pues se enfoca en todas las áreas y niveles que conforman la infraestructura tecnológica de COOPSENA, toda vez que los riesgos que provienen tanto desde su interior como desde el exterior, pueden atentar contra la seguridad de la información, recurso intangible de gran valor para la viabilidad de la misma y su existencia en el mercado.

Por consiguiente, es nuestra convicción que este proyecto sea un generador de conciencia y de conocimientos sobre seguridad informática, ayudando a desarrollar procesos de mejora continua, de competitividad, de mejoramiento operativo, reducción de costos, y al cumplimiento de la normatividad vigente mediante la buena toma de decisiones a través de una información autentica, accesible, integra, precisa, actualizada y verídica.

Además de ser una solución para asumir los riesgos y las amenazas de un sistema informático, este proyecto también pretende aportar al lector un conocimiento más amplio sobre aquellos elementos que afectan seriamente la calidad de la información y le permita conocer las normas y metodologías actuales y apropiadas que se deben utilizar para planear y crear un modelo de seguridad informática para una empresa, y saber cuál es la legislación estatal que regula las disposiciones generales para proteger los datos empresariales y personales, elementos que están ampliamente relacionados a un SGSI.

Por otra parte, el proyecto detalla las ventajas y beneficios que obtiene una empresa al implantar un SGSI y describe los pasos que se deben seguir para lograr una implementación exitosa.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Un SGSI, considerado como el documento más importante que constituye los principios organizativos y funcionales de la actividad de la seguridad informática en una empresa, el cual incorpora políticas, medidas y procedimientos que permiten prevenir, detectar y responder a las amenazas de los sistemas informáticos, se ha convertido en la tarea más importante y más exigente en los procesos de producción de las empresas públicas y privadas, especialmente, porque estas dependen cada día más de las computadoras y de Internet para que los empleados puedan realizar su trabajo.

Sin embargo, el problema no radica en que las empresas y la misma sociedad, dependa de los sistemas informáticos para realizar la mayoría de sus actividades a medida que la evolución de las tecnologías y la complejidad de los sistemas aumenta, si no, en que cada vez son más el número de delitos informáticos que se cometen a través de los recursos de la información por los hackers malignos (Black hat), quienes aumentan tanto en número como en técnicas sofisticadas, haciendo de la seguridad informática un área cada vez decisiva e importante en el cumplimiento de los objetivos de toda organización.

Reconocer que la seguridad informática es actualmente el componente más importante de los sistemas de información, es el principio que toda entidad pública o privada debe tener en cuenta en el momento de realizar las políticas de gestión de la calidad y dedicar recursos materiales y humanos cada vez más significativos en esta área, pues siendo la información el mayor activo, sus técnicas y procedimientos son básicos para garantizar la supervivencia, entregar el mejor servicio a los clientes y mejorar la competitividad en el mercado.

Entre los antecedentes sobre la importancia de diseñar un SGSI en una organización, encontramos los planteamientos y el enfoque basado en procesos del informe final – modelo de seguridad de la información – sistema sansi – SGSI del Ministerio Nacional de las Tecnologías de la Información y las Comunicaciones (MINTIC) , en este documento el equipo del proyecto señala que: " un SGSI, aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua" [2].

Igualmente, el informe del MINTIC señala que:

> "Un SGSI, ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc."[3].

Un SGSI, está compuesto por un manual de normas y políticas de seguridad, sobre el cual Álvaro Arrieta (2011), describe que:" trata de definir; ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de

[2] MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Informe final – modelo de seguridad de la información – sistema sansi - SGSI - modelo de seguridad de la información para la estrategia de gobierno en línea. {En línea}. Diciembre de 2008. {Consultado el 14 de octubre de 2016}. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf.

[3] Ibídem.

seguridad adecuado a las necesidades establecidas dentro de la Corporación. Estos documentos tratan a su vez de ser el medio de interpretación de la seguridad para toda la organización"[4].

Son diversos los autores tanto nacionales e internacionales que han investigado y han propuesto proyectos sobre la implementación de SGSI, que hoy sirven de apoyo a muchas organizaciones como los bancos, las bolsas de valores, las industrias, los organismos gubernamentales y mundiales, etc. Y como base del conocimiento en desarrollos investigativos con el ánimo de prevenir y enfrentar el progresivo y peligroso impacto de la ciberdelincuencia y, aun así, algunos organismos como El Pentágono, la CIA, UNICEF, La ONU y muchas empresas a nivel mundial, han sido víctimas de ataques por parte de los hackers.

El documento Conpes 3701 de 2011, afirma que:

> En el mes de abril de 2007, el gobierno de Estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes bancos.
>
> Este ataque desató una gran crisis que requirió la intervención de la comunidad internacional y alertó a la Organización del Tratado del Atlántico Norte (OTAN), la cual, en agosto de 2008, puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD), con el fin de proteger a sus miembros de este tipo de ataques

[4] Arrieta, Álvaro. Políticas y normas de seguridad informática. {En línea}. 2011. {Consultado el 12 de septiembre de 2016}. Disponible en, http://www.cvs.gov.co/jupgrade/images/stories/docs/Alertas/Politicas_de_Seguridad_Informatica_CVS_2011-.pdf

> y entrenar a personal militar, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad [5] .

Igualmente, el documento menciona otros dos ataques cibernéticos representativos.

> El primero, fue en contra de los Estados Unidos en el mes de julio de 2009, cuando una serie de ataques afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio. Otro suceso fue el que reportó la Guardia Civil española en marzo de 2010, cuando desmanteló a una de las mayores redes de computadores "zombies", conocida con el nombre de "BotNet Mariposa", compuesta por más de 13 millones de direcciones IP9 infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupó el quinto puesto entre los países más afectados por esta red [6] .

Cabe mencionar las acciones realizadas por el pirata informático Andrés Sepúlveda, que según el diario EL TIEMPO (7 de mayo de 2014), "fue capturado y acusado por la Fiscalía de espiar correos electrónicos, hacer interceptaciones ilegales y vender información sobre los negociadores del Gobierno y la guerrilla de las FARC en los diálogos de paz de La Habana (Cuba) "[7] .

El periódico El País (lunes, Diciembre 31, 2012), también afirma que:

---

[5] CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL. Lineamientos de política para ciberseguridad y ciberdefensa. {En línea}. 14 de junio de 2011. {Consultado en septiembre de 2016}. Disponible en, http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[6] Ibídem.

[7] EL TIEMPO. El hacker Andrés Sepúlveda es enviado a la cárcel. El tiempo. {En línea}. 7 de mayo de 2014. {Consultado en septiembre de 2016}. Disponible en: http://www.eltiempo.com/archivo/documento/CMS-13950196

> La cifra de delitos informáticos en el país va en aumento. Tanto que Colombia es, actualmente, el tercer país en Latinoamérica donde más se cometen. Se calcula que 187 denuncias mensuales son interpuestas por fraude a diferentes bancos. Algunos de los delitos electrónicos que más se presentan en el país y que, según expertos de la Fiscalía, van en aumento son acceder a bases de datos de bancos u otras entidades sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias [8] .

Por todo lo anterior, un SGSI cumple un papel decisivo en el éxito de una empresa, pues es el que garantiza la continuidad de las sus operaciones, a pesar de los eventos fortuitos o desastres que puedan presentarse en los sistemas de información, permitiendo el logro de la disponibilidad de los servicios en los tiempos y momentos requeridos.

Sin embargo, hay que reconocer que además de los métodos y herramientas destinados a proteger los sistemas informáticos ante cualquier amenaza, un SGSI, es un proceso en el que directamente participan personas, y por lo tanto, la concienciación es vital para que dicho sistema tenga el éxito esperado.

De manera que, realizar e implementar trabajos investigativos sobre seguridad informática, implica ante todo un compromiso por parte de los actores involucrados (empresarios y funcionarios), de ahí que, este trabajo investigativo busca sentar los procedimientos y la política para la normatividad de un SGSI, en la Cooperativa Multiactiva del Personal del SENA (COOPSENA), y esta debe tener la responsabilidad de generar los mecanismos que permitan garantizar la seguridad del sistema informático para el desarrollo de sus operaciones.

[8] EL PAIS. En Colombia las cifras de delitos informáticos van en aumento. {En línea}. Diciembre 31 de 2012. {Consultado en septiembre de 2016}.Disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento

Para lo anterior, se tendrán en cuenta la norma técnica ISO/IEC 27001:2013, la metodología MAGERIT 3.0 y como base legal, la Ley Estatutaria 1273 de 2009 del congreso de la República de Colombia.

5.2 MARCO TEÓRICO

5.2.1 La seguridad informática. Desde el origen del hombre, la información ha sido el principal recurso de sociabilidad y desarrollo en todos los aspectos a través de todos los tiempos. Esta surge con la necesidad de comunicación entre los individuos primitivos para expresar sus sentimientos, necesidades, costumbres y emociones, cuyas técnicas y métodos fueron mejorando gracias a la evolución del hombre sobre la tierra.

Primero fue la emisión de sonidos articulados que dieron origen a la palabra, lo que luego produjo el lenguaje que fue desencadenando modernas formas de comunicación como la pictografía, la ideografía y por último la escritura; técnica que permitió que en un principio, la información se registrara en medios como la piedra, la arcilla, la madera y el pergamino, siendo este último, el elemento utilizado para almacenar la información a través de los libros manuscritos, como por ejemplo, el legado importante que nos dejaron los pensadores griegos (Aristóteles, platón, Sócrates, Pitágoras, etc.). Con la llegada de la imprenta y el papel, el libro se convirtió en el elemento de mayor portabilidad y difusión masiva de la información y la principal fuente sobre la que descansa el funcionamiento intelectual y la transferencia del conocimiento de la sociedad moderna.

Así comenzó, el desarrollo de producción de los bienes sociales y culturales como la industrialización, el comercio, la ilustración, el método científico, la radio, la televisión, el teléfono y el desarrollo de tecnologías que propició hacia finales del

siglo XX, la aparición de los computadores que revoluciono la microelectrónica y los sistemas distribuidos que conforman la infraestructura informática del actual mundo globalizado, cuya manifestación más evidente es la existencia de la superautopista de información, como comúnmente se le llama a INTERNET.

Este mecanismo integrador de funcionalidades, que de acuerdo a Barry M. Leiner, *et al*. "Es una infraestructura de información muy difundida, el prototipo inicial de lo que se llama a menudo la Infraestructura de Información Nacional (o Global, o Galáctica). Su historia es compleja e implica muchos aspectos: tecnológicos, organizativos y comunitarios. Y su influencia no solo alcanza los campos técnicos de las comunicaciones informáticas, sino también a la sociedad "[9].

Es decir, es un sistema interplanetario, cuyas características son las más firmes representaciones de las Tecnologías de la Información y la Comunicación TIC.

Precisamente, son las TIC, las que en la actualidad conforman el motor de todas las operaciones industriales, comerciales, económicas, de transporte, de servicios, de educación y comunicación. Ellas representan el éxito operativo, estratégico y económico de las organizaciones, presentan novedosas alternativas de solución y métodos necesarios para la formulación, diseño y perfeccionamiento de estudios investigativos relacionados al desarrollo de la ciencia y la tecnología, gracias al tratamiento, almacenamiento y transmisión de la información a través de los diferentes recursos asociados a las mismas; de ahí, su marcada influencia y dependencia en casi todas las actividades humanas; en fin, poco o nada se puede hacer sin la influencia de este tipo de tecnologías, lo que conllevaría a un impacto social de enormes proporciones, si estas dejaran de funcionar.

[9] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard, Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. Breve historia de internet. {En línea}. {Consultado en septiembre de 2016} Disponible en: http://www.internetsociety.org/es/breve-historia-de-internet

Precisamente, esa dependencia al uso masivo de las tecnologías informáticas que ha originado la sociedad del conocimiento, ha desencadenado una serie de conductas delincuenciales y el desarrollo de sofisticados métodos y técnicas para llevar a cabo todo tipo de delitos contra los sistemas de información como los fraudes financieros, robos de identidad, falsificación de documentos, secuestro de datos, sabotaje o daños y alteraciones de los programas o datos computacionales, etc.; los cuales han causado enormes pérdidas económicas en muchas organizaciones del mundo.

Las amenazas a las que está expuesta la información que manejan las empresas, es lo que ha originado las directrices que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, o sea, la Seguridad Informática. Este es un concepto de alta relevancia en el globalizado mundo de las Tecnologías de la Información y la Comunicación TIC, tanto que, según el MINTIC,

> Desde 1988, todos los 30 de noviembre, se celebra el Día Internacional de la Seguridad Informática. Nace con el nombre de Computer Security Day, en los Estados Unidos, para luego expandirse al mundo. Este día fue creado para concientizar y sensibilizar a todos los usuarios de las TIC sobre la importancia de la seguridad de la información, el buen manejo de los contenidos que compartimos diariamente en entornos virtuales y la responsabilidad que todos tenemos de generar espacios de respeto en la red [10].

La seguridad informática, es una disciplina que está conformada por políticas, estándares, modelos, procedimientos y mecanismos tecnológicos cuya acción está destinada a prevenir, detectar, anular o disminuir en cierto grado, las vulnerabilidades; y por tanto, las amenazas que se establecen contra las

[10] MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Día de la Seguridad Informática. {En línea}. 12 de septiembre de 2012. {Consultado en septiembre de 2016}. Disponible en: http://www.enticconfio.gov.co/dia-de-la-seguridad-informatica

infraestructuras de Tecnologías de la información y las comunicaciones TIC'S, que son la base para el funcionamiento y desarrollo de las organizaciones.

Por eso, la seguridad informática se ha estructurado en otros procesos como la seguridad en redes, seguridad en aplicaciones web, seguridad en base de datos, seguridad de los sistemas operativos, etc. Con el fin de gestionar acciones y procedimientos más seguros que permitan conservar, salvaguardar y proteger la información que es producida por los sistemas informáticos de las organizaciones, los cuales de manera constante están sometidos a una gran variedad de riesgos y amenazas que son originados, tanto desde la parte interna, como desde la parte externa de las mismas, debido a los siguientes factores:

A. Por factores humanos.
Externos: (virus, ingeniería social, espionaje, suplantación de identidad, hacking, cracking etc.)
Internos: (Infidelidad del personal, uso indebido de la información, divulgación a terceros, errores accidentales o mal intencionados etc.)

B. Por factores ambientales.
Las causadas por la influencia de la naturaleza (incendios, humedad, movimientos telúricos, lluvias, tormentas eléctricas etc.)

De acuerdo a estos factores, la seguridad informática se divide en dos grandes ramas, a saber:

5.2.1.1 Seguridad física. Comprende el conjunto de procedimientos y técnicas de protección física del sistema informático, por ejemplo: control de acceso de personas, sistemas de respaldo de energía eléctrica, sistemas de aterramiento,

protección electromagnética, medios o alarmas contra incendios, detectores de humedad, sistemas de climatización, pararrayos, etc.

5.2.1.2 Seguridad lógica. Comprende el conjunto de técnicas, herramientas y procedimientos de control para la protección de los datos en el mismo medio en el que se generan, se almacenan o en el medio a través del cual se transmiten. Por ejemplo: instalación de cortafuegos, antivirus, configuración de contraseñas, sistemas Proxy, filtrado de paquetes, aplicaciones de administración y monitoreo de datos, sistemas de auditoría, sistemas de protección criptográfica, dispositivos de identificación y autenticación de usuarios, actualización de los sistemas operativos, configuración del sistema Active Directory, configuraciones de la red, entre otros.

La seguridad lógica, deriva otro término conocido como seguridad de la información, el cual tiende a confundirse con el de seguridad informática; por lo tanto, hay que aprender a diferenciar, pues como se describió anteriormente, la seguridad informática se encarga de establecer los procedimientos y mecanismos de control para proteger las infraestructuras tecnológicas de la información, mientras que la seguridad de la información, aunque es un principio de la seguridad informática, cumple objetivos diferentes los cuales se describen a continuación.

5.2.2 Seguridad de la información. Es un proceso cuyo objetivo principal, es proteger y mantener la integridad de los activos críticos como la información, los aplicativos (software) y los servicios que soportan la razón de ser de una organización, los cuales dependen de las infraestructuras tecnológicas. Además, provee otras medidas de seguridad sobre los medios en donde esté disponible la Información como: cintas magnéticas, discos duros, impresiones en papel, videos e inclusive, sobre las personas que la manipulan o la conocen mediante procesos de

concientización, es decir, asegura una mayor solidez a la confidencialidad, integridad y disponibilidad de la información.

También, utiliza otras técnicas orientadas a minimizar los riesgos que atenten contra los procesos organizacionales, operativos y físicos con los cuales una organización mejora o mantiene su productividad y competitividad en el mercado, gracias al SGSI, que el gobierno corporativo haya decidido implementar, pues en la seguridad de la información, se encuentran involucrados los ejecutivos, líderes y directores empresariales, lo cual implica que ellos más que nadie, deben aprender a poner en práctica la conceptualización, las técnicas, herramientas, métodos y normas que conforman dicho sistema, mediante el cual dan cumplimiento a los decretos de ley, con los cuales, el estado los obliga a la revisión y hacer buen uso de la información disponible en todos los formatos y que es utilizada para el cumplimiento de los objetivos de negocio.

De ahí, que los procesos de seguridad de la información están orientados a hacer resistencia a las acciones que comprometan sus principios básicos a saber:

Confidencialidad: principio que garantiza que la información debe ser accedida solamente por las personas autorizadas. Una técnica de control asociada a este principio, es la encriptación.

Integridad: Permite asegurar que los datos recibidos o recuperados son exactos y completos, es decir, que no han sufrido ningún tipo de modificación. Una de las técnicas que garantiza este principio son los algoritmos de cifrado.

Disponibilidad: principio que garantiza que la información debe ser accesible por las personas autorizadas en el momento de requerirla. Una de las técnicas aplicadas son los planes de contingencia.

Otros principios asociados son:

Autenticación: principio que garantiza la identidad de quien solicita acceso a la información. Una técnica aplicada, las firmas digitales.
Autorización: garantiza el acceso y utilización de la información, solamente por las personas que tienen los permisos especiales o la exclusividad para hacerlo. Una técnica aplicada, los perfiles de usuario.
No repudiación: principio que garantiza la aceptación de una persona como el actor, el responsable o participante de un evento informático. Por ejemplo: Un usuario que realiza la emisión de un mensaje no puede tener un argumento sólido para negar que lo generó y el usuario receptor tampoco podrá negar que lo recibió.

5.2.3 Infraestructura tecnológica. La infraestructura tecnológica de una organización es el soporte de las actividades y funciones que favorecen la gestión de los recursos con el fin de producir bienes o servicios de buena calidad para ser competitiva en el mercado, gracias a los elementos tecnológicos que conforman el hardware y software de los sistemas informáticos.

El hardware, es el conjunto de elementos físicos o tangibles como los ordenadores personales, los servidores, las impresoras, los teléfonos IP, los UPS, los routers, los switches, las cámaras web, etc.

El software, está conformado por los elementos lógicos o intangibles como los sistemas operativos, las bases de datos, los lenguajes de programación, los programas de ofimática, aplicaciones para planeación y gestión administrativa, etc.

Comúnmente, la infraestructura tecnológica de una organización sin considerar su tamaño y actividad económica, se compone de una serie de elementos como los que se ilustran en la tabla 1.

Tabla 1. Niveles de la infraestructura tecnológica en una organización

Nivel	Descripción
Usuarios	Es el conjunto de personas que mediante procesos de autorización, pueden ingresar y hacer uso de los recursos del sistema informático de una organización.
Sala de maquinas	Compuesta por los dispositivos que garantizan la máxima disponibilidad de los servicios de la organización como Sistemas de alimentación interrumpida (SAI o UPS), sistemas de refrigeración, antincendios y monitoreo.
Infraestructura de servidores	Es el conjunto de dispositivos informáticos cuya arquitectura y configuración, permite a los usuarios autorizados, el acceso a los servicios del sistema para las diferentes actividades productivas como el almacenamiento de información. De acuerdo a los criterios y estrategias de negocio pueden ser distribuidos, centralizados, dedicados y no dedicados. Actualmente, algunas empresas han apostado por la virtualización de servidores.
Estaciones de trabajo	Conjunto de dispositivos informáticos que son utilizados por los usuarios para las diferentes actividades de la empresa como computadores de escritorio, portátiles, impresoras, teléfonos, scanner, etc.
Tecnología de la red	Compuesta por las topologías (Estrella, anillo, bus, malla, etc.) y tecnologías (Ethernet, Token ring, ATM, FDDI, entre otras) que soportan los constantes y sostenidos procesos automáticos de operaciones industriales, comerciales, de comunicación, administrativas y estratégicas que permiten cumplir los objetivos de negocio y prestar los servicios con eficacia y calidad. Su estructura física suele presentar una gran diversidad de recursos y servicios tecnológicos como VoIP, internet, correo electrónico,

	telefonía móvil, videoconferencias, etc. Lo que le da características de amplitud y complejidad para responder a las necesidades de los distintos tipos de usuarios, tanto internos como externos, que hacen uso de sus recursos.
Comunicaciones	Este nivel está constituido por las diferentes tecnologías que conforman los medios de transmisión a través de los cuales viaja la información. Estos medios pueden ser: Alámbricos como el cable UTP, F.O y el cable coaxial que son utilizados para generar diferentes tipos de red; LAN, WAN, MAN, PAN, etc. Y los medios inalámbricos como los sistemas Wi-Fi, Wimax y celular que son soportados por las tecnologías de microondas, infrarrojo y satelital. De este nivel, hacen parte también los dispositivos de comunicación como los routers, los switches, acces point, etc.
Infraestructura de aplicaciones	Capa constituida por todas las aplicaciones (software) que proporcionan capacidad productiva, eficiencia administrativa y optimización de los recursos a toda la empresa, como los sistemas de bases de datos, aplicaciones ofimáticas, sistemas operativos, antivirus, sistemas de planeación de recursos, de gestión de relaciones con los clientes, de administración del conocimiento, etc.
Servicios	Es el conjunto de actividades de alta calidad, eficientes y continuas que una empresa es capaz de suministrar a sus clientes, proveedores y trabajadores para un óptimo desarrollo corporativo, tales como call center, Help Desk, Service Desk, auditorias, etc.

Tabla 1. (Continuación)

Fuente: http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/serveis/index.html

5.2.4 SGSI. Suarez Sierra, Lorena nos presenta la siguiente definición:

> "Es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización"[11] .

Es decir, la sigla SGSI, es una herramienta multiservicio con la que cuenta las organizaciones para implementar medidas de protección que permitan garantizar la seguridad de la información contra la exposición de las múltiples amenazas del nivel externo como los virus informáticos, hackers, ingeniería social, denegación de servicios, etc. Las del nivel interno que son producidas a propósito o de manera involuntaria por los usuarios autorizados del sistema, o las que son causadas por los accidentes naturales y fallas técnicas, las cuales pueden causar un impacto negativo de altas proporciones, poniendo en riesgo los niveles de competitividad, rentabilidad, imagen y confianza; y por ende, los objetivos de negocio.

Sin embargo, gestionar e implantar un SGSI, es un proceso que requiere de estudio, que a su vez, hacen establecer cambios en los entornos empresariales.

[11] SUAREZ SIERRA, Lorena Patricia. Sistema de Gestión de la Seguridad de la Información (SGSI). {En línea}. Julio de 2013. {Consultado en octubre de 2016}.Disponible en: https://es.scribd.com/document/202912531/Modulo-SGSI-233003-Listo.

Por eso, la norma ISO/IEC-27001, que en el año 2005 tuvo su aprobación y publicación por parte de la International Organization for Standardization y la International Electrotechnical Commission, se ha convertido en la metodología más utilizada por la mayoría de las organizaciones por su sencillez en la implementación y especificación de los requisitos que son esenciales para establecer un SGSI.

Un SGSI, se apoya en los siguientes aspectos:

- Analizar y organizar adecuadamente, la infraestructura tecnológica de la información y las comunicaciones de la organización.
- Definir e implementar las reglas, los procedimientos operacionales, prácticas óptimas y medidas de índole técnica y organizativa con el fin de garantizar la protección de las tecnologías informáticas y de las personas que las utilizan para sus diferentes actividades empresariales.
- Recomendar el establecimiento de controles adecuados que permitan una evaluación eficiente de las decisiones tomadas.

De acuerdo al portal de ISO27001.es, estos tres aspectos permiten: “que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”[12]. Esto con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información, que es el principal objetivo de la norma ISO/IEC 27001.

5.2.5 Importancia de un SGSI. Además de lo anteriormente expuesto, un SGSI ofrece las herramientas técnicas para la búsqueda, análisis, evaluación y opciones

[12] SO 27000.ES. ¿Qué es un SGSI? {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.iso27000.es/

de tratamiento de riesgos, planes de contingencia que permiten garantizar la continuidad operativa ante un incidente de seguridad, concienciación y formación de los usuarios involucrados en el sistema de información, reevaluación de las medidas tomadas, buenas practicas relacionadas al uso de las TIC, preparación adecuada para el proceso de auditoría y certificación, y el cumplimiento de la ley y normativas vigentes.

En fin, un SGSI, brinda a las organizaciones la oportunidad de mejorar su imagen corporativa, aumentar su valor comercial, aprovechar nuevas oportunidades de negocio, etc. Que son el sinónimo de éxito o el cumplimiento de los objetivos corporativos.

Figura 1. Relación entre los riesgos, vulnerabilidades, amenazas, controles y activos

Fuente: http://www.iso27000.es/

5.2.6 Componentes de un SGSI. Entre los componentes de un SGSI, tenemos:

Manual de seguridad: documento que contiene las directrices que mediante un enfoque preventivo, disuasivo, correctivo y detectivo, reducen la probabilidad de los incidentes de seguridad contra los sistemas de información, además incluye el alcance, las políticas, los objetivos, las responsabilidades, la gestión de procesos, etc. Que deben ser asumidos por la organización, durante y después de la implantación del SGSI.

Procedimientos: son documentos que especifican las acciones, actividades o instrucciones técnicas a realizar durante la planeación, gestión y ejecución de los procesos del SGSI.

Instrucciones, checklists y formularios: son formatos que describen como se deben realizar las actividades de recolección de datos, verificación de operaciones, inspección de activos informáticos, comprobaciones rutinarias, etc. Para no olvidar el más mínimo detalle, relacionado con el SGSI a implantar.

Registros: son formatos que son utilizados como contenedores de evidencias de tareas realizadas por los actores involucrados del SGSI. Estos formatos se encuentran asociados al manual de seguridad, procedimientos, instrucciones, checklists y formularios, como salidas que permiten comprobar el cumplimiento de su contenido.

De manera específica, el portal ISO27001.es, indica que:

> Un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):
>
> - Alcance del SGSI

- Política y objetivos de seguridad
- Procedimientos y mecanismos de control que soportan al SGSI
- Enfoque de evaluación de riesgos
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Procedimientos documentados
- Registros
- Declaración de aplicabilidad [13]

5.3 ESTADO DEL ARTE

5.3.1 Estándares o normas utilizados para la seguridad de la información. En la actualidad, existen varios estándares o normas que establecen metodologías, políticas, técnicas y procedimientos relacionados con la seguridad de la información como: el análisis y gestión de riesgos, gestión de activos, continuidad de negocio, control de acceso, etc. Que son desarrollados y publicados por prestigiosas instituciones mundiales con el fin de brindar las herramientas que permiten gestionar la seguridad de los sistemas informáticos de las organizaciones para mantener la integridad, disponibilidad y autenticidad de los datos. Entre los estándares y metodologías más conocidas y relevantes, tenemos:

5.3.1.1 BS7799-3. Fue publicada en marzo de 2006 por (British Standards Institution), y el portal ISO27001.es, describe que: “Profundiza aspectos y da directrices sobre evaluación de riesgos, tratamiento de riesgos, toma de decisiones por parte de la Dirección, re-evaluación de riesgos, monitorización y revisión del

[13] ISO27001.es. Sistema de Gestión de Seguridad de la Información. {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

perfil de riesgo, riesgos de seguridad de la información en el contexto del gobierno corporativo y conformidad con otros estándares y regulaciones sobre el riesgo” [14] .

5.3.1.2 COBIT. Su última versión (COBIT 5), fue publicada por ISACA el 10 de abril de 2012. Esta metodología se empeña principalmente en la creación de valor para las empresas, integrando otras normas como Val IT y Risk IT, ITIL, e ISO para ayudar a las PYME o a las grandes empresas a optimizar los servicios, coste de las TIC, apoyar el cumplimiento de la legislación vigente, reglamentos, acuerdos contractuales y las políticas que permiten, sostener un equilibrio entre los beneficios obtenidos y la buena utilización de los recursos.

Conforme a Carlos Francabilla, “Cobit se basa en cinco principios:

0. Satisfacer las necesidades de las Partes Interesadas
1. Cubrir la Compañía de Forma Integral
2. Aplicar un solo Marco Integrado
3. Habilitar un Enfoque Holístico
4. Separar el Gobierno de la Administración” [15] .

El estándar Cobit, se divide en cuatro dominios compuestos por procesos relacionados a responsabilidades personales que se derivan de una serie de actividades o tareas para el cumplimiento de los objetivos de control. La tabla 2, ilustra dichos dominios y procesos.

[14] ISO 27000.ES. El portal de ISO 27001 en español. {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.iso27000.es/iso27000.html

[15] FRANCABILLA, Carlos. Como aporta COBIT 5 y gobernanza de TI a la gobernanza empresarial {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014-COBIT%20y%20Gobernanza%20de%20TI.pdf

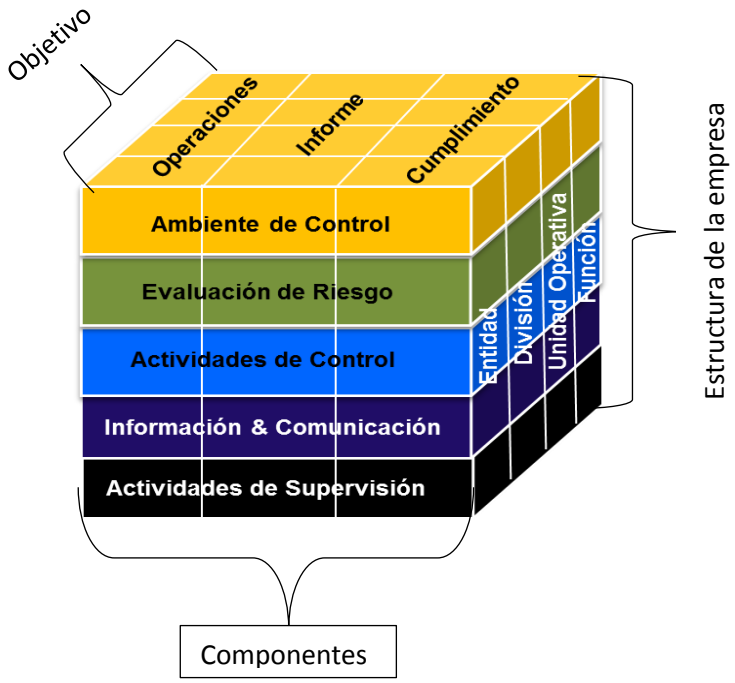
Tabla 2. Dominios y procesos del estándar COBIT

Dominios	Procesos
Planeación y organización (po)	PO1 Definir un Plan Estratégico de TI. PO2 Definir la Arquitectura de Información. PO3 Determinar la dirección tecnológica. PO4 Definir la Organización y Relaciones de TI. PO5 Manejar la Inversión en TI. PO6 Comunicar las directrices gerenciales. PO7 Administrar Recursos Humanos. PO8 Asegurar el cumplir Requerimientos Externos. PO9 Evaluar Riesgos. PO10 Administrar proyectos. PO11 Administrar Calidad.
Adquisición e implementación (ai)	AI1 Identificar Soluciones. AI2 Adquisición y Mantener Software de Aplicación. AI3 Adquirir y Mantener Arquitectura de TI. AI4 Desarrollar y Mantener Procedimientos de TI. AI5 Instalar y Acreditar Sistemas. AI6 Administrar Cambios
Servicios y soporte (ds)	DS1 Definir niveles de servicio. DS2 Administrar Servicios de Terceros. DS3 Administrar Desempeño y Calidad. DS4 Asegurar Servicio Continuo. DS5 Garantizar la Seguridad de Sistemas. DS6 Identificar y Asignar Costos. DS7 Capacitar Usuarios. DS8 Asistir a los Clientes de TI. DS9 Administrar la Configuración. DS10 Administrar Problemas e Incidentes. DS11 Administrar Datos. DS12 Administrar Instalaciones. DS13 Administrar Operaciones
Monitoreo (m)	M1 Monitorear los procesos. M2 Evaluar lo adecuado del control Interno. M3 Obtener aseguramiento independiente. M4 Proveer auditoría independiente.

Fuente: https://sites.google.com/site/auditoriaeninformaticacun/cobit/dominios-y-procesos

5.3.1.3 COSO (Committee of Sponsoring Organizations of Treadway Commission), es una metodología desarrollada en 1985 por iniciativa de organizaciones privadas norteamericanas, especialmente, del sector financiero con el fin de definir controles, políticas, normas y técnicas de seguridad informática, que pudieran detectar factores causantes de procesos fraudulentos y reducir su incidencia.

Figura 2. Relación entre componentes y principios de COSO



Fuente: http://auditoriadegestioncoso1.blogspot.com.co/2015/05/coso-i.html

5.3.1.4 NIST (National Insitute of Standards and Technology). Metodología norteamericana propuesta como estándar para promover la innovación tecnológica y la competitividad industrial en los Estados Unidos, de la cual hacen parte las medidas preventivas y de fiabilidad de los sistemas de información. Tiene una serie de publicaciones entre las que se destacan:

- **800-37**: guía que recomienda una serie de procedimientos que, aplicados de manera ordenada, permiten gestionar y administrar los riesgos que atentan contra los sistemas informáticos de las organizaciones federales.
- **800-53**: publicación de actualización de la metodología realizada en agosto de 2009. Su objetivo principal es la evaluación efectiva de sus 194 controles de seguridad, cuya implementación permiten gestionar sistemas informáticos más seguros y de mayor confiabilidad.
- **800-55**: publicación realizada en 2003 con revisión en 2007, es una guía con medidas de seguridad recomendadas a implementar especialmente, en las infraestructuras TIC.
- **800-80**: su publicación se realizó en el año 2006, está compuesta por un conjunto de medidas o controles recomendados para la protección de la información que es utilizada para los procesos empresariales de los estados federales.

5.3.1.5 Normas ISO/IEC 27000. Es un conjunto de normas recomendadas por la ISO (Organización Internacional para la Estandarización) y por la IEC (Comisión Electrónica Internacional) para el diseño, implementación y desarrollo de un SGSI, en todo tipo de organización.

Las normas están orientadas a la protección de la información que es generada, almacenada y transmitida por los diferentes dispositivos que conforman las infraestructuras tecnológicas, a través de una serie de requerimientos que son necesarios para poder diseñar e implementar los controles, las políticas y procedimientos que por su parte deben estar bien documentados con el fin de revisar, mantener y mejorar continuamente el SGSI, implementado en la organización destino.

A continuación, se describen algunas de las normas que hacen parte del conjunto ISO/IEC 27000.

- **ISO/IEC 27000**: define la terminología y la conceptualización que engloba los estándares 27000.
- **ISO/IEC 27001**: como se mencionó anteriormente, especifica los requisitos que son esenciales para establecer un SGSI, determina las responsabilidades de los actores involucrados, establece los procedimientos para la gestión de riesgos y se basa en el ciclo (PHVA) para el mejoramiento continuo del SGSI.
- **ISO/IEC 27002**: formula un conjunto de reglas orientadas a las buenas prácticas con el fin de proteger los sistemas informáticos, exponiendo medidas preventivas para evitar o minimizar las amenazas que ponen en riesgo, la seguridad de la información.
- **ISO/IEC 27003**: es una guía cuyo interés es describir los pasos adecuados para la exitosa implementación de un SGSI.
- **ISO/IEC 27004**: define mecanismos de medición para evaluar el desempeño de un SGSI y decidir si uno o más controles deben ser mejorados o cambiados.
- **ISO/IEC 27005**: determina las directrices que permiten gestionar los riesgos que afectan la seguridad de la información, además sirve de apoyo a la conceptualización general de la norma ISO/IEC 27001.
- **ISO/IEC 27006**: es una guía de requisitos y procedimientos que deben cumplir y gestionar, los organismos auditores y certificadores de los sistemas de gestión y seguridad de la información, implantados en las organizaciones.
- **ISO/IEC 27007**: es una guía que especifica los lineamientos que deben seguir los organismos auditores para poder realizar auditorías a los SGSI que se han establecido en las organizaciones.

- **ISO/IEC 27011**: define los procedimientos, políticas y medidas preventivas que permiten minimizar las amenazas que afectan los sistemas de telecomunicaciones.
- **ISO/IEC 27031**: es una guía que define las técnicas, políticas y procedimientos adecuados que debe seguir una organización para conseguir la continuidad del negocio ante un evento comprometedor del funcionamiento en una o varias partes del sistema de tecnologías de la información y las comunicaciones.
- **ISO/IEC 27032**: determina una serie de directrices de seguridad con el fin de gestionar y reducir los riesgos que continuamente amenazan los recursos integrados en internet. Proporciona una serie de acciones para manejar los incidentes y hacer más seguros los procesos que tienen que ver con la información que se maneja a través de la red en todo el mundo.

5.3.2 Norma ISO/IEC 27001. La norma ISO/IEC 27001 es un documento que contiene una serie de recomendaciones técnico-organizativas de buenas prácticas para gestionar la seguridad del sistema informático de una organización a bajo costo, de tal forma que le permita en todo momento mantener la calidad de la información que utiliza, en los diferentes procesos organizacionales.

El portal, advisera.com, afirma que: "La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2" [16] .

5.3.2.1 Funcionamiento de la ISO/IEC 27001. Como se mencionó anteriormente, el objetivo principal de la norma, es proteger la información de una organización a

[16] advisera.com. ¿Qué es norma ISO 27001? {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://advisera.com/27001academy/es/que-es-iso-2700

través de una serie de controles de seguridad, políticas y mecanismos tecnológicos, que permitan mantener su integridad, confidencialidad y disponibilidad. Para ello, se deben realizar dos actividades centrales:

- Evaluación de riesgos (procedimiento investigativo que permite determinar las amenazas que podrían causar un efecto negativo a la información)
- Tratamiento de riesgos (recomendación de los recursos que son necesarios establecer para contrarrestar o evitar el impacto o accionar de las amenazas)

Además de implementar las técnicas, controles y procedimientos para evaluar y tratar los riesgos, la norma ISO/IEC 27001, determina los reglamentos que son necesarios cumplir para gestionar los procesos de seguridad de la información de manera eficiente y eficaz, evitando sensaciones incomodas al recurso humano, protegiendo las instalaciones físicas y demás recursos de la organización.

La norma contiene los requisitos que son esenciales para establecer un SGSI, proporcionando un marco estandarizado de procedimientos que pueden ser aplicados en todo tipo de organización sin tener en cuenta su objetivo económico, su naturaleza o su estructura, con el fin de brindar confidencialidad, integridad y disponibilidad de los datos e integrando procesos de mejora continua para garantizar el éxito de los procesos organizacionales.

5.3.2.2 Importancia de la ISO/IEC 27001. De acuerdo al portal advisera.com [17] , la empresa que implante la norma ISO I27001, obtiene los siguientes beneficios:

1. Cumplimiento de requerimientos legales: debido a la proporcionalidad directa entre delitos informáticos y leyes estatales e internacionales, muchas

[17] Ibídem

organizaciones se ven en apuros para demostrar que protegen adecuadamente, sus sistemas de información, por eso, la ISO/IEC 27001, facilita los métodos suficientes y necesarios para dar cumplimiento a los requerimientos de ley.

2. Ventaja competitiva: si una organización demuestra o certifica la forma segura como gestiona su información, indica que va a tener un alto porcentaje de sostenibilidad en el tiempo, aumento de rentabilidad, un mejor desempeño y mayor fidelidad de clientes al contar con información integra, confiable y disponible a todo momento para sus procesos organizacionales y productivos.

3. Menores costos: además de evitar la acción de las amenazas sobre la información de una empresa, la inversión que esta debe hacer en adquirir la ISO/IEC 27001 le va a resultar mucho menor, si se pierden o se dañan datos o registros que son vitales para un determinado proceso comercial o productivo, ante el impacto de un incidente.

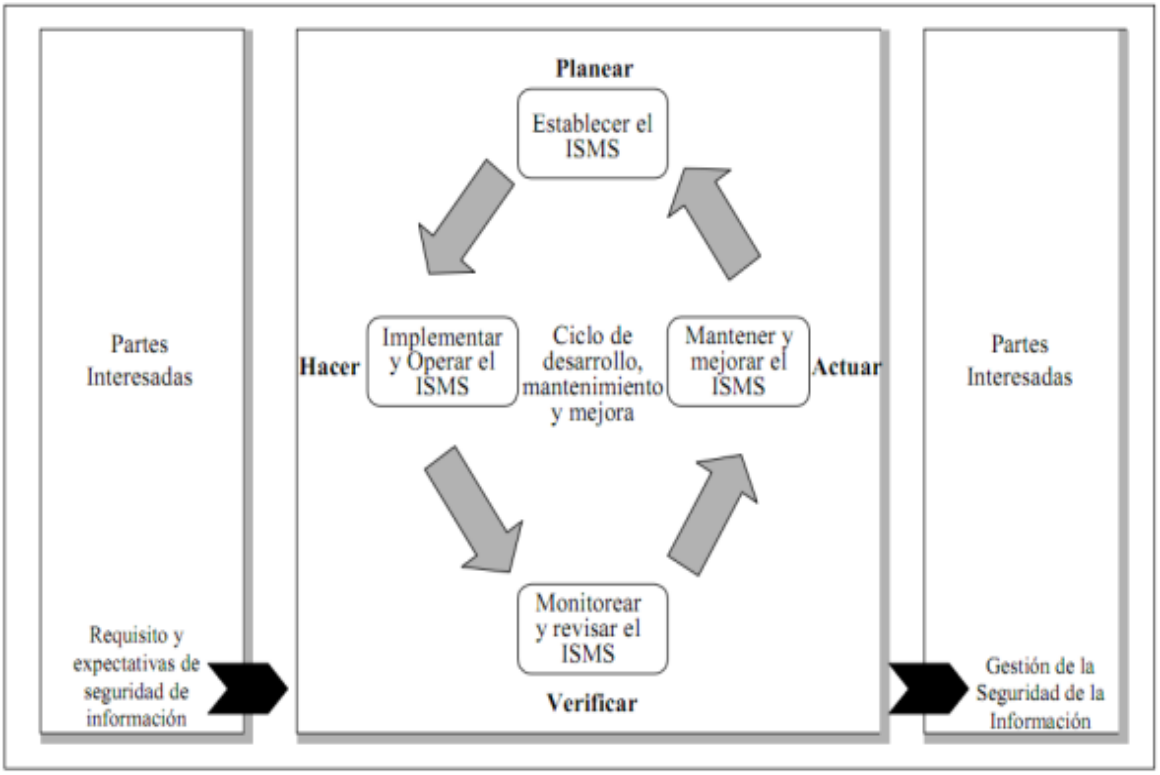
4. Mejor organización de procesos empresariales: las organizaciones generalmente, tienden a apoyar su transformación mediante ajustes o modificación en los procesos operativos, cambios de actitud del recurso humano, mejor estructura organizacional, externalización de servicios, etc. Haciendo uso de nuevas tecnologías con el fin de fortalecer su desempeño, productividad y objetivos de negocio, lo que conllevaría a establecer procedimientos de organización y control en sus operaciones productivas y de confidencialidad comercial, que es precisamente uno de los grandes beneficios que aporta la norma ISO/IEC 27001 en cuanto al manejo y uso de las tecnologías de la información.

En Colombia, la norma fue adoptada por el ICONTEC, y fue ratificada por el consejo directivo, el 22 de marzo de 2006 como NTC-ISO/IEC 27001. Contiene un total de 181 técnicas de seguridad de la información, en cuyo estudio e implementación

colaboraron un total de 16 empresas y otras 61 que actuaron como consultoras públicas de la norma.

La norma ha sido promovida para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización, adoptando el modelo de procesos: Planificar-Hacer-Verificar-Actuar (PHVA), que se aplica para estructurar todos los procesos del SGSI en las organizaciones, cuyas acciones y procesos se resumen en la figura 3

Figura 3. Modelo PHVA



Fuente: https://www.google.com.co/search?q=modelo+pdca&biw=1366&bih=657&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiI3-qeob_PAhVIJB4KHbkvDxIQ_AUIBigB#imgrc=ItuYEnzXtrhxpM%3A

Planear: establecer el SGSI

- Creación de las Políticas de seguridad
- Descripción del alcance del SGSI
- Identificación de los activos informáticos
- Análisis y gestión de riesgos
- Selección de controles
- Análisis de condiciones para aplicar el SGSI

Hacer: implementar y utilizar el SGSI

- Implementación del SGSI
- Implementación del proceso de gestión de riesgos
- Determinación e Implementación de controles para la gestión de los incidentes de seguridad
- Capacitación y concienciación de usuarios

Verificar: monitorear y revisar el SGSI

- Monitorización de las actividades en el sistema de información para establecer la eficiencia del SGSI implementado o las deficiencias del mismo.
- Revisión regular de los niveles de seguridad implementados por el SGSI para analizar la efectividad de los controles y el cumplimiento de la política de seguridad
- Realización de auditorías internas para fortalecer las actividades de monitorización y revisión

Actuar: mantener y mejorar el SGSI

- Implementación de mejoras en el sistema para que exista una mayor repercusión en relación con el cumplimiento de los objetivos propuestos por la organización
- Implementar acciones preventivas y correctivas para el mejoramiento y robustez del sistema.

El documento NTC-ISO/IEC 27001 de ICONTEC señala que:

Los requisitos establecidos en la norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza. La organización que, a bien, acepte y declare la conformidad con la norma, bajo ninguna circunstancia, puede omitir 5 requisitos elementales para evitar posibles sanciones, ellos son:

1. **Sistema de gestión de la seguridad de la información.** La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta. Para los propósitos de esta norma, el proceso usado se basa en el modelo PHVA.

2. **Responsabilidad de la dirección.** La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI.

3. **Auditorías internas del SGSI.** La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI.

4. **Revisión del SGSI por la dirección.** La dirección debe revisar el SGSI de la organización a intervalos planificados (por lo menos una vez al año), para asegurar su conveniencia, suficiencia y eficacia continuas. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros.

5. **Mejora del SGSI.** La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos

de seguridad de la información, los resultados de la auditoría, el análisis de los eventos a los que se les ha hecho seguimiento, las acciones correctivas y preventivas y la revisión por la dirección [18] .

5.3.3 Gestión de riesgos. Metodologías. La gestión de riesgos, es considerado el proceso más importante para lograr el éxito de la implementación de un SGSI, pues es el que permite determinar el nivel de seguridad del sistema informático de la empresa objetivo, teniendo en cuenta como primera medida, la identificación rigurosa de los diferentes elementos (activos informáticos) que conforman la infraestructura tecnológica y las áreas en las que se encuentran dispuestos para poder establecer los riesgos a los que se encuentran expuestos, estimar la magnitud de los mismos, conocer su probabilidad de ocurrencia y el impacto económico que se deriva como consecuencia de un fallo sobre el sistema; y con ello, tener conclusiones precisas que permitan una buena toma de decisiones para evitar inversiones o adopción de medidas de seguridad desproporcionadas por parte de la organización.

Por eso, la gestión de riesgos se apoya en una serie de criterios que mediante acciones sucesivas permiten el mejoramiento continuo del SGSI para alcanzar el nivel de seguridad pretendido por la organización. De ahí, la necesidad de hacer uso de métodos que sistemáticamente, faciliten de manera organizativa las diferentes actividades de estos dos procesos que conforman la gestión de riesgos.

[18] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Norma Técnica Colombiana NTC-ISO/IEC 27001. Marzo de 2006. {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

Entre las metodologías más importantes para realizar el análisis y tratamiento de riesgos en una organización tenemos: Octave, Nist SP 800-30, Mehari, ISO 27005, y Magerit. Para las cuatro primeras se dará una descripción general de cada una de ellas, mientras que la metodología Magerit, por ser la seleccionada para el desarrollo del presente proyecto, centraremos nuestro estudio con más detalle en su estructura, debido a que los resultados obtenidos de la gestión de riesgo se pueden expresar en valores cualitativos y cuantitativos, lo que implica una mejor toma de decisiones por parte de los dirigentes de la cooperativa.

5.3.3.1 OCTAVE. Es una metodología que está enfocada a las pequeñas y medianas empresas, orientada a los procesos de planificación y consultoría en seguridad informática, enfocados principalmente en la evaluación de los riesgos operativos que se derivan del uso masivo de las tecnologías informáticas, permitiendo a las organizaciones, disponer de técnicas, procedimientos y buenas prácticas de seguridad para mantener la confidencialidad, integridad y disponibilidad de la información mediante el buen manejo de los recursos que la gestionan.

Acorde a Duque Ochoa;

> El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos.
>
> - Identificación de la información a nivel gerencial.
> - Identificación de la información a nivel operacional.
> - Identificación de la información a nivel de usuario final.
>
> Estos tres pasos dan lugar a otros 5 procesos para completar los 8 puntos de los que consta OCTAVE
>
> - Consolidación de la información y creación de perfiles de amenazas.

- Identificación de componentes claves.
- Evaluación de componentes seleccionados.
- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección [19] .

5.3.3.2 NIST SP 800-30: La metodología National Institute of Standards and Technology (NIST), está compuesta por un conjunto de documentos cuyo contenido se centra en la aplicación de procedimientos y normas enfocados a la seguridad de la información. Desde 1990 ha venido realizando una serie de publicaciones entre las que se destaca la (SP 800), dedicada exclusivamente al análisis y gestión de riesgos de los sistemas informáticos.

La guía de evaluación de riesgos de NIST (9/18/2012), describe lo siguiente:

> La NIST SP 800-30, está compuesta por 9 tareas o procesos que se deben seguir de manera ordenada para obtener los resultados previstos, esos procesos son;
>
> - Caracterización de Sistemas.
> - Identificación de amenazas.
> - Identificación de vulnerabilidades.
> - Análisis de controles.
> - Determinación de probabilidades.
> - Análisis de impacto.
> - Determinación del riesgo
> - Recomendación de controles.

[19] DUQUE OCHOA, Blanca Rubiela. Metodologías de gestión de riesgos (OCTAVE, MAGERIT, DAFP). {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

- Documentación de resultados [20] .

5.3.3.3 MEHARI. Es una metodología que fue diseñada de tal manera, que permite actualizaciones constantes y es muy utilizada en actividades relacionadas generalmente, a la seguridad informática, aunque también está ampliamente relacionada con los procedimientos encaminados a la gestión de riesgos, tarea básica para implementación de un SGSI. Su estructura está definida mediante 7 procesos.

1. Evaluación de la exposición natural del riesgo
2. Evaluación de los factores disuasivos y preventivos
3. Evaluación de la potencialidad del riesgo
4. Evaluación del impacto intrínseco
5. Evaluación de factores protectores, paliativos y recuperativos
6. Evaluación y reducción del impacto
7. Evaluación global de los riesgos

5.3.3.4 ISO 27005. Es una norma cuya primera publicación se realizó el 4 de Junio de 2008, y desde entonces se han venido realizando una serie de actualizaciones y publicaciones con el objetivo de ofrecer procedimientos que permitan apoyar y desplegar plataformas solidas de protección frente a las amenazas que buscan la manera de explotar las vulnerabilidades que presentan los sistemas informáticos; y con ello, incrementar los riesgos que pueden causar un impacto altamente negativo en la seguridad de la información.

[20] NIST. Risk Management Guide for Information Technology Systems Julio de 2002. {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Por eso, proporciona una serie de directrices para dar soporte a las actividades de la gestión de riesgos, uno de requisitos más importantes para implementar con éxito, un SGSI bajo la norma ISO 27001, metodología que a su vez no especifica un método AGR en particular, si no que permite quedar a criterio de la organización.

Como bien lo indica Diego Espinosa, *et al*. La norma ISO 27005 cuenta con 7 pasos los cuales son:

1. Establecimiento del contexto
2. Identificación del riesgo
3. Estimación del riesgo
4. Evaluación del riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Comunicación del riesgo [21] .

5.3.3.5 MAGERIT. Es una metodología de análisis y gestión de riesgos para los sistemas de información, la cual presenta una estructura de tal forma que soporta de manera flexible y satisfactoria un proyecto de investigación o de aplicación, pues permite la identificación y evaluación de los riesgos a los que diariamente se ve sometido un sistema informático y las consecuencias que de ellos se derivan. De ahí, que este modelo establece unos principios para planificar, conocer y ajustar una estructura informática antes de ser desarrollada o realizar las modificaciones necesarias si esta ya existiese, en aras de mantener un sistema funcional, económico y seguro.

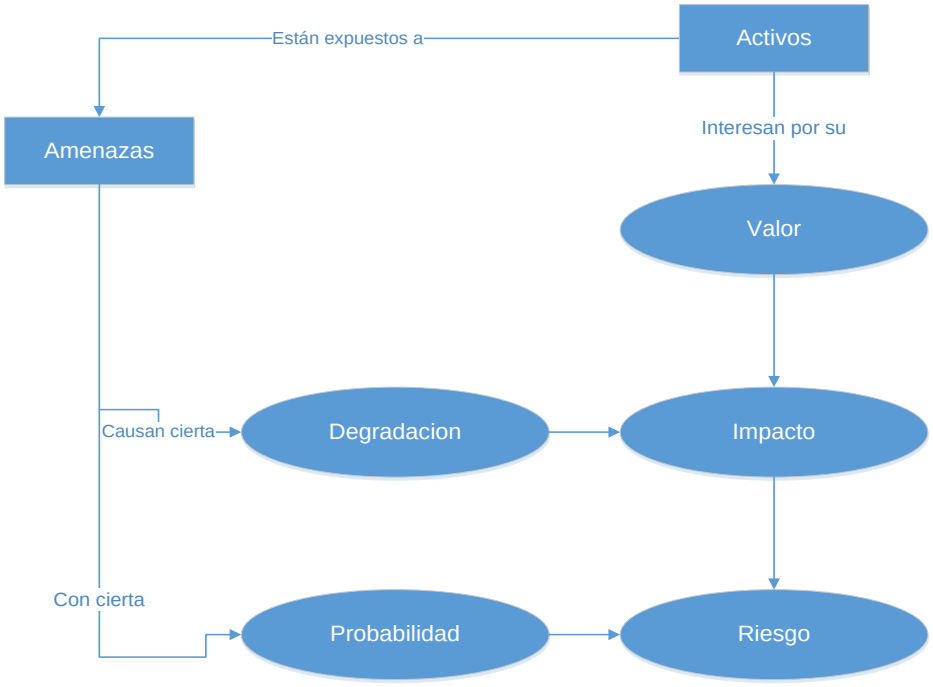
[21] ESPINOSA T Diego, MARTÍNEZ P Juan, AMADOR D Siler. Gestión del riesgo en la seguridad de la información con base en la norma iso/iec 27005 de 2011, proponiendo una adaptación de la metodología octave-s. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control académico (darca) de la universidad del cauca. Febrero de 2014. {En línea}. {Consultado en noviembre de 2016}.disponible en: http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion.

La metodología se encuentra estructurada en tres partes a saber:

A Método: compuesta por cinco pasos determinados por procedimientos bien definidos para realizar la gestión de riesgos en un sistema de información, dichos pasos son:

1. Inventario de activos y su valoración
2. Identificación de amenazas y valoración de las mismas
3. Determinación de salvaguardas para enfrentar los riesgos
4. Estimación del impacto de las amenazas sobre los activos
5. Estimación de los riesgos o expectativa de la confirmación de las amenazas sobre los activos

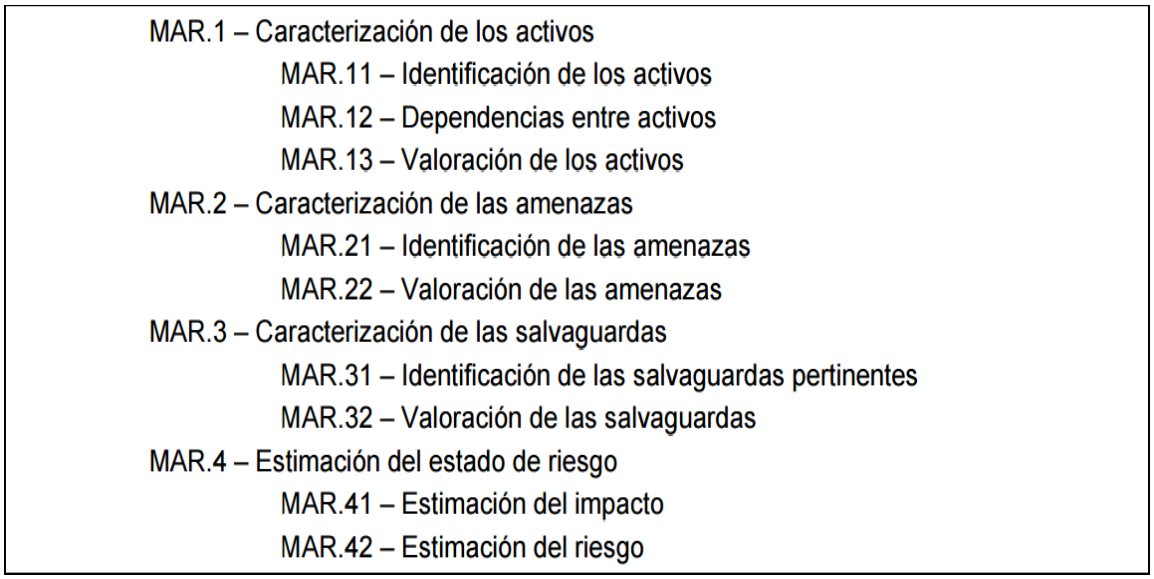
Figura 4. Elementos del análisis de riesgos potenciales



Fuente: MAGERIT 3.0, (Libro 1, P.28)

Estos cinco pasos hacen relación a las actividades que son relevantes para el desarrollo de la gestión de riesgos MAR.

Figura 5. MAR – Método de Análisis de Riesgos



Fuente: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

B Catálogo de Elementos: parte de la metodología que permite establecer la clasificación de los activos informáticos de acuerdo al tipo y teniendo en cuenta un código de identificación, la valoración de los mismos conforme a las dimensiones de seguridad. También establece un catálogo de amenazas típicas sobre los sistemas informáticos, y presenta una clasificación de salvaguardas a tener en cuenta para brindar protección a un sistema informático.

C Guía de Técnicas: es la parte que describe los procedimientos y métodos que se deben utilizar para la valoración cuantitativa y cualitativa de los activos, así como

la magnitud del impacto de los riesgos sobre los activos informáticos, presentando los resultados de forma gráfica y detallada.

La metodología se centra principalmente en el análisis del impacto que pueden generar los riesgos en una organización, basándose en la identificación de las vulnerabilidades que pueden ser aprovechadas por las amenazas para afectar el sistema informático y de esta manera, identificar los controles preventivos y correctivos más apropiados para poder contar con un sistema generador de información de alta calidad. Por eso, la metodología está bien alineada con el estándar ISO/27001, que busca que las organizaciones se certifiquen y cumplan con los requerimientos legales que contempla la seguridad informática mediante un ciclo de mejora continua a través de sus cuatro etapas: planificar, hacer, verificar y actuar.

Precisamente, de la fase Planificar, hace parte el análisis y gestión de riesgos AGR, considerada como la etapa más importante de un sistema de seguridad, la cual es apoyada por la implementación de los objetivos, estrategia, normativa, política y definición del alcance del SGSI.

Por eso, para la etapa AGR, se han diseñado modelos con una serie de componentes y técnicas que buscan identificar los riesgos para establecer las salvaguardas y obtener el beneficio esperado, proporcional al coste que implica el desarrollo de las fases que componen un SGSI; de ahí, la necesidad de realizar una buena toma de decisiones, y el modelo MAGERIT no ha sido ajeno a dicho objetivo.

El modelo MAGERIT, ha sido diseñado de acuerdo a dos propósitos. Uno, investigar los riesgos a los que está sometido un sistema informático y los posibles daños que les podrían sobrevenir, y dos, sugerir las medidas oportunas y apropiadas a implementar con el fin de prevenir, disuadir, corregir o minimizar los riesgos resultantes del estudio investigativo.

Según esto, Duque Ochoa señala que: MAGERIT persigue los siguientes objetivos.

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso [22] .

5.3.3.5.1 Paso 1: inventario y valoración de activos. Este paso permite identificar los recursos informáticos (hardware, software) y recurso humano que la organización posee y necesita para realizar las diferentes operaciones productivas y alcanzar los objetivos propuestos. Para lograr esta tarea de manera eficiente, es necesario el apoyo de las personas responsables del manejo del sistema informático de la empresa. MAGERIT, hace una diferenciación de los activos agrupándolos en varios tipos conforme a la función relacionada con en el procesamiento de la información. La tabla 3 establece la relación de cada tipo de activo según MAGERIT

[22] DUQUE OCHOA, Blanca Rubiela. Metodologías de gestión de riesgos (Octave, Magerit, Dafp). {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

Tabla 3. Clasificación de activos según MAGERIT

Tipos de activos	Descripción
Activos esenciales	Información que se maneja, p.e, (bases de datos, contratos, manuales de usuario, políticas, pólizas de seguros etc. Servicios prestados
Servicios internos	Los que estructuran ordenadamente el sistema informático, p.e, (conexión a internet, mantenimiento, apoyo logístico, soporte a usuarios, mejoramiento de procesos, etc.)
Equipamiento informático	Equipos informáticos (hardware) Aplicaciones (software) Comunicaciones (dispositivos y elementos de conectividad física o inalámbrica). Soportes de información (discos duros, pendrives, cintas magnéticas, etc.)
Activos del entorno	Equipos para el suministro de energía, sistemas SAI, sistema de climatización, red del acueducto, etc. Mobiliario
Servicios subcontratados a terceros	Help Desk, DRP, mantenimiento y soporte de infraestructura de TI, consultoría, capacitación, etc.
Instalaciones físicas	Entorno físico del CPD, instalaciones eléctricas, arquitectura de la red, y características generales del edificio.
Recurso humano	Personal ejecutivo Personal administrativo Operarios Usuarios, etc.

Fuente: Magerit 3.0, Libro I. P.24

Valoración de los activos: para valorar cada activo no es tan relevante el precio que paga la empresa para adquirirlo, si no teniendo en cuenta los costos relacionados a dos variables diferentes

1. El costo de acuerdo a la función que cumple en el sistema informático. Cuanto mayor es su función, mayor debe ser su nivel de protección.
2. El costo que implica ponerlo nuevamente en funcionamiento debido a una falla de seguridad o por deterioro del mismo.

De acuerdo a Magerit 3.0, Libro I. p.25, esta segunda variable está sujeta a varios factores a considerar:

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales [23] .

Magerit 3.0, libro II. P.24, también expone que la valoración de los activos es proporcional al nivel de protección requerida en cinco dimensiones de seguridad.

[23] INSTITUTO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Metodología de análisis y gestión de riesgos de los sistemas de información. {En línea}. Octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WABC-cmdDIU

Confidencialidad: principio o característica que garantiza que la información debe ser accedida exclusivamente por las personas autorizadas; por lo tanto, bajo ninguna circunstancia puede ser suministrada a personas ajenas. Esta característica conlleva a que la información debe estar es protegida bajo normas éticas, legislativas y técnicas. Desde el punto de vista técnico, la seguridad informática aporta herramientas que apoyan el cumplimiento de la confidencialidad de la información como la criptografía o la esteganografía.

Integridad: permite asegurar que los datos recibidos o recuperados son exactos y completos, es decir, que no han sufrido ningún tipo de modificación durante la transmisión de los mismos. Una de las técnicas que garantiza este principio son los algoritmos de cifrado o la firma digital.

La ley 527 de 1999 formulada por el Congreso de Colombia, presenta la siguiente definición de firma digital: "se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación"[24].

Disponibilidad: principio que garantiza que la información debe ser accesible por las personas autorizadas en el momento de requerirla para el cumplimiento de sus funciones y correcta operatividad de la organización.

Existen una variedad de riesgos que atentan contra esta dimensión de la seguridad como los cortes de suministro eléctrico, daños o rupturas de los medios físicos e

[24] CONGRESO DE COLOMBIA. Ley 527 de 1999 (agosto 18). {En línea}. Disponible en: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

inalámbricos del sistema de telecomunicaciones, inundaciones, la denegación de servicios, software malicioso, etc.

Una de las técnicas aplicadas ante este tipo de eventos son los planes de contingencia.

Autenticidad: principio que garantiza la identidad y validez de quien solicita acceso a la información y hacer uso de la misma en tiempo, forma, disposición y distribución, es decir, evita suplantación de identidades. También permite garantizar el origen o fuente de donde se emitió la información. Una técnica aplicada, son las firmas digitales.

Trazabilidad: Característica orientada a mantener y asegurar la confidencialidad e integridad de ciertos activos informáticos, mediante acciones y procedimientos que permiten registrar e identificar el acceso y uso de la información en todas sus etapas desde su origen hasta su destino, es decir, monitorizar el sistema en búsqueda de actividades o incidencias peligrosas, con el fin de evitar la violación de una política que repercutiría negativamente en la organización, como el incumplimiento de requisitos u obligaciones legales. Técnica aplicada los IDS/IPS

Según Magerit 3.0, Libro I. P. 26, la valoración a establecer sobre los activos informáticos puede ser cuantitativa y cualitativa.

Valoración cualitativa: permite calcular el valor de un activo de acuerdo a la función que cumple en el sistema informático, o sea, permite identificar la importancia relativa de los activos identificados en relación con el impacto que pueda generar una amenaza sobre los mismos, causando daños o pérdidas significativas a la organización. La tabla 4, permite relacionar este tipo de valoración.

Tabla 4. Estimación cualitativa del riesgo

Escalas		
Impacto	Probabilidad	Riesgo
MA: muy alto	**MA**: prácticamente seguro	**MA**: critico
A: alto	**A**: probable	**A**: importante
M: medio	**M**: posible	**M**: apreciable
B: bajo	**B**: poco probable	**B**: bajo
MB: muy bajo	**MB**: muy raro	**MB**: despreciable

Fuente: Magerit 3.0, Libro III. P.7

Valoración cuantitativa: mediante este modelo, el valor de un activo se estima mediante valores superiores a cero pesos, teniendo como representación matemática los números reales positivos. La tabla 5 representa un ejemplo de valoración cuantitativa.

Tabla 5. Relación entre escala cualitativa y cuantitativa

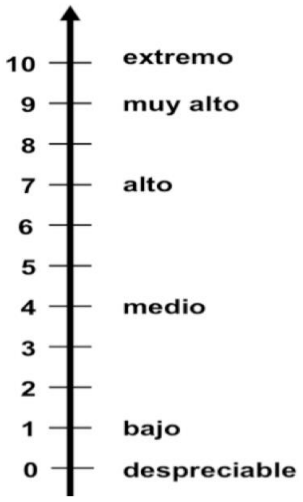
Valoración cualitativa	Escala cuantitativa	Valoración cuantitativa en $
MA: muy alto	5	[4’510.000, 10.000.000]
A: alto	4	[1’510.000, 4’500.000]
M: medio	3	[610.000, 1’500.000]
B: bajo	2	[310.000, 600.000]
MB: muy bajo	1	[0, 300.000]

Fuente: el autor

Criterios de valoración: Para establecer una valoración de activos en cada una de las dimensiones de seguridad, Magerit define unos criterios de valoración que nos permiten ubicar y posicionar cada activo con relación a cada dimensión. La tabla 6,

relaciona unos criterios a tener en cuenta a la hora de valorar activos con respecto al grado de exposición a que una amenaza se materialice sobre los mismos.

Tabla 6. Criterios de valoración de activos de acuerdo al grado de la amenaza



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

Fuente: Magerit 3.0, Libro II. P.19

5.3.3.5.2 Paso 2: identificación y valoración de amenazas. En los entornos de los sistemas informáticos organizacionales, existe una gran variedad de amenazas que pueden afectar seriamente, sus procesos productivos y de cumplimiento legal. De ahí, que el análisis de las mismas ha generado tres momentos distintos: antes de realizado un ataque, durante y después de su realización. Esto ha originado una serie de mecanismos y políticas enfocados a la prevención, detección y recuperación de los sistemas de información ante cualquier evento anómalo que pueda afectar el rendimiento del sistema, impactándolo de manera directa en cualquiera de sus cinco dimensiones de seguridad.

Identificación de amenazas: para llevar a cabo esta tarea, Magerit 3.0, Libro II. p. 25-47, presenta una clasificación de amenazas que pueden dañar un determinado

activo, esta clasificación se enumera con las letras N, I, E y A, en donde cada una representa un grupo de amenazas diferentes.

Valoración de amenazas: De acuerdo a la lista de amenazas descritas en el libro II de la metodología MAGERIT 3.0, el siguiente paso es determinar la valoración de las mismas con el fin de especificar su influencia y en cuanto puede impactar y afectar el valor del o de los activos relacionados.

Magerit 3.0, libro I. P. 28, señala que: "Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

Degradación: cuán perjudicado resultaría el valor activo. Matemáticamente se suele representar como una expresión fraccionaria sobre el valor del activo en sí.

Probabilidad: cuán probable o improbable es que se materialice la amenaza "[25].

Si la amenaza no es intencional, será más sencillo determinar la fracción del valor del activo que es afectada para calcular su perdida proporcional, pero si la amenaza es intencional la perdida proporcional es dificil de calcular debido a la magnitud del daño que esta puede causar sobre el valor del activo. De ahí que, la probabilidad de ocurrencia de una amenaza se suele representar mediante una escala nominal como lo indica la tabla 7.

[25] INSTITUTO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Magerit-versión 3.0, Metodología de análisis y gestión de riesgos de los sistemas de información. {En línea}. Octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WgJgbXa23IU

Tabla 7. Probabilidad de ocurrencia de la amenaza

	Valoración cualitativa	Valoración cuantitativa	Rango
MA	Muy alta	100	1 vez al día
A	Alta	70	1 vez cada semana
M	Media	50	1 vez cada mes
B	Baja	10	1 vez cada 6 meses
MB	Muy baja	5	1 vez cada año

Fuente: https://es.scribd.com/document/202912531/Modulo-SGSI-233003-Listo

Impacto potencial: son los daños o pérdidas que resultan de la acción de una amenaza sobre un activo, las cuales son expresadas en niveles de destrucción, modificación, denegación de servicios, etc. Para valorar cuantitativamente las consecuencias del impacto de las amenazas sobre los activos en función de los costos económicos representativos para la organización, se presenta una escala porcentual de impactos posibles sobre las dimensiones de seguridad de los activos, representados en la tabla 8.

Tabla 8. Impacto de las amenazas sobre las dimensiones de seguridad

Impacto	Valoración cualitativa	Valoración cuantitativa
MA	Muy alto	100%
A	Alto	75%
M	Medio	50%
B	Bajo	10%
MB	Muy bajo	5%

Fuente: https://es.scribd.com/document/202912531/Modulo-SGSI-233003-Listo

5.3.3.5.3 Paso 3: análisis de salvaguardas. Las salvaguardas son las medidas, procedimientos y mecanismos aplicados para reducir los riesgos que podrían afectar los activos informáticos de la organización.

De acuerdo a Magerit 3.0, Libro I. p. 31 para la selección de salvaguardas; "se debe tener en cuenta los siguientes aspectos:

- Tipo de activo que se debe proteger
- Dimensiones de seguridad que requieren protección
- Amenazas de las que debemos protegernos
- Si existen salvaguardas alternativas "[26].

Tipos de salvaguardas: Existen diferentes tipos de protección los cuales se resumen en la tabla 9

Tabla 9. Tipos de salvaguardas

Efecto	Tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Magerit 3.0, Libro I. P.34

[26] Ibíd.; p.31

5.3.3.5.4 Paso 4: Impacto residual: es la condición de posible impacto en que queda el sistema después de aplicar las salvaguardas de seguridad con el fin de modificar (reducir) el impacto potencial o la magnitud de degradación de la amenaza. En este sentido, el impacto residual debe estar muy por debajo del impacto potencial.

5.3.3.5.5 Paso 5: Riesgo residual: situación de riesgo en que queda el sistema después de aplicarse las medidas o tipos de protección una vez que se hallan identificado las vulnerabilidades y las amenazas que inciden sobre cada una de las dimensiones de seguridad. Esta situación de riesgo debe superar el riesgo potencial y toda fracción de riesgo que este por debajo de dicho nivel, no se considera como una importante amenaza; por lo tanto, puede ser aceptado por la organización o reducirse hasta un determinado punto de aceptación.

5.4 MARCO CONCEPTUAL

5.4.1 MARCO LEGAL

El uso masivo de las tecnologías de la información y las comunicaciones TIC, ha derivado el incremento de delitos informáticos los cuales pueden desencadenar consecuencias fatales como la destrucción o perdida de la información que, es el activo más crítico y valioso con el que cuentan las empresas u organizaciones para el cumplimiento de sus objetivos corporativos.

Este hecho, ha originado la creación de leyes y normas internacionales que son adoptadas e implementadas por parte de los gobiernos mundiales con el fin de

brindar los procedimientos adecuados para el aseguramiento de la información y de las tecnologías que la soportan.

Por eso, su cumplimiento es sinónimo de prevención, protección y minimización del impacto de las amenazas externas e internas, fidelidad y respeto con los derechos del cliente, mejores beneficios comerciales y evitarse infracciones gubernamentales o estatales.

5.4.2 Ley 1273 de 2009. Promulgada por el congreso de la República de Colombia, es la que está orientada a castigar los delitos y el irrespeto que se cometen contra la integridad, la disponibilidad y la confidencialidad de la información de la empresa pública y privada del país, como también la relacionada de manera individual a las personas.

Esta ley si bien es cierto, castiga con penas que van desde los 48 hasta 120 meses de prisión y desde los 100 hasta 1500 SMLMV de multa a quien comete algún tipo de delito tipificado por la ley, también promulga a través de sus 10 artículos, sobre la importancia que tiene la implementación de sistemas de seguridad para la protección de los datos, por parte de las empresas. La tabla 10, ilustra la estructura de dicha ley.

De ahí, el significado de esta ley, que se adiciona en 4 artículos al Código Penal colombiano, y cuya estructura se relaciona en la Tabla 10.

Tabla 10. Estructura de la ley 1273 de 2009

capitulo	articulo	Descripción
1. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	Artículo 269a: acceso abusivo a un sistema informático.	Hacer uso de un activo informático sin previa autorización del ente público o privado.
	Artículo 269b: obstaculización ilegítima de sistema informático o red de telecomunicación.	Aplicación de técnicas fraudulentas como denegación de servicios (dos), sabotajes o uso de programas dañinos.
	Artículo 269c: interceptación de datos informáticos.	Delito sancionado con [36, 72] meses de prisión por realizar acciones como spoofing, keylogging, phishing, botnets, etc.
	Artículo 269d: daño informático.	Delito sancionado con [48,96] meses de prisión y [100,1000] smlmv por destruir, borrar o modificar información o un sistema informático.
	Artículo 269e: uso de software malicioso.	Delito penalizado con [48,96] meses de prisión y [100,1000] smlmv por vender, traficar o hacer uso de software malicioso.
	Artículo 269f: violación de datos personales.	Delito penalizado con [48,96] meses de prisión y [100,1000] smlmv por obtener, divulgar, vender, suplantar o utilizar toda información de índole personal.

	Artículo 269g: suplantación de sitios web para capturar datos personales	Delito penalizado con [48,96] meses de prisión y [100,1000] smlmv por utilizar técnicas como web spoofing, ip spoofing, phishing, etc.
	Artículo 269h: circunstancias de agravación punitiva:	Delito penalizado con el doble o las 3/4 más que los últimos 4 delitos por cometer acciones fraudulentas contra organizaciones estatales y extranjeras que pongan en riesgo la seguridad nacional, y aún más, cuando de funcionarios públicos se trata.
2. De los atentados informáticos y otras infracciones	Artículo 269i: hurto por medios informáticos y semejantes.	Delito castigado por la ley, al realizar acciones que su superen medidas de seguridad implantadas en sistema informático para suplantar usuarios o hurtar información
	Artículo 269j: transferencia no consentida de activos.	Delito penalizado con [48,120] meses de prisión y [200,1500] smlmv por hacer uso de medios tecnológicos para hacer transferencias de un activo o patrimonio económico de una persona a otra.

Tabla 10. (Continuación

Fuente: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

5.4.3 Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones [27] .

5.4.4 Ley estatutaria 1581 de octubre 17 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales [28] .

5.4.5 Decreto 1377 de junio 27 de 2013. Por el cual se reglamenta parcialmente la ley 1581 de 2012 [29] .

[27] CONGRESO DE COLOMBIA. Ley 1341 del 30 de julio de 2009. {En línea}. 30 de julio de 2009. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles 3707_documento.pdf

[28] CONGRESO DE COLOMBIA. Ley estatutaria 1581 del 17 de octubre de 2012. {En línea}.17 de octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf

[29] MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO. Decreto 1377 del 27 de junio de 2013. {En línea}. 27 de junio de 2013. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

5.5 MARCO CONTEXTUAL

5.5.1 Cooperativa Multiactiva del Personal del SENA, COOPSENA. COOPSENA es una entidad de primer grado, de economía solidaria de responsabilidad limitada, con número de asociados y capital variable e ilimitado, vigilada por la Superintendencia de la Economía Solidaria Delegataria para el Sector Real, autorizada y acreditada con aval al programa de educación solidaria con énfasis en trabajo asociado, por la Unidad Administrativa Especial de Organizaciones Solidarias; su base social está compuesta por funcionarios del SENA activos y pensionados [30] .

5.5.2 Reseña Histórica.

RAZÓN SOCIAL: Cooperativa Multiactiva del Personal del SENA.
ACTA DE CONSTITUCIÓN: Acta 001 del día 10 de Marzo de 1965 en la ciudad de Bogotá
PERSONERIA JURÍDICA: Resolución 0365 del 13 de Julio de 1965 otorgada por la Superintendencia Nacional de Cooperativas.
PROTOCOLIZACION: Escritura Pública No. 2.105 del 27 de Julio de 1965 en la Notaría Octava del Circulo de Bogotá, a fin de dar cumplimiento al Art 30 del Decreto Ley 1.598 de 1963.
CAPITAL INICIAL: $ 7.500 aportado por los socios fundadores [31] .

[30] COOPSENA. Quienes somos. {En línea}. {Consultado en noviembre de 2016}.Disponible en: http://www.coopsena.com.co/html/somos.html

[31] Ibídem

5.5.3 Misión. Nuestro compromiso solidario es ofrecer servicios de calidad a nuestros asociados, su grupo familiar y la comunidad, contribuyendo al bienestar y desarrollo social[32].

5.5.4 Visión. Ser la entidad preferida por la calidad de sus servicios[33].

5.5.5 Política de Calidad. COOPSENA, con fundamento en su direccionamiento estratégico, satisface las necesidades de los asociados buscando el desarrollo humano y bienestar de su grupo familiar, ofreciendo servicios de crédito oportuno, eficaz, confiable y de recuperación efectiva; enmarcados en la mejora continua de la eficacia del sistema de gestión de calidad, el desarrollo y aprendizaje de nuestro talento humano, cumpliendo requisitos legales aplicables [34].

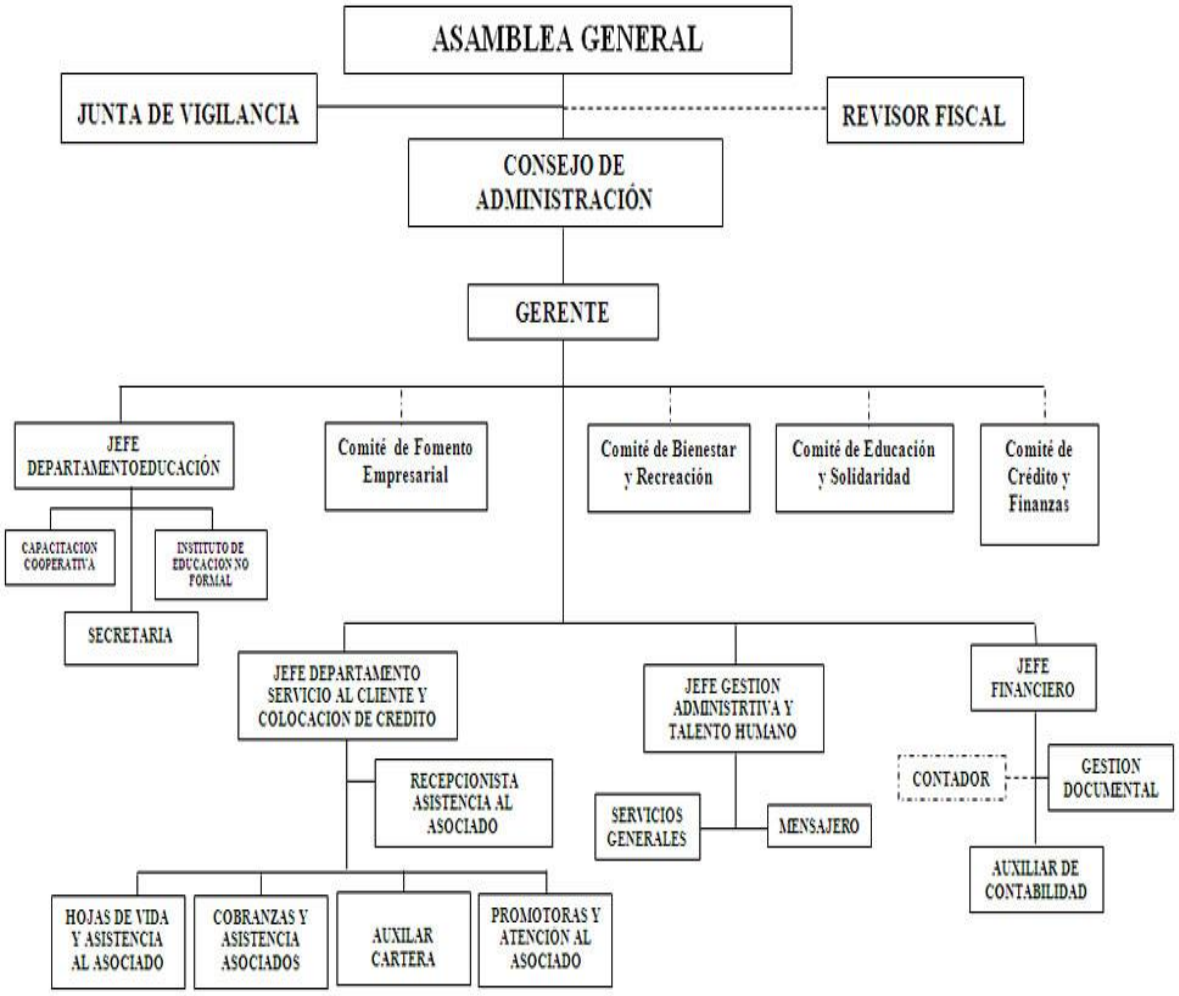
[32] Ibídem

[33] Ibídem

[34] Ibídem

5.5.6 Organigrama institucional.

Figura 6. Organigrama institucional COOPSENA



Fuente: http://www.coopsena.com.co/html/somos.html

5.5.7 Integrantes de los órganos de administración y control, periodo 2016 – 2018

Tabla 11. Consejo administrativo COOPSENA

CONSEJO DE ADMINISTRACIÓN		
CARGO	PRINCIPALES	SUPLENTES
Presidente	Aniceto Córdoba Moreno	Olga Lucía Agudelo Hernández
Vicepresidente	José Alveroni Velasco	Luz Margarita María Romero Acosta
Secretario	Heberto Guzmán Chávez	Fidel Mallama Benavides
Vocal	José Martín Díaz Villamarín	Diego González Páez
Vocal	Carmelina Espitia Mancera	Esaú Astudillo Díaz
Vocal	José Fernando Franco Hincapié	Mónica Andrade Ríos
Vocal	Fabio de Jesús Guio Jiménez	Libia del Carmen Marentes

Fuente: http://www.coopsena.com.co/html/somos.html

Tabla 12. Junta de vigilancia

UNTA DE VIGILANCIA	
PRINCIPALES	SUPLENTES
Ricardo González Badillo	Alberto Vargas Vásquez
Domingo Salas Chaverra	Luis Alberto Camacho Bolaños
Carlos Adbeiro Cruz Chávez	Daniel Holguín Pinto

Fuente: http://www.coopsena.com.co/html/somos.html

Tabla 13. Revisoría fiscal y gerencia

REVISORIA FISCAL		
EMPRESA	PRINCIPAL	SUPLENTE
AUDIGRUP LTDA	Henry Mauricio Puentes Cruz	Javier Rodrigo Jiménez Amaya
GERENTE	Edgar Edwin Polanco Botello	

Fuente: http://www.coopsena.com.co/html/somos.html

6. MARCO METODOLOGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

Hernández, Fernández y Baptista 1997) sostienen que: “todo trabajo investigativo se sustenta en dos enfoques principales: el enfoque cuantitativo y el enfoque cualitativo, los cuales de manera conjunta forman un tercer enfoque: El enfoque mixto, el cual se puede utilizar para responder distintas preguntas de investigación de un planteamiento del problema”[35].

De acuerdo a este criterio, se establece que el presente estudio de investigación para diseñar un SGSI en COOPSENA, se acerca a un enfoque mixto debido a que se requiere la recolección de datos cuantitativos y cualitativos con el fin de obtener un conocimiento más claro y profundo sobre la importancia de proteger la información para una operatividad eficiencia y rentable.

6.2 METODOLOGÍA DE DESARROLLO

De acuerdo a La metodología de la Investigación de Sampieri (1997), “en la práctica, cualquier estudio puede incluir elementos de más de una de estas cuatro clases de investigación (exploratoria, descriptiva, correlacional y explicativa)”[36].

[35] HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos; BAPTISTA LUCIO, Pilar. Metodología de la investigación. {En línea}. Abril de 2006. {Consultado en octubre de 2016}. Disponible en: https://competenciashg.files.wordpress.com/2012/10/sampieri-et-al-metodologia-de-la-investigacion-4ta-edicion-sampieri-2006_ocr.pdf

[36] Ibídem

6.2.1 Investigación descriptiva. Para Sampieri (1997), citando a (Dankhe, 1986), indica que: “los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Miden y evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar”[37].

O sea, desde el punto de vista científico-investigativo, describir un fenómeno es realizar mediciones sobre el mismo. Es decir, para Sampieri (1997), “en un estudio descriptivo se selecciona una serie de cuestiones y se mide cada una de ellas independientemente, para así -y valga la redundancia- describir lo que se investiga”[38].

De acuerdo a este análisis, podemos deducir que en el presente estudio investigativo, se describen una serie de aspectos relacionados a los mecanismos y procedimientos para la protección de la información, y los requerimientos técnicos, normativos, políticos y legislativos que son necesarios establecer para salvaguardar los sistemas informáticos, y con ello contribuir al desarrollo social y económico de las organizaciones.

6.2.2 Investigación explicativa. Según La metodología de la investigación de Hernández, Fernández y Baptista (1997) señala que: “los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales.

[37] Ibídem

[38] Ibídem

Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condición se manifiesta, o por qué se relacionan dos o más variables"[39].

Esto quiere decir, que la investigación explicativa, permite exponer el porqué de la ocurrencia de un problema o fenómeno, y así poder presentar a través de las técnicas de investigación aplicadas, una propuesta de solución para resolver gran parte de los inconvenientes o problemas detectados, en este caso, en un sistema de información, buscando establecer por qué se presenta el problema, bajo qué condiciones se presenta, a quiénes afecta y cuáles son sus consecuencias.

[39] Ibídem

7. DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN COOPSENA

7.1 IMPLICACIÓN DE LOS DIRECTIVOS PARA EL DESARROLLO DEL PROYECTO

Sin lugar a dudas, que una de las principales actividades para el diseño de un SGSI y su posterior implementación, es la implicación o el apoyo de la alta dirección institucional, de lo contrario, es imposible llevar a cabo un proyecto de esta envergadura, pues son los líderes de la organización quienes deben dirigir el proceso, por ser los que conocen mejor que nadie, los diferentes procesos, objetivos y la forma como se maneja y se gestiona la información; por consiguiente, deben estar comprometidos con la gestión de los riesgos asociados a los sistemas informáticos, con los cuales, la empresa puede quedar altamente comprometida, pues estas herramientas son el corazón de las diferentes funciones para la existencia y el éxito de la misma.

Por tal motivo, se solicitó el apoyo a la gerencia de la Cooperativa y al consejo administrativo, quienes de común acuerdo, tomaron la decisión de autorizar y apoyar las diferentes actividades relacionadas al cumplimiento de los objetivos y realización del proyecto.

7.2 ALCANCE DEL PROYECTO

El desarrollo del proyecto está determinado por las siguientes actividades:

- Localización y descripción de los activos informáticos disponibles en la entidad, sobre los cuales se deben establecer medidas de protección conforme al estándar de la ISO/27001:2013.
- Identificación de los riesgos, vulnerabilidades y amenazas de seguridad presentes en los activos informáticos de la empresa.
- Análisis y evaluación de los riesgos, para establecer una calificación cualitativa o cuantitativa de sus consecuencias y gestionar su tratamiento.
- Identificación y análisis de los controles utilizados para salvaguardar los activos informáticos de la entidad.

7.3 ELECCIÓN DE LA METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

Para la gestión de riesgos del Sistema de Información de COOPSENA, se ha elegido utilizar la metodología MAGERIT, por los diferentes aspectos descritos anteriormente en el presente documento.

7.4 GESTIÓN DE RIESGOS DEL SISTEMA DE INFORMACIÓN DE COOPSENA

7.4.1 Inventario de activos: para el desarrollo de esta actividad tomamos como modelo el inventario establecido por la metodología Magerit 3.0, libro II. P. 7-13.

De acuerdo a esta clasificación, los activos informáticos disponibles en la Cooperativa Multiactiva del personal del SENA COOPSENA, se relacionan en las siguientes tablas.

Tabla 14. Activos esenciales

[ESSENTIAL] ACTIVOS ESENCIALES			
Nombre grupo de activo MAGERIT	Código grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[info] Información	[vr] datos vitales (registros de la organización)	D_admon	Hojas de vida de funcionarios. Estatutos. Acuerdos administrativos. Resoluciones. Garantías. Licencias. Convenios. Licitaciones vigentes Actas. Informes. Memorias. Autorizaciones.
		D_políticas	Políticas de salud ocupacional. Política de seguridad informática. Política interna.
		D_Contratos	Documentos de contratación privada. Contratos de arrendamiento. Manuales de contratación.
		D_Financieros	Cuentas corrientes. Cuentas de ahorro. Estados financieros. Líneas de crédito. Acciones financieras. Flujos de caja. Títulos valores. Nomina Recibos de caja menor. Notas de remisión.

		D_Inversion	Comprobantes de consignación. Comprobantes de recaudo. Extractos bancarios Recibos de pago de los impuestos. Obligaciones contraídas. Pago de contratos. Cuentas de cobro Inventarios de propiedades. Inventario de activos fijos.
		D_Polizas	Pólizas de seguros
	[Per] datos de carácter personal.	O_Financieras	Pagares Aceptaciones bancarias.
	[classified] datos clasificados	D_Historicos	Historias laborales. Documentos históricos institucionales.
		D_Proyectos	Proyectos en curso
[Services] servicios		Serv_Empresarial	Servicio de Correo electrónico Troncal telefónica Mantenimiento planta telefónica Canales dedicados de internet Mantenimiento informático general

Fuente: el autor Tabla 14. (Continuación)

Tabla 15. Archivos de datos

[D] DATOS/INFORMACIÓN			
Nombre grupo de activo MAGERIT	Código grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
Datos	[files] ficheros	Arch_gadmva	Archivos de gestión administrativa
		Arch_politicas	Archivos de las políticas de la institución
		Arch_Contratos	Archivos de contratación
		Arch_hisnt	Archivos históricos institucionales
		Arch_audit	Archivos de auditorias
		Arch_pipu	Archivos privados de interés publico
		Arch_inv	Archivos de inventarios
[backup]	Copias de Respaldo	Backup	Copia de respaldo de la información institucional
[conf]	Datos de configuración	Dtos_config	Información relacionada a la configuración de servidores , estaciones de trabajo y dispositivos de red
[int]	Datos de gestión interna	Dtos_ginst	Información de la gestión estratégica institucional
[password]	Credenciales	Contraseñas_us	Contraseñas de acceso de los usuarios al SI
[acl]	datos de control de acceso	List_caus	Lista de control con nivel de acceso de los usuarios al SI

Fuente: el autor

Tabla 16. Infraestructura de clave publica

[PUBLIC_ENCRYPTION]			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[public_encryption]	clave pública de cifra	Claves_pub	Sistema de claves publicas emitidas por CERTICAMARA para funcionarios de alto nivel de acceso al sistema mediante certificados digitales bajo el estándar X509
[disk]	cifrado de soportes de información	Cifr_disalm	Cifrado de dispositivos de almacenamiento (usb, discos duros)

Fuente: el autor

Tabla 17. Servicios

[S] SERVICIOS			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[pub]	al público en general (sin relación contractual)	S_Afiliados	Servicios ofrecidos a todo el personal de afiliados (convenios, actividades sociales, actividades solidarias y líneas de crédito)
[int]	a usuarios de la organización	S_funcionarios	Servicios ofrecidos a todo el personal de funcionarios para el buen desempeño de sus funciones.

[www]	world wide web	P_web	Página web de la entidad a través de la cual se brinda toda la información relacionada a su actividad económica.
[email]	Correo electrónico	S_email	Servicio de correo electrónico institucional
[file]	Almacenamiento de archivos	Alm_archivos	Servicio de almacenamiento de datos en la plataforma de servidores
[ftp]	Transferencia de ficheros	S_transfarch	Servicio usado por los usuarios del sistema para transferir información entre las oficinas institucionales a nivel nacional
[edi]	intercambio electrónico de datos	I_Digidatos	Sistema de intercambio de datos digitales entre las distintas sucursales del país a través del ftp.
[idm]	gestión de identidades	G_identidad	Sistema de gestión de alta y baja de usuarios.
[ipm]	gestión de privilegios	G_privilegios	Sistema de gestión de privilegios de usuarios del sistema
[pki]	infraestructura de clave pública	Inf_clavePub	Sistema de gestión de claves publicas ofrecido por Certicamara

Fuente: el autor Tabla 17. (Continuación)

Tabla 18. Aplicaciones (software)

[SW] APLICACIONES (SOFTWARE)			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
		Sist_contable	Sistema contable institucional SAPIENS
[email_server]	Servidor de correo electrónico	Sistema_correos	Sistema de correos de la Cooperativa.
[dbms]	Sistema de gestión de bases de datos	Sistema_SGBD	Sistema de base de datos de la entidad.
[office]	Ofimática	A_OF	OFFICE 2010, 2013 y 2016
[os]	Sistema operativo	A_SO	Windows XP Professional, Windows 7 Pro, Windows 10, Windows Server, Novell Small Business 6.5
[av]	Antivirus	Antivirus	Mcafee End Point Protection Suite
[backup]	Sistema de backup	A_CS	Cobian Backup

Fuente: el autor

Tabla 19. Equipos informáticos

[HW] EQUIPOS INFORMÁTICOS (HARDWARE)			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[host]	Grandes quipos	Sist_ servidores	Servidores para el almacenamiento de información y servicios tecnológicos de la institución (BD, impresión, proxy, web). HP ML 150 G3, HP DL 120 G7
[pc]	Informática personal	E_Trabajo	Computadores de escritorio

[mobile]	Informática móvil	E_portatiles	Portátiles
[backup]	Equipamiento de respaldo	E_respaldo	Servidor de respaldo
[print]	Medios de impresión	E_Impresion	Impresoras
[router]	Encaminadores	Routers	Routers
[switch]	Conmutadores	Switch	Switches
[firewall]	Cortafuegos	Firewall	Firewall basado en linux
[wap]	Punto de acceso inalámbrico	Acces Point	Acces Point
[pabx]	Centralita telefónica	C_tel	Central telefónica administrada externamente por la ETB
[ipphone]	Teléfono IP	Tel_IP	Teléfonos IP

Fuente: el autor Tabla 19. (Continuación)

Tabla 20. Redes de comunicaciones

[COM] REDES DE COMUNICACIONES			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[wifi]	red inalámbrica	Red_wifi	Red de acceso inalámbrico de la entidad.
[LAN]	Red local	Red_LAN	Red de área local encargada de gestionar todas las comunicaciones internas de la entidad.
[internet]	Internet	Internet	Servicio de interconexión nacional.

Fuente: el autor

Tabla 21. Soportes de información

[MEDIA] SOPORTES DE INFORMACIÓN			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[disk]	discos	DiscosD	Discos duros externos para el almacenamiento de información
[usb] memorias USB	Memorias USB	Memorias USB	Memorias USB para el almacenamiento y transporte de información

Fuente: el autor

Tabla 22. Equipamiento auxiliar

[AUX] EQUIPAMIENTO AUXILIAR			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[ups]	sistemas de alimentación ininterrumpida	UPS	Sistema de alimentación eléctrica ininterrumpida
[ac]	equipos de climatización	Sist_climatizacion	Sistema todo aire
		Sist_cincendios	Sistema de extintores clase A, B y C
[cabling]	[wire] cable eléctrico	Cable eléctrico	Cable que conforma el sistema eléctrico del edificio
	[fiber] fibra óptica	F.O	Elemento físico que conforma la red troncal de telecomunicaciones
		UTP cat.6	Elemento físico que conforma la red horizontal de telecomunicaciones

Fuente: el autor

Tabla 23. Instalaciones

[L] INSTALACIONES			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[building]	edificio	edificio	Edificio Las Palmas ubicado en la Calle 57 Nº 24 -11 de la ciudad de Bogotá D.C.
[local]	cuarto	Cuarto_ sistemas	Cuarto de resguardo de los dispositivos centrales del sistema informático

Fuente: el autor

Tabla 24. Personal

[P] Personal			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según COOPSENA	Nombre grupo según COOPSENA
[ue]	Usuarios externos	Af_Cadm	Afiliados y consejo administrativo
[ui]	Funcionarios	Funcionarios	Personal encargado de las diferentes tareas administrativas de la entidad.
[adm]	Administradores de sistemas	Adm_sist	Ingeniero encargado de administrar el sistema informático de la empresa

Fuente: el autor

7.4.1.1 Valoración de activos. De acuerdo a la Tabla 5, en la que se relacionan una serie de criterios de valoración tanto cualitativa como cuantitativa según

Magerit, nos apoyaremos en la valoración cuantitativa con el fin de establecer sumas matemáticas naturales que nos van a permitir obtener posibles resúmenes y un mejor entendimiento de resultados en cuanto a la importancia de cada activo para la empresa, mediante gráficos estadísticos.

Para valorar el nivel de criticidad de cada activo, utilizaremos la tabla 26, teniendo en cuenta su valor promedio de acuerdo a los valores de las dimensiones de seguridad.

Tabla 25. Criterios de valoración del nivel de criticidad de los activos

criterios de valoración de los activos	**valor relacional**	**valor cualitativo de criticidad**
El activo gestionado es altamente potente para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad.	>=4	Alto
El activo gestionado es medianamente potente para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad	>2 y <4	Medio
El activo gestionado tiene un bajo potencial para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad.	>0 y <2	Bajo
El activo gestionado es irrelevante como para para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad	= 0	N/A

Fuente: el autor

Tabla 26. Valoración de activos y nivel de criticidad

ACTIVOS		VALORACION DE ACTIVOS Y NIVEL DE CRITICIDAD						
Código grupo según Magerit	Código grupo según COOPSENA	Confidencialidad	Disponibilidad	Integridad	Autenticidad	Trazabilidad	Promedio total	Nivel de criticidad
[vr]	D_admon	5	5	4	3	3	4	Alto
	D_politicas	5	5	4	3	3	4	Alto
	D_Contratos	4	4	4	3	3	3,6	Medio
	D_Financieros	5	5	5	5	4	4,8	Alto
	D_Inversiones	5	5	5	4	3	4,4	Alto
	D_Polizas	5	5	5	4	4	4,6	Alto
[Per]	O_Financieras	5	5	5	4	3	4,4	Alto
[classified]	D_Historicos	3	3	2	1	1	2	Bajo
	D_Proyectos	4	4	4	4	3	3,8	Medio
[Services]	Serv_Empresarial	4	4	4	4	3	3,8	Medio
[files]	Arch_gadmva	5	5	5	3	3	4,2	Alto
	A_ContA	5	5	5	4	4	4,6	Alto
	A_FinanA	5	5	5	5	4	4,8	Alto

	Arch_politicas	5	5	4	3	3	4	Alto
	Arch_hisnt	5	4	4	3	3	3,8	Medio
	Arch_audit	4	4	4	3	3	3,6	Medio
	A_AuditA	4	4	4	3	3	3,6	Medio
	Arch_pipu	4	4	4	3	3	3,6	Medio
	Arch_inv	5	5	5	4	3	4,4	Alto
[backup]	Backups	5	5	5	4	4	4,6	Alto
[conf]	Dtos_Config	4	4	4	3	3	3,6	Medio
[int]	Dtos_ginst	4	4	4	3	3	3,6	Medio
[password]	Contraseñas_us	5	5	4	3	3	4	Alto
[acl]	List_caus	5	5	5	4	3	4,4	Alto
[public_encryption]	Claves_pub	5	5	5	5	5	5	Alto
[pub]	S_Afiliados	5	5	5	4	3	4,4	Alto
[int]	S_Funcionarios	4	4	4	4	3	3,8	Medio
[www]	P_Web	5	5	5	4	4	4,6	Alto
[email]	e-mail	3	3	2	1	1	2	Bajo
[file]	Alm_Archivos	5	5	4	3	3	4	Alto
[ftp]	S_transfarch	5	5	4	4	4	4,4	Alto
[edi]	I_Digidatos	5	5	5	5	4	4,8	Alto
[idm]	G_identidad	5	5	4	4	3	4,2	Alto
[ipm]	G_privilegios	4	4	4	4	4	4	Alto
[pki]	Inf_clavePub	5	5	5	5	4	4,8	Alto
[email_server]	Sistema_correo	3	3	2	1	1	2	Bajo

[dbms]	Sistema_BD	5	5	5	4	4	4,6	Alto
[office]	Her_office	3	3	2	1	1	2	Bajo
[av]	Sist_antivirus	4	4	4	3	3	3,6	Medio
[os]	Sist_operativo	5	5	5	4	4	4,6	Alto
[backup]	Sist_buckup	5	5	5	4	4	4,6	Alto
[host]	Sist_servidores	5	5	5	4	4	4,6	Alto
[pc]	E_Trabajo	3	3	2	1	1	2	Bajo
[mobile]	E_portatiles	2	2	1	1	0	1,2	Bajo
[backup]	E_respaldo	5	5	4	3	3	4	Alto
[print]	E_Impresion	1	1	1	0	0	0,6	Bajo
[router]	Router	5	5	4	3	3	4	Alto
[switch]	Switch	3	3	3	3	2	2,8	Bajo
[firewall]	Firewall	5	5	4	3	3	4	Alto
[wap]	AccesPoint	2	2	2	1	1	1,6	Bajo
[pabx]	C_tel	4	4	4	3	3	3,6	Medio
[ipphone]	Tel_IP	4	4	4	3	2	3,4	Medio
[wifi]	Red_wifi	3	3	2	1	1	2	Bajo
[LAN]	Red_LAN	5	5	5	4	4	4,6	Alto
[Internet]	Internet	4	4	4	3	3	3,6	Medio
[disk]	DiscosD	4	4	4	3	3	3,6	Medio
[usb]	USB	4	4	4	3	3	3,6	Medio
[ups]	UPS	3	3	3	3	4	3,2	Medio
[ac]	Sist_climatizacion	1	1	1	1	0	0,8	Bajo

	Sist_cincendios	1	1	1	1	0	0,8	Bajo
[wire]	Cable electrico	4	4	3	3	3	3,4	Medio
[fiber]	F.O	5	5	4	3	3	4	Alto
	UTP cat.6	5	4	4	3	3	3,8	Medio
[building]	Edificio	5	5	5	5	5	5	Alto
	Cuarto de sistemas	5	5	5	4	4	4,6	Alto
[ue]	Af_Cadm	4	4	4	4	4	4	Alto
[ui]	Funcionarios	5	5	4	4	4	4,4	Alto
[adm]	ADMS	4	4	4	4	3	3,8	Medio

Fuente: el autor Tabla 26. (Continuación)

7.4.2 Identificación y valoración de riesgos. Para llevar a cabo esta tarea tomaremos como referencia los criterios de valoración cuantitativa de amenazas relacionados en la tabla 8, el catálogo de amenazas posibles sobre los activos de Magerit 3.0, libro II. P. 25-47, los niveles de criticidad de la valoración de activos de la tabla 26, los controles de la ISO/IEC 27002:2013 y las tablas 27, 28, 29 y 30, que ilustran una serie de parámetros a tener en cuenta para los cálculos respectivos.

Tabla 27. Probabilidad de ocurrencia de la amenaza

Valoración cualitativa	frecuencia	Valoración cuantitativa
MA (muy alta)	A diario	5
A (alta)	Semanalmente	4
M (media)	1 vez al mes	3
B (baja)	Cada seis meses	2
MB (muy baja)	Cada año	1

Fuente: el autor

Tabla 28. Dimensiones de seguridad según MAGERIT

Dimensión	Código
Autenticidad	A
Disponibilidad	D
Integridad	I
Confiabilidad	C
Trazabilidad	T

Fuente. El autor

La tabla 29, ilustra la efectividad cualitativa y cuantitativa de los controles de la ISO/IEC 27002:2013, indicados a establecer, como respuesta a los riesgos identificados para minimizar su impacto y mejorar las oportunidades del negocio.

Tabla 29. Eficacia de controles

Eficacia del control	
Alto	4
Medio	3
Bajo	2
Inexistente	1

Fuente: https://webcache.googleusercontent.com/search?q=cache:A5e9SFbwzK0J:https://repositorio.escuelaing.edu.co/bitstream/001/501/3/Anexo2.xls+&cd=9&hl=es-419&ct=clnk&gl=co

Una vez establecidos los controles como respuesta al impacto de los riesgos, algunos de ellos no serán eliminados completamente; por lo tanto, van a permanecer sobre los activos implicados, a este tipo de riesgos se les conoce como *riesgos residuales*, y para evitar un incremento de su impacto o que afecte otros activos de la institución COOPSENA, esta deberá asumir un procedimiento de monitorización constante. La tabla 30, ilustra la valoración de los riesgos residuales cuyo cálculo es fácil determinar mediante la siguiente formula:

$$\text{Riesgo residual} = \frac{\text{Valor del riesgo inherente}}{\text{Valor eficacia del control}}$$

Tabla 30. Valoración del riesgo residual

Valoración del riesgo residual	
Nivel	Valoración
Extremo	>=16
Alto	10 a 15
Moderado	3 a 9
Bajo	0,1 a 2,9

Fuente. El autor

Para la valoración del riesgo potencial, haremos uso de los parámetros (colores) relacionados en la figura 7. En consecuencia, la lista de riesgos con la respectiva valoración de frecuencia, impacto y riesgo residual sobre las dimensiones de seguridad de los elementos informáticos que conforman la infraestructura tecnológica de COOPSENA, se relaciona a continuación.

Tabla 31. Valoración de riesgos y el impacto sobre los activos x cada dimensión de seguridad de acuerdo a la metodología MAGERIT.

VALORACION DE RIESGOS POR CADA ACTIVO INFORMATICO DE LA INSTITUCION COOPSENA																		
Amenazas	Activos	Frecuencia	Valoración del impacto potencial					Valoración del riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoración del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[N.1] Fuego	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	Discos duros, pendrives, DVD	1		3	3		3		3	3		3	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1	1	0	1
	UPS, cableado eléctrico, cableado de comunicaciones	1		4	4		4		4	4		3	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1
	Edificio	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
[N.2] Daños por agua	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	Discos duros, pendrives, DVD	1		3	3		3		3	3		3	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1	1	0	1
	UPS, cableado eléctrico, cableado de comunicaciones	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	Edificio	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
[N.7] Fenómeno sísmico	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	Discos duros, pendrives, DVD	1		3	3		3		3	3		3	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1	1	0	1
	UPS, cableado eléctrico, cableado de comunicaciones	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	Edificio	1		4	4		4		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
[I.3] Contaminación mecánica	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		4	4		4		8	8		8	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	2,7	2,7	0	2,7
	Discos duros, pendrives, DVD	1		2	2		2		2	2		2	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	0,7	0,7	0	0,7
	UPS, cableado eléctrico, cableado de comunicaciones	3		4	4		4		12	12		12	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	4	4	0	4
[I.4] Contaminación electromagnética	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		3	3		3		6	6		6	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	2	2	0	2
	Discos duros, pendrives, DVD	2		2	2		2		4	4		4	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1,3	1,3	0	1,3
	UPS, cableado eléctrico, cableado de comunicaciones	3		4	4		4		12	12		12	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	4	4	0	4
[I.5] Avería de origen físico o lógico	Software administrativo, contable y de seguridad	2		4	4		4		8	8		8	11.2.4 Mantenimiento de los equipos.	4	0	2	2	0	2
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	3		4	4		4		12	12		12	11.2.4 Mantenimiento de los equipos.	4	0	3	3	0	3
	Discos duros, pendrives, DVD	2		4	4		4		8	8		8	11.2.4 Mantenimiento de los equipos.	4	0	2	2	0	2
	UPS, cableado eléctrico, cableado de comunicaciones	2		4	4		4		8	8		8	11.2.4 Mantenimiento de los equipos.	4	0	2	2	0	2

Amenazas	Activos	Frecuencia	Valoracion del impacto potencial					Valoracion del riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[I.6] Corte del suministro eléctrico	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	3		5	4		4		15	12		12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	0	3,8	3	0	3
	Discos duros, pendrives, DVD	3		3	3		3		9	9		9	12.6.1 Gestión de las vulnerabilidades técnicas.	4	0	2,3	2,3	0	2,3
	UPS, cableado eléctrico, cableado de comunicaciones	3		5	4		4		15	12		12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	0	3,8	3	0	3
[I.7] Condiciones inadecuadas de temperatura o humedad	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		4	4		4		8	8		8	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	2,7	2,7	0	2,7
	Discos duros, pendrives, DVD	1		3	3		2		3	3		2	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	1	1	0	0,7
	UPS, cableado eléctrico, cableado de comunicaciones	2		4	4		3		8	8		6	11.1.4 Protección contra las amenazas externas y ambientales.	3	0	2,7	2,7	0	2
[I.8] Fallo de servicios de comunicaciones	F.O, cable UTP, servidores	2		5	4		4		10	8		8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	0	3,3	2,7	0	2,7
[I.10] Degradación de los soportes de almacenamiento de la información	Discos duros, pendrives, DVD	1		4	4		3		4	4		3	8.3.1 Gestión de soportes extraíbles.	3	0	1,3	1,3	0	1
|[E.1] Errores de los usuarios	datos / información	3		4	4	4	3		12	12	12	9	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	4	4	4	3
	claves criptográficas	2		5	5	5	4		10	10	10	8	10.1.1 Política de uso de los controles criptográficos.	4	0	2,5	2,5	2,5	2
	Servicios	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	Software se sistemas, aplicaciones administrativas, contable y de seguridad	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	DD, Pendrives, DVD	1		4	4	4	3		4	4	4	3	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	1,3	1,3	1,3	1
[E.2] Errores del administrador	datos / información	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	claves criptográficas	1		5	5	5	4		5	5	5	4	10.1.1 Política de uso de los controles criptográficos.	4	0	1,3	1,3	1,3	1
	Servicios	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	Software contable administrativo y de sistemas	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	Redes de comunicaciones	2		4	4	4	3		8	8	8	6	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	2,7	2
	DD, DVD, pendrives.	1		4	4	4	3		4	4	4	3	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	1,3	1,3	1,3	1

Tabla 31. (Continuación)

Amenazas	Activos	Frecuencia	Valoracion del impacto potencial					Valoracion del riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[E.4] Errores de configuración	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		4	4		3		8	8		6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	3	0	2,7	2,7	0	2
[E.7] Deficiencias en la organización	Funcionarios.	2		4					8				6.1.1 Asignación de responsabilidades para la segur. de la información.	3	0	2,7	0	0	0
[E.8] Difusión de software dañino	Software de sistemas, contable y administrativo.	2		4	4	5			8	8	10		12.2.1 Controles contra el código malicioso.	3	0	2,7	2,7	3,3	0
[E.9] Errores de [re-]encaminamiento	Servicios	2				4					8		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	0	2,7	0
	Software de sistemas, administrativo y contable	2				4					8		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	0	2,7	0
	Redes de comunicaciones	2				5					10		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	0	3,3	0
[E.15] Alteración accidental de la información	Datos / información	1		5	5	5	4		5	5	5	4	9.4.1 Restricción del acceso a la información.	3	0	1,7	1,7	1,7	1,3
	Contraseñas	2		5	5	5	4		10	10	10	8	9.4.2 Procedimientos seguros de inicio de sesión.	4	0	2,5	2,5	2,5	2
	Servicios	1		5	5	5	4		5	5	5	4	9.4.1 Restricción del acceso a la información.	3	0	1,7	1,7	1,7	1,3
	Software de sistemas, contable y administrativo	1		5	5	5	4		5	5	5	4	9.4.1 Restricción del acceso a la información.	3	0	1,7	1,7	1,7	1,3
	Comunicación vía red	1		5	5	5	4		5	5	5	4	13.2.1 Políticas y procedimientos de intercambio de información.	3	0	1,7	1,7	1,7	1,3
	DD, DVD, pendrives	1		5	5	5	4		5	5	5	4	9.4.1 Restricción del acceso a la información.	3	0	1,7	1,7	1,7	1,3
[E.18] Destrucción de información	Datos / información	1		5	4		4		5	4		4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1	0	1
	Contraseñas	1		5	4		4		5	4		4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1	0	1
	Servicios	1		5	4		4		5	4		4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1	0	1
	Aplicaciones	1		5	4		4		5	4		4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1	0	1
	Comunicaciones en transito	1		4	4		3		4	4		3	12.3.1 Copias de seguridad de la información.	4	0	1	1	0	0,8
	DD, DVD, pendrives	2		4	4		3		8	8		6	12.3.1 Copias de seguridad de la información.	4	0	2	2	0	1,5

Tabla 31. (Continuación)

Amenazas	Activos	Frecuencia	Valoracion impacto potencial					Valoracion riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[E.19] Fugas de información	Datos / información	1			4	5	3			4	5	3	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	1,3	1,7	1
	Contraseñas	1			4	5	3			4	5	3	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	1,3	1,7	1
	Servicios	2			4	4	3			8	8	6	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	2,7	2,7	2
	Software de sistemas, contable y administrativo	1			4	5	3			4	5	3	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	1,3	1,7	1
	Comunicaciones en tránsito	2			4	5	3			8	10	6	13.1.2 Mecanismos de seguridad asociados a servicios en red.	3	0	0	2,7	3,3	2
	Soportes de información	3			4	5	4			12	15	12	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	4	5	4
	Personal (revelación)	1			4	5	3			4	5	3	13.2.4 Acuerdos de confidencialidad y secreto.	3	0	0	1,3	1,7	1
[E.20] Vulnerabilidades de los programas (software)	Software de sistemas, contable y administrativo.	2		4	4	4	3		8	8	8	6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	3	0	2,7	2,7	2,7	2
[E.21] Errores de mantenimiento / actualización de programas (software)	Software de sistemas, contable y administrativo.	2		4	4		3		8	8		6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	3	0	2,7	2,7	0	2
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		5	4		3		10	8		6	14.2.2 Procedimientos de control de cambios en los sistemas.	3	0	3,3	2,7	0	2
	Discos duros, pendrives, DVD	2		5	4		3		10	8		6	14.2.2 Procedimientos de control de cambios en los sistemas.	3	0	3,3	2,7	0	2
	UPS, cableado eléctrico, cableado de comunicaciones	2		4	4		3		8	8		6	14.2.2 Procedimientos de control de cambios en los sistemas.	3	0	2,7	2,7	0	2
[E.24] Caída del sistema por agotamiento de recursos	Servicios	2		4					8				11.2.4 Mantenimiento de los equipos.	3	0	2,7	0	0	0
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		3					6				11.2.4 Mantenimiento de los equipos.	3	0	2	0	0	0
	Redes de comunicaciones	2		4					8				11.2.4 Mantenimiento de los equipos.	3	0	2,7	0	0	0
[E.25] Pérdida de equipos	Equipos informáticos (hardware)	1		5	5	5	5		5	5	5	5	8.1.1 Inventario de activos.	4	0	1,3	1,3	1,3	1,3
	Soportes de información	2		5	5	5	5		10	10	10	10	8.1.1 Inventario de activos.	4	0	2,5	2,5	2,5	2,5
	UPS, cableado eléctrico, cableado de comunicaciones, servidores	1		5	5	5	5		5	5	5	5	8.1.1 Inventario de activos.	4	0	1,3	1,3	1,3	1,3
[E.28] Indisponibilidad del personal	Personal interno	1		3					3				7.2.2 Concienciación, educación y capacitación en segur. de la informac.	4	0	0,8	0	0	0

Tabla 31. (Continuación)

Amenazas	Activos	Frecuencia	Valoracion impacto potencial					Valoracion riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[A.4] Manipulación de la configuración	Registros de actividad	1	5	4	5	5	3	5	4	5	5	3	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	1,7	1,3	1,7	1,7	1
[A.5] Suplantación de la identidad del usuario	Datos / información	2	5	4	5	5	3	10	8	10	10	6	9.3.1 Uso de información confidencial para la autenticación.	4	2,5	2	2,5	2,5	1,5
	Contraseñas	2	5	4	5	5	4	10	8	10	10	8	9.3.1 Uso de información confidencial para la autenticación.	4	2,5	2	2,5	2,5	2
	Servicios	2	5	4	5	5	3	10	8	10	10	6	9.3.1 Uso de información confidencial para la autenticación.	4	2,5	2	2,5	2,5	1,5
	Aplicaciones (software)	2	5	3	5	5	3	10	6	10	10	6	9.3.1 Uso de información confidencial para la autenticación.	4	2,5	1,5	2,5	2,5	1,5
	Redes de comunicaciones	2	5	4	5	5	4	10	8	10	10	8	9.3.1 Uso de información confidencial para la autenticación.	4	2,5	2	2,5	2,5	2
[A.6] Abuso de privilegios de acceso	Datos / información	2	5	4	4	4	3	10	8	8	8	6	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	3,3	2,7	2,7	2,7	2
	Contraseñas	2	4	4	4	4	3	8	8	8	8	6	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,7	2,7	2,7	2,7	2
	Servicios	2	3	3	4	4	3	6	6	8	8	6	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2	2	2,7	2,7	2
	Aplicaciones (software)	2	3	4	4	4	3	6	8	8	8	6	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2	2,7	2,7	2,7	2
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2	4	3	3	3	2	8	6	6	6	4	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,7	2	2	2	1,3
	Redes de comunicaciones	2	3	4	4	4	3	6	8	8	8	6	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2	2,7	2,7	2,7	2
[A.7] Uso no previsto	Servicios	2		4	4	4	3		8	8	8	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	2,7	2
	Aplicaciones (software)	2		4	4	4	3		8	8	8	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	2,7	2
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2		3	3	3			6	6	6		8.1.3 Uso aceptable de los activos.	3	0	2	2	2	0
	Redes de comunicaciones	2		4	4	4	3		8	8	8	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	2,7	2
	Soportes de información	2		4	4	4	3		8	8	8	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	2,7	2
	UPS,servidores	2		4	4	4	3		8	8	8	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	2,7	2
[A.9] Re-encaminamiento de mensajes	Servicios	2			4	5				8	10		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	2,7	3,3	0
	Aplicaciones (software)	2			3	4				6	8		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	2	2,7	0
	Redes de comunicaciones.	2			4	5				8	10		13.2.1 Políticas y procedimientos de intercambio de información.	3	0	0	2,7	3,3	0

Tabla 31. (Continuación)

Amenazas	Activos	Frecuencia	Valoracion impacto potencial					Valoracion riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[A.11] Acceso no autorizado	Datos / información	2	4		4	5	3	8		8	10	6	9.1.1 Política de control de accesos.	4	2	0	2	2,5	1,5
	Claves criptográficas	2	4		5	5		8		10	10		10.1.1 Política de uso de los controles criptográficos.	4	2	0	2,5	2,5	0
	Contraseñas	2	4		4	5	3	8		8	10	6	9.1.1 Política de control de accesos.	4	2	0	2	2,5	1,5
	Servicios	2	4		4	5	2	8		8	10	4	9.1.1 Política de control de accesos.	4	2	0	2	2,5	1
	Aplicaciones (software)	2	4		4	5	2	8		8	10	4	9.1.1 Política de control de accesos.	4	2	0	2	2,5	1
	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2	3		4	5	3	6		8	10	6	9.1.1 Política de control de accesos.	4	1,5	0	2	2,5	1,5
	Redes de comunicaciones	2	3		5	5	2	6		10	10	4	9.1.1 Política de control de accesos.	4	1,5	0	2,5	2,5	1
	Soportes de información	2	4		4	5	3	8		8	10	6	9.1.1 Política de control de accesos.	4	2	0	2	2,5	1,5
	Equipamiento auxiliar	1	3		3	4		3		3	4		9.1.1 Política de control de accesos.	4	0,8	0	0,8	1	0
	Instalaciones	1	3		3	5		3		3	5		9.1.1 Política de control de accesos.	4	0,8	0	0,8	1,3	0
[A.12] Análisis de tráfico	Redes de comunicaciones	1		3		4	2		3		4	2	13.1.1 Controles de red.	4	0	0,8	0	1	0,5
[A.13] Repudio	Servicios	1		3	4		3		3	4		3	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3	0	1	1,3	0	1
[A.14] Interceptación de información (escucha)	Redes de comunicaciones	1	3		3	4	2	3		3	4	2	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	1	0	1	1,3	0,7
[A.15] Modificación deliberada de la información	Datos / información	1	4	4	4	5	3	4	4	4	5	3	9.4.1 Restricción del acceso a la información.	4	1	1	1	1,3	0,8
	Contraseñas	1	5	4	4	5	4	5	4	4	5	4	9.4.1 Restricción del acceso a la información.	4	1,3	1	1	1,3	1
	Servicios (acceso)	1	4	4	4	5	3	4	4	4	5	3	9.4.1 Restricción del acceso a la información.	4	1	1	1	1,3	0,8
	Aplicaciones	1	4	4	4	5	3	4	4	4	5	3	9.4.1 Restricción del acceso a la información.	4	1	1	1	1,3	0,8
	Comunicaciones en (tránsito)	2	4	4	4	5	3	8	8	8	10	6	9.4.1 Restricción del acceso a la información.	4	2	2	2	2,5	1,5
	Soportes de información	2	4	4	4	4	3	8	8	8	8	6	9.4.1 Restricción del acceso a la información.	4	2	2	2	2	1,5
	Instalaciones	1	4	4	4	4	2	4	4	4	4	2	9.4.1 Restricción del acceso a la información.	4	1	1	1	1	0,5
[A.18] Destrucción de información	Instalaciones	1		5	5	4	3		5	5	4	3	12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	1	0,8
	datos / información	1		5	5	4	3		5	5	4	3	12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	1	0,8
	claves criptográficas	1		5	5	4	4		5	5	4	4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	1	1
	Servicios	1		5	5	4	3		5	5	4	3	12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	1	0,8
	Aplicaciones	1		5	5	4	4		5	5	4	4	12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	1	1
	Soportes de información	2		5	4	4	3		10	8	8	6	12.3.1 Copias de seguridad de la información.	4	0	2,5	2	2	1,5

Tabla 31. (Continuación)

Amenazas	Activos	Frecuencia	Valoracion impacto potencial					Valoracion riesgo potencial					Controles ISO 27002:2013	Eficacia del control	Valoracion del riesgo residual				
			A	D	I	C	T	A	D	I	C	T			A	D	I	C	T
[A.22] Manipulación de programas	Computadores de escritorio, portátiles, impresoras, teléfonos IP, servidores.	2	4	4	5	4	3	8	8	10	8	6	9.4.4 Uso de herramientas de administración de sistemas.	4	2	2	2,5	2	1,5
[A.23] Manipulación de los equipos	Equipos informáticos	2		4	4	5	3		8	8	10	6	8.1.3 Uso aceptable de los activos.	3	0	2,7	2,7	3,3	2
	Soportes de información	2		4	5	5	4		8	10	10	8	8.1.3 Uso aceptable de los activos.	3	0	2,7	3,3	3,3	2,7
	UPS, redes, routers	1		4	5	5	3		4	5	5	3	8.1.3 Uso aceptable de los activos.	3	0	1,3	1,7	1,7	1
[A.24] Denegación de servicio	Servicios	2		5	4		3		10	8		6	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0	2,5	2	0	1,5
	Equipos informáticos (hardware)	2		4	4		3		8	8		6	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0	2	2	0	1,5
	[COM] redes de comunicaciones	2		4	4		3		8	8		6	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0	2	2	0	1,5
[A.25] Robo	Equipos informáticos (hardware)	1		4	4	5	3		4	4	5	3	11.1.3 Seguridad de oficinas, despachos y recursos.	3	0	1,3	1,3	1,7	1
	Soportes de información	1		4	4	5	4		4	4	5	4	11.1.3 Seguridad de oficinas, despachos y recursos.	3	0	1,3	1,3	1,7	1,3
	UPS, routers, switches	1		5	4	5	3		5	4	5	3	11.1.3 Seguridad de oficinas, despachos y recursos.	3	0	1,7	1,3	1,7	1
[A.26] Ataque destructivo	Equipos informáticos (hardware)	1		4	5		3		4	5		3	12.3.1 Copias de seguridad de la información.	4	0	1	1,3	0	0,8
	Soportes de información	1		5	4		3		5	4		3	12.3.1 Copias de seguridad de la información.	4	0	1,3	1	0	0,8
	Equipamiento auxiliar	1		5	5				5	5			12.3.1 Copias de seguridad de la información.	4	0	1,3	1,3	0	0
	Instalaciones	1		4	4				4	4			12.3.1 Copias de seguridad de la información.	4	0	1	1	0	0
[A.28] Indisponibilidad del personal	Personal interno	1		5			4		5			4	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	1,7	0	0	1,3
[A.29] Extorsión	Personal interno	2		4	4	5			8	8	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	2,7	3,3	0
[A.30] Ingeniería social (picaresca)	Gerente	2		4	5	5			8	10	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	3,3	3,3	0
	Asistente de gerencia	2		4	5	5			8	10	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	3,3	3,3	0
	Contador publico	2		4	5	5			8	10	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	3,3	3,3	0
	Tesorero	2		4	5	5			8	10	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	3,3	3,3	0
	Revisor fiscal	2		4	5	5			8	10	10		7.2.2 Concienciación, educación y capacitación en segur. de la informac.	3	0	2,7	3,3	3,3	0

Tabla 31. (Continuación)

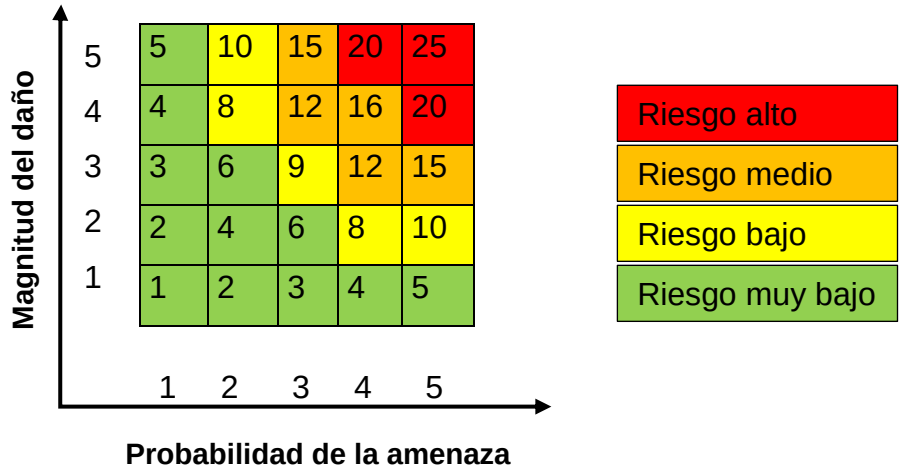
Fuente: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12685/1/80378557.pdf

7.4.3 Gestión de riesgos. El objetivo de este proceso es presentar un resumen detallado de los riesgos de seguridad identificados en la entidad, establecer la magnitud de los mismos y determinar las áreas que requieren implantación de salvaguardas. Para llevar a cabo el proceso, nos apoyaremos en los datos relacionados en la tabla 26, y para cuantificar las consecuencias de los riesgos, utilizaremos la fórmula matemática: R= P x M; de donde, R=riesgo; P= probabilidad de amenaza; M= magnitud del riesgo.

Sus consecuencias las analizaremos cualitativamente, mediante los siguientes criterios:

Riesgo muy bajo (insignificante)= 1; bajo =2; medio = 3; alto = 4; muy alto =5.

Figura 7. Análisis cuantitativo de los riesgos



Fuente: el autor

La aplicación de la fórmula matemática, arroja resultados que agruparemos en cuatro categorías (bajo, medio, alto y muy alto), las cuales identificaremos mediante los colores verde, amarillo, naranja y rojo para un mejor análisis de los mismos tal y como lo muestra la figura 7.

Tabla 32. Matriz de gestión de riesgos (empresa COOPSENA)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Información empresarial	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Actos originados por los delincuentes comunes o cibernaticos
	Activos esenciales	Datos/Información	Encriptacion publica	Servicios	Aplicaciones (software)		Manipulacion de la configuracion
							2
Documentos vitales (administrativos, politicas etc)	x					3	6
Documentos personales (obligaciones financieras)	x					3	6
Documentos clasificados (Proyectos,dtos historicos)	x					2	4
Servicios (Correo electronico, troncal telefonica, etc)	x					3	6
Ficheros (administrativos, auditorias, etc)		x				3	6
Copias de respaldo		x				3	6
Datos de configuracion		x				3	6
Datos de gestion interna		x				4	8
Credenciales		x				3	6
Datos de control de acceso		x				3	6
Claves publicas de cifra (base de datos de claves publicas)			x			3	6
Cifrado de sooprtes de informacion			x			3	6
Al publico en general (sin relacion contractual)				x		1	2
A usuarios de la propia organización				x		1	2
WWW (pagina web)				x		4	8
Correo electronico				x		3	6
Almacenamiento de archivos				x		4	8
Transferencia de ficheros				x		3	6
Intercambio electronico de datos				x		3	6
Gestion de identidades				x		3	6
Gestion de privilegios				x		3	6
Sistema de claves publicas				x		3	6
Sistema contable					x	4	8
Sistema de correo electronico					x	3	6
Sistema Gestion base de datos					x	3	6
Ofimatica					x	3	6
Sistame operativo					x	4	8
Antivirus					x	3	6
Sistema backup					x	4	8

Actos originados por los delincuentes comunes o cibernaticos											
Suplantacion de la identidad del usuario	Alteracion de secuencia	Analisis de trafico	Interceptacion de la informacion (escucha)	Modificacion deliberada de la informacion	Destruccion de la informacion	Robo	Fraude o estafa	Ataque destructivo	Extorsion	Difusion o ataque con software dañino
2	2	3	3	3	2	3	3	2	3	3
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
2	2	3	3	3	2	3	3	2	3	3
2	2	3	3	3	2	3	3	2	3	3
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Información empresarial	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos de origen físico o logico
	Activos esenciales	Datos/Información	Encriptacion publica	Servicios	Aplicaciones (software)		Fuego
							3
Documentos vitales (administrativos, politicas etc)	x					3	9
Documentos personales (obligaciones financieras)	x					3	9
Documentos clasificados (Proyectos,dtos historicos)	x					2	6
Servicios (Correo electronico, troncal telefonica, etc)	x					3	9
Ficheros (administrativos, auditorias, etc)		x				3	9
Copias de respaldo		x				3	9
Datos de configuracion		x				3	9
Datos de gestion interna		x				4	12
Credenciales		x				3	9
Datos de control de acceso		x				3	9
Claves publicas de cifra (base de datos de claves publicas)			x			3	9
Cifrado de sooprtes de informacion			x			3	9
Al publico en general (sin relacion contractual)				x		1	3
A usuarios de la propia organización				x		1	3
WWW (pagina web)				x		4	12
Correo electronico				x		3	9
Almacenamiento de archivos				x		4	12
Transferencia de ficheros				x		3	9
Intercambio electronico de datos				x		3	9
Gestion de identidades				x		3	9
Gestion de privilegios				x		3	9
Sistema de claves publicas				x		3	9
Sistema contable					x	4	12
Sistema de correo electronico					x	3	9
Sistema Gestion base de datos					x	3	9
Ofimatica					x	3	9
Sistame operativo					x	4	12
Antivirus					x	3	9
Sistema backup					x	4	12

Daños por agua	Sismo	Contaminacion mecanica	Contaminacion electromagnetica	Averias de origen fisico o logico	Corte del suministro electrico	Condiciones inadecuadas de temperatura o humedad	Fallo de servicios de comunicaciones	Caida del sistema por agotamiento de recursos	Degradacion de los soportes de almacenamiento de informacion	Vulnerabilidades de los programas (software)
2	3	2	3	2	3	2	3	3	3	3
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
4	6	4	6	4	6	4	6	6	6	6
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
8	12	8	12	8	12	8	12	12	12	12
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
2	3	2	3	2	3	2	3	3	3	3
2	3	2	3	2	3	2	3	3	3	3
8	12	8	12	8	12	8	12	12	12	12
6	9	6	9	6	9	6	9	9	9	9
8	12	8	12	8	12	8	12	12	12	12
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
8	12	8	12	8	12	8	12	12	12	12
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
6	9	6	9	6	9	6	9	9	9	9
8	12	8	12	8	12	8	12	12	12	12
6	9	6	9	6	9	6	9	9	9	9
8	12	8	12	8	12	8	12	12	12	12

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta, 5=muy
Información empresarial	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Activos esenciales	Datos/Información	Encriptacion publica	Servicios	Aplicaciones (software)		Errores de los usuarios
							4
Documentos vitales (administrativos, politicas etc)	x					3	12
Documentos personales (obligaciones financieras)	x					3	12
Documentos clasificados (Proyectos,dtos historicos)	x					2	8
Servicios (Correo electronico, troncal telefonica, etc)	x					3	12
Ficheros (administrativos, auditorias, etc)		x				3	12
Copias de respaldo		x				3	12
Datos de configuracion		x				3	12
Datos de gestion interna		x				4	16
Credenciales		x				3	12
Datos de control de acceso		x				3	12
Claves publicas de cifra (base de datos de claves publicas)			x			3	12
Cifrado de sooprtes de informacion			x			3	12
Al publico en general (sin relacion contractual)				x		1	4
A usuarios de la propia organización				x		1	4
WWW (pagina web)				x		4	16
Correo electronico				x		3	12
Almacenamiento de archivos				x		4	16
Transferencia de ficheros				x		3	12
Intercambio electronico de datos				x		3	12
Gestion de identidades				x		3	12
Gestion de privilegios				x		3	12
Sistema de claves publicas				x		3	12
Sistema contable					x	4	16
Sistema de correo electronico					x	3	12
Sistema Gestion base de datos					x	3	12
Ofimatica					x	3	12
Sistame operativo					x	4	16
Antivirus					x	3	12
Sistema backup					x	4	16

Errores del administrador	Errores de configuracion	Deficiencias de la organización	Difusion de software dañino	Errores de re-encaminamiento	Alteracion accidental de la informacion	Destruccion de la informacion	Fugas de informacion	Errores de mantenimiento/actualizacion de equipos (hardware)	Errores de mantenimiento/actualizacion de programas (software)	Perdida de equipos	Manipulacion de la configuracion	Suplantacion de la identidad del usuario
3	3	3	4	3	2	2	3	3	3	2	3	2
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
6	6	6	8	6	4	4	6	6	6	4	6	4
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
12	12	12	16	12	8	8	12	12	12	8	12	8
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
3	3	3	4	3	2	2	3	3	3	2	3	2
3	3	3	4	3	2	2	3	3	3	2	3	2
12	12	12	16	12	8	8	12	12	12	8	12	8
9	9	9	12	9	6	6	9	9	9	6	9	6
12	12	12	16	12	8	8	12	12	12	8	12	8
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
12	12	12	16	12	8	8	12	12	12	8	12	8
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
12	12	12	16	12	8	8	12	12	12	8	12	8
9	9	9	12	9	6	6	9	9	9	6	9	6
12	12	12	16	12	8	8	12	12	12	8	12	8

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta,
Información empresarial	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	
	Activos esenciales	Datos/Información	Encriptacion publica	Servicios	Aplicaciones (software)		
							3
Documentos vitales (administrativos, politicas etc)	x					3	9
Documentos personales (obligaciones financieras)	x					3	9
Documentos clasificados (Proyectos,dtos historicos)	x					2	6
Servicios (Correo electronico, troncal telefonica, etc)	x					3	9
Ficheros (administrativos, auditorias, etc)		x				3	9
Copias de respaldo		x				3	9
Datos de configuracion		x				3	9
Datos de gestion interna		x				4	12
Credenciales		x				3	9
Datos de control de acceso		x				3	9
Claves publicas de cifra (base de datos de claves publicas)			x			3	9
Cifrado de sooprtes de informacion			x			3	9
Al publico en general (sin relacion contractual)				x		1	3
A usuarios de la propia organización				x		1	3
WWW (pagina web)				x		4	12
Correo electronico				x		3	9
Almacenamiento de archivos				x		4	12
Transferencia de ficheros				x		3	9
Intercambio electronico de datos				x		3	9
Gestion de identidades				x		3	9
Gestion de privilegios				x		3	9
Sistema de claves publicas				x		3	9
Sistema contable					x	4	12
Sistema de correo electronico					x	3	9
Sistema Gestion base de datos					x	3	9
Ofimatica					x	3	9
Sistame operativo					x	4	12
Antivirus					x	3	9
Sistema backup					x	4	12

Abuso de privilegios de acceso	Uso no previsto	Re-encaminamiento de mensajes	Repudio	Modificacion deliberada de la informacion	Divulgacion de la informacion	Manipulacion de programas	Manipulacion de los equipos	Denegacion de servicios	Robo	Indisponibilidad del personal	Extorsion	Ingenieria social (picaresca)
3	3	3	3	2	2	3	3	3	2	3	3	3
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
3	3	3	3	2	2	3	3	3	2	3	3	3
3	3	3	3	2	2	3	3	3	2	3	3	3
12	12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	12	8	8	12	12	12	8	12	12	12

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Sistemas e Infraestructura	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Actos originados por los delincuentes comunes o cibernaticos
	Equipos informaticos (hardware)	Redes de comunicaciones	Soportes de informacion	Equipamiento auxiliar	Instalaciones		Manipulacion de la configuracion
							2
Servidores	x					3	6
Computadoras de escritorio	x					2	4
Portátiles	x					3	6
Sevidor de respaldo	x					3	6
Impresoras	x					1	2
Routers	x					2	4
Switches	x					2	4
Firewall	x					2	4
Acces point	x					2	4
Central telefonica	x					3	6
Telefonos IP	x					2	4
Red wi-fi		x				2	4
Red LAN		x				3	6
Internet		x				3	6
Discos duros			x			2	4
Memorias USB			x			2	4
UPS				x		2	4
Sistema climatizacion				x		1	2
Sistema contra incendios				x		2	4
Cable electrico				x		2	4
Fibra optica				x		3	6
Cable UTP cat.6				x		3	6
Edificio					x	2	4
Cuarto de sistemas					x	2	4

Suplantacion de la identidad del usuario	Alteracion de secuencia	Analisis de trafico	Interceptacion de la informacion (escucha)	Modificacion deliberada de la informacion	Destruccion de la informacion	Robo	Fraude o estafa	Ataque destructivo	Extorsion	Difusion o ataque con software dañino
2	2	3	3	3	2	3	3	2	3	3
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
2	2	3	3	3	2	3	3	2	3	3
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
2	2	3	3	3	2	3	3	2	3	3
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
4	4	6	6	6	4	6	6	4	6	6

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Sistemas e Infraestructura	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos de origen físico o logico
	Equipos informaticos (hardware)	Redes de comunicaciones	Soportes de informacion	Equipamiento auxiliar	Instalaciones		Fuego
							3
Servidores	x					3	9
Computadoras de escritorio	x					2	6
Portátiles	x					3	9
Sevidor de respaldo	x					3	9
Impresoras	x					1	3
Routers	x					2	6
Switches	x					2	6
Firewall	x					2	6
Acces point	x					2	6
Central telefonica	x					3	9
Telefonos IP	x					2	6
Red wi-fi		x				2	6
Red LAN		x				3	9
Internet		x				3	9
Discos duros			x			2	6
Memorias USB			x			2	6
UPS				x		2	6
Sistema climatizacion				x		1	3
Sistema contra incendios				x		2	6
Cable electrico				x		2	6
Fibra optica				x		3	9
Cable UTP cat.6				x		3	9
Edificio					x	2	6
Cuarto de sistemas					x	2	6

Daños por agua	Sismo	Contaminacion mecanica	Contaminacion electromagnetica	Averias de origen físico o logico	Corte del suministro electrico	Condiciones inadecuadas de temperatura o humedad	Fallo de servicios de comunicaciones	Caida del sistema por agotamiento de recursos	Degradacion de los soportes de almacenamiento de informacion	Vulnerabilidades de los programas (software)
2	3	2	3	2	3	2	3	2	2	2
6	9	6	9	6	9	6	9	6	6	6
4	6	4	6	4	6	4	6	4	4	4
6	9	6	9	6	9	6	9	6	6	6
6	9	6	9	6	9	6	9	6	6	6
2	3	2	3	2	3	2	3	2	2	2
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
6	9	6	9	6	9	6	9	6	6	6
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
6	9	6	9	6	9	6	9	6	6	6
6	9	6	9	6	9	6	9	6	6	6
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
2	3	2	3	2	3	2	3	2	2	2
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4
6	9	6	9	6	9	6	9	6	6	6
6	9	6	9	6	9	6	9	6	6	6
4	6	4	6	4	6	4	6	4	4	4
4	6	4	6	4	6	4	6	4	4	4

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta, 5=muy
Sistemas e Infraestructura	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Equipos informaticos (hardware)	Redes de comunicaciones	Soportes de informacion	Equipamiento auxiliar	Instalaciones		Errores de los usuarios
							4
Servidores	x					3	12
Computadoras de escritorio	x					2	8
Portátiles	x					3	12
Sevidor de respaldo	x					3	12
Impresoras	x					1	4
Routers	x					2	8
Switches	x					2	8
Firewall	x					2	8
Acces point	x					2	8
Central telefonica	x					3	12
Telefonos IP	x					2	8
Red wi-fi		x				2	8
Red LAN		x				3	12
Internet		x				3	12
Discos duros			x			2	8
Memorias USB			x			2	8
UPS				x		2	8
Sistema climatizacion				x		1	4
Sistema contra incendios				x		2	8
Cable electrico				x		2	8
Fibra optica				x		3	12
Cable UTP cat.6				x		3	12
Edificio					x	2	8
Cuarto de sistemas					x	2	8

Errores del administrador	Errores de configuracion	Deficiencias de la organización	Difusion de software dañino	Errores de re-encaminamiento	Alteracion accidental de la informacion	Destruccion de la informacion	Fugas de informacion	Errores de mantenimiento/actualizacion de programas (hardware)	Errores de mantenimiento/actualizacion de programas (software)	Perdida de equipos	Manipulacion de la configuracion	Suplantacion de la identidad del usuario
3	3	3	4	3	2	2	3	3	3	2	3	2
9	9	9	12	9	6	6	9	9	9	6	9	6
6	6	6	8	6	4	4	6	6	6	4	6	4
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
3	3	3	4	3	2	2	3	3	3	2	3	2
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
9	9	9	12	9	6	6	9	9	9	6	9	6
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
3	3	3	4	3	2	2	3	3	3	2	3	2
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4
9	9	9	12	9	6	6	9	9	9	6	9	6
9	9	9	12	9	6	6	9	9	9	6	9	6
6	6	6	8	6	4	4	6	6	6	4	6	4
6	6	6	8	6	4	4	6	6	6	4	6	4

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)							Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta,
Sistemas e Infraestructura	Clasificación MAGERIT					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	
	Equipos informaticos (hardware)	Redes de comunicaciones	Soportes de informacion	Equipamiento auxiliar	Instalaciones		Abuso de privilegios de acceso
							3
Servidores	x					3	9
Computadoras de escritorio	x					2	6
Portátiles	x					3	9
Sevidor de respaldo	x					3	9
Impresoras	x					1	3
Routers	x					2	6
Switches	x					2	6
Firewall	x					2	6
Acces point	x					2	6
Central telefonica	x					3	9
Telefonos IP	x					2	6
Red wi-fi		x				2	6
Red LAN		x				3	9
Internet		x				3	9
Discos duros			x			2	6
Memorias USB			x			2	6
UPS				x		2	6
Sistema climatizacion				x		1	3
Sistema contra incendios				x		2	6
Cable electrico				x		2	6
Fibra optica				x		3	9
Cable UTP cat.6				x		3	9
Edificio					x	2	6
Cuarto de sistemas					x	2	6

Uso no previsto	Re-encaminamiento de mensajes	Repudio	Modificacion deliberada de la informacion	Divulgacion de la informacion	Manipulacion de programas	Manipulacion de los equipos	Denegacion de servicios	Robo	Indisponibilidad del personal	Extorsion	Ingenieria social (picaresca)
3	3	3	2	2	3	3	3	2	3	3	3
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
3	3	3	2	2	3	3	3	2	3	3	3
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
3	3	3	2	2	3	3	3	2	3	3	3
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
6	6	6	4	4	6	6	6	4	6	6	6

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)					Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Personal	Clasificación MAGERIT			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Actos originados por los delincuentes comunes o cibernaticos
	Usuarios externos	Funcionarios	Administradores de sistemas		Manipulacion de la configuracion
					2
Consejo administrativo	x			3	6
Junta de vigilancia	x			2	4
Revisoria fisvcal	x			3	6
Comité de credito y finanzas	x			3	6
Comité de bienestar y recreacion	x			3	6
Comité de fomento empresarial	x			3	6
Comité de apelaciones	x			2	4
Comité de educacion y solidaridad	x			3	6
Gerente		x		4	8
Asistente de gerencia		x		4	8
Jefe de servicio al cliente		x		4	8
Tesorera		x		4	8
Asistente de cartera		x		4	8
Asistente de cobranzas		x		4	8
Auxiliar de cobranzas		x		3	6
Asistente de contabilidad		x		4	8
Recepcionista		x		3	6
Auxiliar de archivo		x		4	8
Promotoras deservicios		x		2	4
Mensajero		x		3	6
Contador publico		x		4	8
Revisor fiscal		x		4	8
Asesor juridico		x		4	8
Administrador de sistemas			x	3	6

Suplantacion de la identidad del usuario	Alteracion de secuencia	Analisis de trafico	Interceptacion de la informacion (escucha)	Modificacion deliberada de la informacion	Destruccion de la informacion	Robo	Fraude o estafa	Ataque destructivo	Extorsion	Difusion o ataque con software dañino
2	2	3	3	3	2	3	3	2	3	3
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
6	6	9	9	9	6	9	9	6	9	9
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
4	4	6	6	6	4	6	6	4	6	6
6	6	9	9	9	6	9	9	6	9	9
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
8	8	12	12	12	8	12	12	8	12	12
6	6	9	9	9	6	9	9	6	9	9

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)					Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 =
Personal	Clasificación MAGERIT			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos de origen físico o logico
	Usuarios externos	Funcionarios	Administradores de sistemas		Fuego
					3
Consejo administrativo	x			3	9
Junta de vigilancia	x			2	6
Revisoria fisvcal	x			3	9
Comité de credito y finanzas	x			3	9
Comité de bienestar y recreacion	x			3	9
Comité de fomento empresarial	x			3	9
Comité de apelaciones	x			2	6
Comité de educacion y solidaridad	x			3	9
Gerente		x		4	12
Asistente de gerencia		x		4	12
Jefe de servicio al cliente		x		4	12
Tesorera		x		4	12
Asistente de cartera		x		4	12
Asistente de cobranzas		x		4	12
Auxiliar de cobranzas		x		3	9
Asistente de contabilidad		x		4	12
Recepcionista		x		3	9
Auxiliar de archivo		x		4	12
Promotoras deservicios		x		2	6
Mensajero		x		3	9
Contador publico		x		4	12
Revisor fiscal		x		4	12
Asesor juridico		x		4	12
Administrador de sistemas			x	3	9

Daños por agua	Sismo	Contaminacion mecanica	Contaminacion electromagnetica	Averias de origen fisico o logico	Corte del suministro electrico	Condiciones inadecuadas de temperatura o humedad	Fallo de servicios de comunicaciones	Caida del sistema por agotamiento de recursos	Degradacion de los soportes de almacenamiento de informacion	Vulnerabilidades de los programas (software)
2	3	2	3	2	3	2	3	3	3	2
6	9	6	9	6	9	6	9	9	9	6
4	6	4	6	4	6	4	6	6	6	4
6	9	6	9	6	9	6	9	9	9	6
6	9	6	9	6	9	6	9	9	9	6
6	9	6	9	6	9	6	9	9	9	6
6	9	6	9	6	9	6	9	9	9	6
4	6	4	6	4	6	4	6	6	6	4
6	9	6	9	6	9	6	9	9	9	6
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
6	9	6	9	6	9	6	9	9	9	6
8	12	8	12	8	12	8	12	12	12	8
6	9	6	9	6	9	6	9	9	9	6
8	12	8	12	8	12	8	12	12	12	8
4	6	4	6	4	6	4	6	6	6	4
6	9	6	9	6	9	6	9	9	9	6
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
8	12	8	12	8	12	8	12	12	12	8
6	9	6	9	6	9	6	9	9	9	6

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)					Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta, 5=muy													
Personal	Clasificación MAGERIT			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales													
	Usuarios externos	Funcionarios	Administradores de sistemas		Errores de los usuarios	Errores del administrador	Errores de configuracion	Deficiencias de la organización	Difusion de software dañino	Errores de re-encaminamiento	Alteracion accidental de la informacion	Destruccion de la informacion	Fugas de informacion	Errores de mantenimiento/actualizacion de equipos (hardware)	Errores de mantenimiento/actualizacion de programas (software)	Perdida de equipos	Manipulacion de la configuracion	Suplantacion de la identidad del usuario
					4	3	3	3	4	3	2	2	3	3	3	2	3	2
Consejo administrativo	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Junta de vigilancia	x			2	8	6	6	6	8	6	4	4	6	6	6	4	6	4
Revisoria fisvcal	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Comité de credito y finanzas	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Comité de bienestar y recreacion	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Comité de fomento empresarial	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Comité de apelaciones	x			2	8	6	6	6	8	6	4	4	6	6	6	4	6	4
Comité de educacion y solidaridad	x			3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Gerente		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Asistente de gerencia		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Jefe de servicio al cliente		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Tesorera		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Asistente de cartera		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Asistente de cobranzas		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Auxiliar de cobranzas		x		3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Asistente de contabilidad		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Recepcionista		x		3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Auxiliar de archivo		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Promotoras deservicios		x		2	8	6	6	6	8	6	4	4	6	6	6	4	6	4
Mensajero		x		3	12	9	9	9	12	9	6	6	9	9	9	6	9	6
Contador publico		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Revisor fiscal		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Asesor juridico		x		4	16	12	12	12	16	12	8	8	12	12	12	8	12	8
Administrador de sistemas			x	3	12	9	9	9	12	9	6	6	9	9	9	6	9	6

Tabla 32. (Continuación)

Matriz de Análisis de Riesgo (Empresa COOPSENA)					Probabilidad de Amenaza [=1 muy baja(Insignificante), 2 = Baja, 3= Mediana, 4 = Alta, 5
Personal	Clasificación MAGERIT			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto 5= Muy alto]	
	Usuarios externos	Funcionarios	Administradores de sistemas		Abuso de privilegios de acceso
					3
Consejo administrativo	x			3	9
Junta de vigilancia	x			2	6
Revisoria fisvcal	x			3	9
Comité de credito y finanzas	x			3	9
Comité de bienestar y recreacion	x			3	9
Comité de fomento empresarial	x			3	9
Comité de apelaciones	x			2	6
Comité de educacion y solidaridad	x			3	9
Gerente		x		4	12
Asistente de gerencia		x		4	12
Jefe de servicio al cliente		x		4	12
Tesorera		x		4	12
Asistente de cartera		x		4	12
Asistente de cobranzas		x		4	12
Auxiliar de cobranzas		x		3	9
Asistente de contabilidad		x		4	12
Recepcionista		x		3	9
Auxiliar de archivo		x		4	12
Promotoras deservicios		x		2	6
Mensajero		x		3	9
Contador publico		x		4	12
Revisor fiscal		x		4	12
Asesor juridico		x		4	12
Administrador de sistemas			x	3	9

Uso no previsto	Re-encaminamiento de mensajes	Repudio	Modificacion deliberada de la informacion	Divulgacion de la informacion	Manipulacion de programas	Manipulacion de los equipos	Denegacion de servicios	Robo	Indisponibilidad del personal	Extorsion	Ingenieria social (picaresca)
3	3	3	2	2	3	3	3	2	3	3	3
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
9	9	9	6	6	9	9	9	6	9	9	9
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	8	8	12	12	12	8	12	12	12
6	6	6	4	4	6	6	6	4	6	6	6
9	9	9	6	6	9	9	9	6	9	9	9
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
12	12	12	8	8	12	12	12	8	12	12	12
9	9	9	6	6	9	9	9	6	9	9	9

Tabla 32. (Continuación)

Fuente: https://protejete.wordpress.com/descargas/

Tabla 33. Análisis de riesgo promedio

Análisis de Riesgo promedio				
		Probabilidad de Amenaza		
		Actos originados por los delincuentes comunes o cibernéticos	**Sucesos de origen físico o lógico**	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**
	Información empresarial	7,8	8,1	8,5
Magnitud de Daño	**Sistemas e Infraestructura**	5,8	5,4	6,3
	Personal	8,6	8,6	9,4

Fuente: https://protejete.wordpress.com/descargas/

7.4.4 Determinación de salvaguardas. Esta tarea permite establecer los controles técnicos y organizativos que hay disponibles y cuán eficientes son frente a los riesgos; de igual modo, determinar cuáles son inactivos o están ausentes para encontrar procedimientos de fortalecimiento e implementación con el fin de mejorar la seguridad de la infraestructura tecnológica de la organización. Para lograr dicho propósito, existen una serie de técnicas y documentos que permiten identificar y recoger los controles o salvaguardas que aplican o no aplican en el sistema de seguridad de la información como lo son la lista de chequeo, la declaración de aplicabilidad y el plan de tratamiento de riesgos.

Estos documentos son de gran importancia, pues para el proceso de certificación del SGSI, están seleccionados en el primer orden a evaluar por parte de los especialistas encargados de realizar las auditorias. En ese sentido, una vez obtenida la matriz de análisis de riesgos que es el nexo principal entre dichos elementos, se procede a realizar una descripción de los mismos y a continuación su respectivo desarrollo.

7.4.4.1 Lista de chequeo. En términos de seguridad informática, esta es una técnica metodológica que, de manera coherente, permite verificar la presencia o ausencia de controles técnicos u organizativos en un sistema de seguridad a través de una serie de preguntas que, en forma de cuestionario, proporciona de manera rápida el grado de aplicabilidad y cumplimiento de los mismos. Para establecer la estructura de una lista de chequeo es necesario contar con la relación de dominios, objetivos de control y controles de la metodología o estándar utilizado para llevar a cabo la auditoria en cada área y procesos relacionados. Para este caso, utilizaremos la lista de dominios y controles establecida en la norma ISO/IEC 27002:2013, y que está relacionada en el anexo A.

La lista de chequeo conformada por las preguntas planteadas a los usuarios relacionados a cada área y función de la Cooperativa Multiactiva del Personal del

SENA COOPSENA y los resultados de la misma, corresponde al Anexo B del presente documento.

7.4.4.2 Declaración de aplicabilidad. Este documento conocido comúnmente como SOA, tiene como objetivo el permitir identificar los dominios que serán trabajados de acuerdo al inventario de activos y cuáles de los 114 controles (salvaguardas), de la norma ISO/IEC 27002:2013, serán utilizados para una posible implementación o función de mejoramiento por requerimientos legales, contractuales, buenas prácticas etc. Y que en sí, son un complemento a los controles identificados e implementados durante el proceso de gestión de riesgos.

La redacción de este documento que define los criterios de implementación o actualización de controles del SGSI en COOPSENA, corresponde a la tabla 34.

7.4.4.3 Plan de tratamiento de riesgos. Esta técnica conocida comúnmente como PTR, permite planificar la forma como se deben implementar o actualizar los controles o salvaguardas definidos en la declaración de aplicabilidad (SOA), es decir, que su desarrollo depende de los resultados de dicho documento.

La función principal de este proceso, está basada en la selección de una o más opciones de tratamiento de cada riesgo identificado en la evaluación de riesgos, con el fin de modificar su situación o nivel de impacto sobre el activo que se deriva de la materialización de la amenaza. De acuerdo a la metodología MAGAERIT, existen cuatro opciones básicas para realizar el tratamiento de riesgos:

Eliminar el riesgo: esta acción consiste en modificar configuraciones, cambiar o eliminar activos informáticos que se encuentren relacionados al riesgo; sin embargo, esta es una de las elecciones que para la organización resulta regularmente costosa y con altos índices de severidad, lo que pondría en mucho más riesgo el o los procesos auditados. De ahí, que deban buscarse acciones alternativas.

Mitigar el riesgo: o reducir el riesgo, es la opción que está en función con las decisiones que tome la organización con respecto a la implementación de medidas técnicas u organizativas para proteger los activos.

Aceptar el riesgo: esta opción es viable siempre y cuando el riesgo no tenga un alto nivel de degradación sobre el activo; por lo tanto, no se tomarán medidas de protección al respecto, ni se realizarán modificaciones sobre el sistema, la organización simplemente asume el control del riesgo y mantiene vigilancia permanente para que este no aumente. Sin embargo, la organización debe mantener recursos económicos necesarios, dado el caso de que el riesgo aumente su grado de exposición y haya que actuar de manera inmediata para evitar sus consecuencias.

Transferir el riesgo: generalmente esta alternativa financiera es asumida por la organización para el caso de un riesgo residual o "riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información". [Magerit3.0, Libro I. P. 103]. Por tanto, para evitar pérdidas potenciales, la organización contrata los servicios de una entidad externa especializada para que asuma el control y reducción del mismo o la adquisición de una póliza de seguros que se encargara de cubrir los gastos que se deriven de una posible incidencia que afecte o cause daños en los activos.

De acuerdo a estos criterios, una vez determinado los riesgos existentes en la infraestructura tecnológica de COOPSENA e identificado los controles que deben ser implementados para mejorar el nivel de seguridad del sistema informático de la entidad, procedemos a desarrollar el plan de tratamiento de riesgos, cuyo resultado corresponde a la tabla 35.

Tabla 34. Declaración de aplicabilidad (SOA)

RL: Requerimiento legal, **CO**: Obligación contractual, **RN/BP**: Requerimiento del negocio/Buenas practicas, **RER**: Resultado de la evaluación de riesgos

Controles ISO 27001:2013		Comentarios (Descripción de la implementación / Justificación de la exclusión)	Seleccionar la razón			
			RL	CO	RN/ BP	RER
Sec	**Objetivo de control/Control**					
5.1	Directrices de la Dirección en seguridad de la información.					
5.1.1	Conjunto de políticas para la seguridad de la información.	La gerencia de la Cooperativa debería considerar, la implementación de un programa de formación y concienciación sobre seguridad informática para todos sus funcionarios.	x		x	
6.1	Organización interna.					
6.1.4	Contacto con grupos de interés especial.	Se debería considerar tener un acercamiento con alguna organización o, tener registros en páginas web especializadas en seguridad informática para crear conciencia, generar confianza y mejorar los aspectos de seguridad en aras de que el negocio sea más efectivo.			x	
7.2	Durante la contratación.					
7.2.2	Concienciación, educación y capacitación en seguridad de la información	Es necesario que la gerencia de la Cooperativa, atienda y considere la implementación de los requisitos relacionados en los dos anteriores comentarios.	x		x	
8.1	Responsabilidad sobre los activos					
8.1.1	Inventario de activos.	Procedimientos automáticos que permiten relacionar los inventarios a cuentadantes, para mantener un control sobre las existencias de los activos informáticos que fueron puestos al servicio de los empleados, para el desempeño de sus funciones.			x	
8.1.2	Propiedad de los activos.	Procedimiento contable que verifica automáticamente, las pérdidas o daños en la disposición de los equipos informáticos y evitar desorganización de la información al momento de gestionar los estados financieros de la organización.				x
8.1.3	Uso aceptable de los activos.	Procedimiento que debe tenerse como una guía de comportamiento relacionado a las buenas practicas, el sentido común y lo que estipula la legislación del ordenamiento jurídico del estado, así como las responsabilidades y pautas básicas que deben seguir, en el desempeño de sus funciones, todos los funcionarios de la organización para contribuir a la protección del sistema informático.	x			
8.1.4	Devolución de activos.	Se especifica como una práctica que debe ser usual y desempeñada por una persona con buenos conocimientos en tecnologías de la información para una mejor administración del diagnóstico devolutivo.			x	
8.2	Clasificación de la información.					
8.2.3	Manipulación de activos.	Control Interno Informático que va a permitir una mejor inspección de las actividades o acciones realizadas manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento del sistema.			x	
9.1	Requisitos de negocio para el control de accesos.					
9.1.1	Política de control de accesos	Aunque está contemplado en la política de la empresa, no está formalizado, por lo tanto, es necesaria su implementación para fortalecer el acceso exclusivamente al personal autorizado.	x		x	

9.1.2	Control de acceso a las redes y servicios asociados	La gerencia debe considerar la implementación de normas que permita sensibilizar y restringir a los usuarios sobre el uso de los servicios de la red y el tamaño que pueden tener ciertos archivos para realizar descargas, y evitar saturaciones en el sistema.			x	
13.2	13.2 Intercambio de información con partes externas.					
13.2.1	Políticas y procedimientos de intercambio de información.	La gerencia debe considerar el diseño y ejecución de programa de formación y concienciación en seguridad de la información, con el fin de proteger adecuadamente la información y los activos informáticos de la entidad.	x		x	
18.1	Cumplimiento de los requisitos legales y contractuales.					
18.2.1	Revisión independiente de la seguridad de la información.	Se debería implementar una política que permita realizar pruebas de penetración de manera controlada, sin malicia y sin producir daño alguno, con una adecuada planificación y realizada por personal especializado, para mostrar de manera más efectiva los riesgos a los que está expuesta la información, y establecer procedimientos correctivos más eficaces y mejorar el nivel de seguridad de la información.			x	

Tabla 34. (Continuación)

Fuente: http://www.iso27001security.com/ISO27k_SOA_2013_in_4_languages.xlsx

Tabla 35. Plan de tratamiento de riesgos (PTR)

PLAN DE TRATAMIENTO DE RIESGOS (COOPSENA)							
ID	Dominio/Control	Activos	Actividad/Descripción	PTR			
				Aceptar	Reducir	Transferir	Eliminar
5	POLÍTICAS DE SEGURIDAD						
5.1.1	Conjunto de políticas para la seguridad de la información.	RR.HH, activos informáticos (hardware, software)	Se debe diseñar e implementar un programa de formación y concienciación en seguridad informática para todos los funcionarios de la entidad.			x	
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.						
6.1.4	Contacto con grupos de interés especial.	RR.HH, activos informáticos (hardware, software)	La Cooperativa debería adquirir vínculos con entidades o sitios web especializados en seguridad informática con el fin de fomentar la consulta, el conocimiento y la cooperación para obtener asesorías en relación con la seguridad de la información.		x	x	
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.						
7.2.2	Concienciación, educación y capacitación en seguridad de la información.	RR.HH, activos informáticos (datos, hardware, software)	La gerencia de la entidad debe implementar una norma de capacitación y entrenamiento en seguridad de la información a los servidores internos y externos para evitar posibles riesgos de seguridad.			x	
8	GESTIÓN DE ACTIVOS.						
8.1.1	Inventario de activos.	Activos informáticos (hardware, soportes de información, equipamiento auxiliar).	Se debe implementar un procedimiento que permita la relación de inventarios a cuentadantes, para mantener un control sobre las existencias de los activos informáticos que fueron puestos al servicio de los empleados, para el desempeño de sus funciones.	x			
8.1.2	Propiedad de los activos.	Activos informáticos (hardware, soportes de información, equipamiento auxiliar).	Se debe establecer procedimientos que permitan verificar que las pérdidas o daños en la disposición de los equipos informáticos sean las mínimas posibles y en caso tal, contabilizarlas debidamente.	x			
8.1.3	Uso aceptable de los activos.	Activos informáticos (hardware, soportes de información, equipamiento auxiliar).	Se debe implementar un código ético y de conducta mediante el cual los empleados asuman su responsabilidad sobre el uso correcto y legal de los equipos informáticos y de toda la infraestructura tecnológica complementaria puesto a su disposición.	x			
8.1.4	Devolución de activos.	Activos informáticos (hardware, soportes de información, equipamiento auxiliar).	Se debe gestionar administrativamente en lo posible, el cargo a un funcionario profesional en TI, para que se responsabilice de diagnosticar la viabilidad devolutiva de los activos informáticos, puestos al servicio de los empleados de la entidad.	x			
8.2.3	Manipulación de activos.	Activos informáticos (hardware, soportes de información, equipamiento auxiliar).	Se debe establecer un procedimiento sistematizado que permita controlar el manejo adecuado de los equipos informáticos.	x			

9	CONTROL DE ACCESOS						
9.1.1	Política de control de accesos	Activos informáticos (datos vitales, servidores, redes de comunicaciones, equipamiento auxiliar).	La gerencia debe asegurar que las áreas críticas de la entidad cuenten con un método de autenticación biométrica para evitar accesos no autorizados.		x		
9.1.2	Control de acceso a las redes y servicios asociados	Activos informáticos (redes de comunicaciones, servidores, equipamiento auxiliar).	La gerencia debe restringir las funcionalidades, servicios y utilitarios de la red y establecer una configuración mínima de descarga de archivos, de acuerdo con las labores desempeñadas.		x		
13	SEGURIDAD EN LAS TELECOMUNICACIONES.						
13.1.1	Controles de red.	Activos informáticos (redes de comunicaciones, servidores, equipamiento auxiliar).	Las solicitudes de acceso al cuarto de sistemas o a los centros de cableado deben ser aprobadas por la gerencia bajo privilegios de acceso físico y autenticación, especialmente, mediante un método biométrico; no obstante, se deben realizar los registros en una bitácora ubicada en la entrada del lugar.		x		

Tabla 35. (Continuación)

Fuente: el autor

7.5 POLITICAS RECOMENDADAS A IMPLEMENTAR EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA COOPSENA

1. **INTRODUCCION**

La Cooperativa Multiactiva del Personal del SENA COOPSENA, define la información como el activo más importante para el cumplimiento de los objetivos establecidos como empresa de economía solidaria y de responsabilidad limitada, motivo por la cual es indispensable que fortalezca su sistema de seguridad con el fin de mejorar los niveles de protección de la información, indistintamente de la forma como se maneja, se procesa, se almacena o se transporta.

Este apartado, describe las normas y técnicas de seguridad que deberían ser implementadas para sustentar la confianza de los usuarios del sistema de información con que cuenta la institución. Para la elaboración de las mismas, se toman como base los resultados obtenidos del análisis y gestión de riesgos, determinación de salvaguardas, la legislación promulgada por el congreso de la república de Colombia y los controles y recomendaciones de la norma estándar ISO/IEC 27001:2013.

Si bien es cierto que la seguridad de la información es un proceso prioritario que toda organización debe gestionar, queda a criterio de los directivos de COOPSENA, llevar a cabo la implementación de estas normas y técnicas que sin lugar a dudas van a contribuir en el mejoramiento de las operaciones informáticas y en el cumplimiento de la legislación vigente en Colombia.

2. **OBJETIVO.**

El objetivo del apartado de este documento, es sugerir la implementación de las normas y técnicas registradas en la declaración de aplicabilidad (SOA), producto de

los nexos existentes entre la lista de chequeo y el plan de tratamiento de riesgos (PTR), con el firme propósito de mejorar el sistema de seguridad de la información de la institución COOPSENA.

3. ALCANCE

Las normas y técnicas a implementar, han de cubrir todos los procesos administrativos y de control que deben cumplir todos los funcionarios y colaboradores externos que cumplan actividades relacionadas con la función de interés social y solidario de COOPSENA, para lograr un mejor nivel de seguridad y calidad de la información que es utilizada para el cumplimiento de sus objetivos.

Por lo tanto, las normas aquí descritas estarán relacionadas con los acuerdos de confidencialidad y las sanciones para las violaciones a la política global de la seguridad informática, implementada en la Cooperativa, como también con los ocho (8) dominios del estándar ISO/IEC 27001:2013, trabajados para el desarrollo del presente proyecto.

Políticas de la entidad de la seguridad de la información

Norma a implementar.

El comité de control Interno debe planificar la realización de auditorías más constantes (por lo menos cada 2 años) al sistema de seguridad de la Información de COOPSENA a fin de establecer si las políticas, los procesos, los procedimientos y los controles implementados, están en concordancia con los requisitos de la entidad, de la seguridad y con la legislación vigente.

Política estructural de la entidad de la seguridad de la información

Normas a implementar.

a) El comité de control interno, debe velar porque se establezca la implementación de los controles técnicos y administrativos que se deriven de un proceso de evaluación y tratamiento de riesgos.

b) La dirección debe gestionar que la empresa este suscrita a una institución, páginas web o grupos de investigación especializados en seguridad de la información para fortalecer los conocimientos, mejorar y mantener actualizada la gestión de riesgos y demás procesos de la protección de los activos informáticos.

Políticas durante la vinculación de funcionarios y personal externo.

Normas a implementar.

a) La dirección debe diseñar y poner en funcionamiento permanentemente, un programa de formación y concienciación en seguridad informática, con el fin de apoyar la protección de la información y de los activos informáticos utilizados para el tratamiento, procesamiento, almacenamiento y distribución de la misma.

b) La dirección debe convocar regularmente, a los funcionarios a charlas y eventos relacionados con el programa de formación y concienciación en seguridad informática, asignar los recursos para su ejecución, controlar la asistencia y aplicar las sanciones correspondientes por fallas no justificadas.

Política para uso de estaciones de trabajo

Normas a implementar.

a) La dirección debe implementar un método de bloqueo, por ejemplo, contraseñas o un procedimiento biométrico para las estaciones de trabajo de la entidad que son entregados a los funcionarios. Se debe realizar la configuración de estos elementos para que después de un tiempo de inactividad, sean suspendidos automáticamente, igualmente, sea activado el bloqueo de la pantalla que requerirá el método de desbloqueo configurado.

b) El funcionario que por x o y motivos abandone por un determinado tiempo la estación de trabajo, debe activar el protector de pantalla, en caso contrario será objeto de aplicación de las sanciones respectivas.

c) Los usuarios del sistema informático, por ningún motivo deben almacenar imágenes, fotografías, videos, u otro tipo de información de carácter personal en los recursos de almacenamiento de las estaciones de trabajo.

Política de uso de medios de almacenamiento

Normas a implementar.
La dirección debe gestionar la implementación de controles que regulen el volumen de archivos a almacenar en los medios de almacenamiento de la plataforma tecnológica de la entidad, de acuerdo con los requerimientos y condiciones establecidas en el nivel de privilegios.

Política de acceso al cuarto de sistemas

La Dirección de COOPSENA, como directo responsable de las redes de datos y activos relacionados a las mismas, debe implementar un mecanismo de control de acceso biométrico para que dichos recursos tengan un nivel de acceso más eficiente contra accesos no autorizados.

Política de gestión de vulnerabilidades

Normas a implementar.

a) El comité de control interno debe gestionar ante la dirección de COOPSENA, los trámites correspondientes para la realización de pruebas de penetración y hacking ético con una planificación bien establecida, por una entidad especializada e independiente, con el fin de garantizar un mejor análisis e identificación de vulnerabilidades en el sistema.

b) La Dirección debe gestionar los lineamientos y recomendaciones para las pruebas de hacking ético que permitirían un mejor análisis y una óptima reducción de vulnerabilidades.

Políticas de uso adecuado de internet

Normas a implementar

La Dirección debe implementar controles para evitar el acceso no autorizado a los sitios restringidos de la red que van en contra de las funciones administrativas de la entidad.

7.6 PLAN DE CONTINUIDAD DE NEGOCIO PARA LA COOPERATIVA MULTIACTIVA DEL PERSONAL DE SENA, COOPSENA.

Fase l. Marco teórico, alcance, propósito y objetivos

Marco teórico

El contenido expuesto en este plan, es un proceso complementario del SGSI, pues constituye una serie de procedimientos que inspiran y dirigen la toma de decisiones por parte de la directiva de COOPSENA para prepararla y protegerla ante un incidente o amenaza, y fomentar su capacidad de supervivencia, mejorar la imagen corporativa y mantener la ventaja competitiva, atribuido por la capacidad de ofrecer servicios de buena calidad para lograr sus objetivos y asegurar sus beneficios sociales, económicos y legales.

El Plan de Continuidad del negocio (en adelante identificado como PCN), comprende una serie de actividades limitadas exclusivamente al ámbito del sistema de tecnología de la información y las comunicaciones; por consiguiente, necesita de la colaboración activa de las diferentes áreas funcionales de la institución. Por eso, en este documento se ha establecido el nombramiento de una persona con suficiente capacidad y confianza para que asuma el liderazgo del comité del PCN.

Sin embargo, la gestión de dicho equipo y el cumplimiento de los objetivos planteados ante una situación crítica por un incidente, que permitan que la institución pueda recuperarse lo más pronto posible, necesariamente depende de la directiva de COOPSENA quien debe comprometerse con los procedimientos propios del plan, gestionando y asegurando los recursos y el presupuesto suficientes para el equipo del PCN, así como el programa de capacitación y entrenamiento con el fin lograr los resultados esperados.

Para la adecuada implementación del PCN, es necesario tener en cuenta las normas internacionales que especifican los requisitos y procedimientos para asegurar la infraestructura de un sistema de tecnologías de la información y sus procesos relacionados, al igual que las normas estatales que regulan el uso y la protección de los datos, como lo son:

- Estándar ISO/IEC 27001:2013.
- Estándar ISO/ IEC/22301
- Ley 1273 de 2009
- Ley 1341 del 30 de julio de 2009
- Decreto 1377 de junio 27 de 2013

Alcance

Este plan está limitado al departamento de sistemas y telecomunicaciones de COOPSENA, sobre el cual están soportados el 98% de los procesos que rigen su actividad económica solidaria.

Propósito

Proporcionar las medidas específicas que la directiva de COOPSENA debe desarrollar para prepararse y reaccionar apropiadamente, ante un desastre, accidente o ataque cibernético que podría afectar de manera crítica, el correcto funcionamiento de los sistemas que soportan su información y recuperar los servicios y procesos en el menor tiempo posible.

Objetivos

- Establecer los mecanismos y los recursos que permitan una reacción inmediata ante cualquier interrupción del área de sistemas y comunicaciones,

que pueda verse comprometido por circunstancias de índole natural o humana, y poder recuperar los procesos críticos del negocio lo más pronto posible.

- Enumerar los servicios, aplicaciones y plataformas tecnológicas consideradas como críticas para las funciones operativas y de soporte del negocio.

- Identificar el recurso humano altamente capacitado que se requiere a nivel interno y externo para llevar a cabo las actividades operativas de recuperación del sistema de tecnología de la información ante un evento crítico.

- Fijar los tiempos menores posibles que se requieren para recuperar las funciones del sistema de tecnología de la información en las que se vean afectado los demás procesos del negocio.

- Indicar el desarrollo de un plan de pruebas para identificar su efectividad o falencias con el fin de mejorar su diseño y procedimientos.

- Sugerir el desarrollo de un plan de capacitación para el adecuado funcionamiento del PCN.

Fase II: organización del comité del PCN

El conjunto de personas a conformar el comité del PCN, deben tener las competencias necesarias para la activación y desarrollo de las diferentes actividades destinadas a la reducción de los incidentes y la incertidumbre generada, así como mantener informados de la situación, a los directivos de la institución.

Tabla 36. Principales actividades y roles del comité del PCN

Rol	Responsabilidades
Director del PCN	▪ Establecer las políticas del PCN. ▪ Programa las sesiones de sensibilización y capacitación a cada uno de los integrantes del comité del PCN y demás funcionarios de la institución. ▪ Programa las actividades de ejecución de pruebas del PCN. ▪ Implementar la estrategia de recuperación seleccionada teniendo en cuenta el recurso humano y financiero, asignados. ▪ Analizar el incidente presentado. ▪ Determinar si se activa o no el PCN. ▪ Comunicar oficialmente a los funcionarios de la institución, sobre el incidente presentado a través de los coordinadores del comité. ▪ Coordinar la reunión de los miembros del comité del PCN y poner en marcha el proceso de recuperación y restauración. ▪ Analizar el impacto generado por el incidente. ▪ Coordinar el proceso de retorno a la normalidad.
Coordinador del equipo de recuperación del SI.	▪ Dar respuesta inmediata sobre el incidente presentado al director del PCN, quien activa el plan si el incidente es grave. ▪ Establece los procesos de actualización de la infraestructura tecnológica necesaria para la recuperación funcional del sistema (Computadores, servidores, enrutadores, switches, etc.). ▪ Liderar la recuperación de los elementos tecnológicos, teniendo en cuenta las actividades de continuidad. ▪ Mantiene comunicación con los proveedores de servicios y elementos de tecnología.

	▪ Revisa la documentación correspondiente al plan de pruebas y establece los resultados obtenidos.
Coordinador del equipo logístico	▪ Responsable de dirigir las actividades internas o externas asociadas al proceso logístico de recuperación, como: transporte de equipos, materiales, personas al sitio de recuperación, suministro de víveres, etc. ▪ Gestionar la consecución y adecuación de los centros alternos de operaciones según el plan de operaciones en contingencia.
Coordinador del equipo de las unidades de negocio	Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.
Coordinador del equipo de relaciones publicas	Responsable de administrar y dirigir los canales de comunicación con los clientes, proveedores y equipos noticiosos.

Tabla 36. (Continuación)

Fuente: el autor

Sitio de reunión del comité del PCN

Por la cercanía y fácil acceso en caso de presentarse un incidente de altas proporciones, el sitio de reunión será la casa ubicada en la calle 52 No. 9-36 (anterior sede).

Fase III. Análisis de impacto del negocio (BIA – Business Impact Analysis)

El BIA, es el proceso analítico de las funciones operativas críticas de un negocio y el impacto que una interrupción de un sistema podría generar sobre las mismas.

Entre las actividades para llevar a cabo este proceso tenemos:

- Entrevistas; actividad que se debe realizar en cada departamento para conocer los procesos en cada uno de ellos.
- Inspeccionar las dependencias de los procesos con relación al sistema de información y de telecomunicaciones.
- Establecer reuniones con los usuarios finales de los procesos más críticos con el fin de obtener información más clara y sensible.
- Determinar las exigencias temporales de las aplicaciones o procesos, fortalezas y debilidades en la perdida de datos.
- Examinar la capacidad del sistema de información y telecomunicaciones en cuanto a respaldo de datos, seguridad de la información, tiempo de recuperación, procesamiento y almacenamiento de datos.

Los resultados de la evaluación y análisis de la información obtenida de este proceso, permiten determinar los siguientes parámetros.

- RTO
- RPO
- MTD
- Nivel de criticidad

También permite determinar, cuales son los recursos informáticos y tecnológicos que generan una mayor intervención por estar condicionados a las altas exigencias temporales de continuidad operativa del negocio.

Las tablas 37, 38 y 39, ilustran el análisis de tres de los procesos más críticos de COOPSENA.

Tabla 37. Descripción de procesos críticos en COOPSENA

Proceso	Descripción	Frecuencia	Líder
Crédito y cartera	Se encarga de administrar los requisitos de legalización, viabilidad jurídica, novedades, renovación y simulación de los créditos otorgados a los asociados, como también, el manejo de los procedimientos técnicos para la administración y control eficiente de la cartera que permitan fomentar y proyectar el negocio dentro del mínimo riesgo posible.	Diaria	María Esnedy Arango González
Servicio al cliente	Se ocupa de establecer la buena relación entre la COOPERATIVA y sus asociados con el fin de mantener su fidelidad, gracias a los servicios y programas de economía solidaria que permiten	Diaria	Carlos Javier Garzón Lasprilla

	satisfacer sus necesidades.		
Contabilidad	Se ocupa del control de las operaciones económicas, financieras y sociales, mediante el correcto tratamiento de la información para apoyar la toma de decisiones de la institución que la orienten a obtener adecuados indicadores de desempeño.	Semanal	Pedro Pablo Chacón Hernández

Tabla 37. (Continuación)

Fuente: http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Tabla 38. Componentes informáticos de los procesos críticos en COOPSENA

Proceso	Servicio o aplicación	Tipo de sistema	Nivel de criticidad	N° de equipos con la aplicación o servicio	Responsable
Crédito y cartera	SAPIENS. Software para la gestión de crédito y cartera.	Servidor de aplicaciones/ S.O/PC'S/Impresoras	Alto	5	Héctor Fabio Barón.

Servicio al cliente.	Correo electrónico	Servidor de correos/Sistema de comunicaciones/PC'S/S.O	Alto	6	Héctor Fabio Barón.
Contabilidad	SAPIENS. Software para la gestión contable.	Servidor de aplicaciones/ S.O/PC'S/Impresoras	Medio	3	Héctor Fabio Barón.

Tabla 38. (Continuación)

Fuente: http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Tabla 39. Parámetros del análisis de impacto del negocio

Proceso	MTD	RTO	RPO
Servicio al cliente	5 días	24 horas	72 horas
Crédito y cartera	6 días	36 horas	72 horas
Contabilidad	8 días	48 horas	72 horas

Fuente: https://webcache.googleusercontent.com/search?q=cache:YoKjI8eriNAJ:https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/contingencia_y_continuidad_de_negocio/plantilla_ejemplo_bia.xls+&cd=12&hl=es&ct=clnk&gl=co&client=firefox-b

Fase IV. Determinación de la estrategia de respaldo

La estrategia de respaldo, es una herramienta que se fundamenta en los resultados del BIA y del análisis y gestión de riesgos y, cuyo objetivo es garantizar la continuidad de las operaciones de los sistemas de información y telecomunicaciones, de los cuales dependen los procesos críticos del negocio frente a una interrupción de alto impacto.

Estrategia de sitio alterno

Aunque existen varias estrategias de recuperación, como los acuerdos recíprocos, centro replicado, sitio alternativo subcontratado a terceros, etc. Todos ellos requerirían una mayor inversión por parte de la institución; por eso, la mejor solución para la continuidad del negocio en caso de un incidente de altas proporciones, corresponde a la estrategia de sitio alterno, teniendo en cuenta que COOPSENA cuenta con los siguientes bienes y servicios.

- Instalaciones de la casa ubicada en la calle 52 No. 9-36 (anterior sede)
- Servicio Datacenter Cloud Computing
- Servicio de tecnología VPN

También existe la posibilidad de continuar operaciones desde ubicaciones externas mediante la modalidad de *Teletrabajo*.

Fase V. Determinación de los recursos para la continuidad de los procesos críticos.

La continuidad de los procesos críticos, depende de la disponibilidad de los recursos que la organización haya gestionado tanto interna como externamente, de lo contrario el PCN, será un fracaso. La tabla 40, ilustra una lista de recursos que son indispensables para apoyar un PCN.

Tabla 40. Recursos para la continuidad de los procesos críticos

Tipos de recursos		Contenido
Recursos internos	Inmuebles	
	Mobiliario de oficina	
	Dispositivos informáticos	
	Sistema de comunicaciones	
	Aplicaciones	
	Servicios	
	Recurso humano	
	Fondos disponibles	
	Medidas financieras	
Servicios esenciales	Agua	
	Luz	
	Electricidad	
	Gas	
	Comunicaciones	
	Transporte	
Recursos externos	Proveedores	
	Clientes	
	Soluciones financieras	

Fuente: https://apecmsmemarketplace.com/sites/default/files/doc/bcp_guidebook_abridged_version_spanish_20140829.pdf

Fase VI. Activación y ejecución del PCN

Esta fase es la que define los procedimientos que deben llevar a cabo los equipos del PCN, como respuesta a la contingencia que ponga en riesgo de pérdida parcial o total, uno o más de los procesos críticos de la organización. Esta etapa al igual que las demás, debe estar minuciosamente documentada, pues es un elemento clave para la gestión de una situación de crisis, cuya finalidad es evitar situaciones de pánico, que se tomen decisiones imprevistas o equivocadas que puedan agravar aún más la situación.

Por eso, esos procedimientos deben estar redactados en un lenguaje claro y comprensible, y deben ser de fácil acceso a las personas involucradas o que tienen una relación de responsabilidad directa con el PCN para el cumplimiento de la metodología establecida, y recuperar el estado normal de las actividades criticas del negocio en el menor tiempo posible.

Procedimiento de activación del PCN

Dado que cualquier funcionario de COOPSENA, debe estar en capacidad de reconocer un incidente importante que pueda afectar a la institución (por el conocimiento adquirido en el programa de capacitación y concienciación), debe comunicarlo de manera inmediata al líder del PCN, quien a paso seguido, debe informar a los directivos de la institución y convocar el comité respectivo al sitio de reunión para determinar si se activa o no el PCN, de acuerdo a los siguientes criterios:

- Identificación del tipo de incidente
- Análisis y evaluación para determinar su nivel de impacto.
- Identificación de procesos involucrados
- Tiempo de interrupción generado por el incidente.

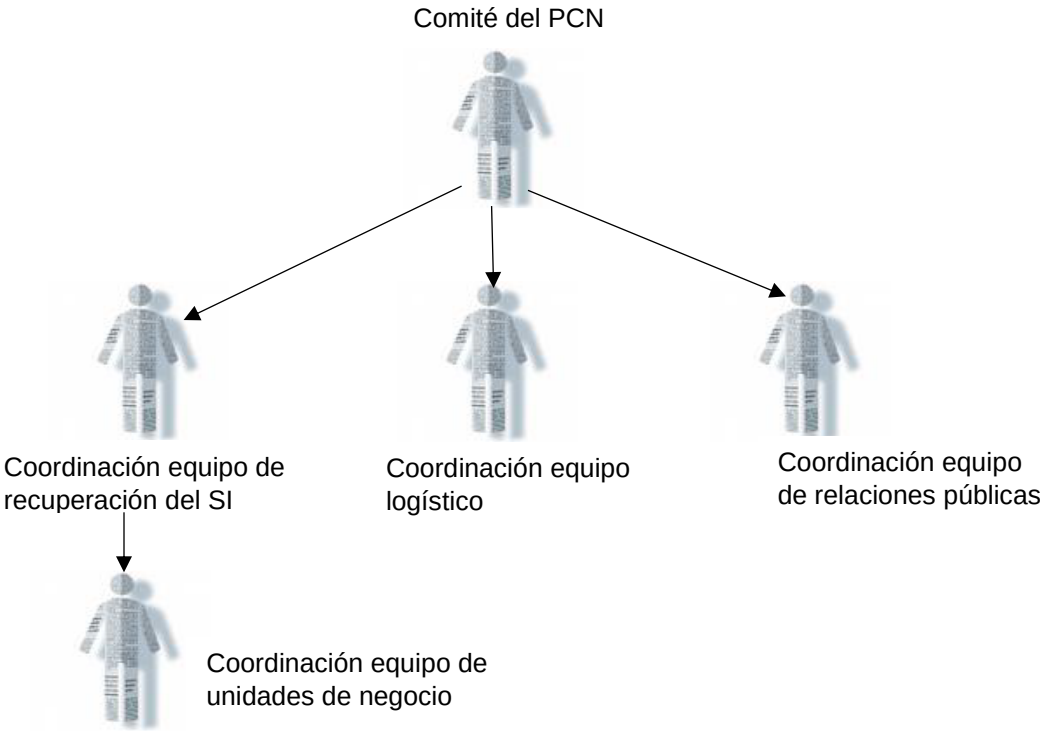
Una vez obtenidos los resultados de este procedimiento, el líder junto con el comité del PCN, será quien toma la decisión de activarlo y poner en ejecución los procedimientos de recuperación. Si por el contrario el comité decide no activar el PCN, deberán establecer las medidas necesarias de gestión del incidente para evitar un impacto significativo en el futuro.

Procedimientos de recuperación

Una vez que los directivos de la organización y el comité del PNC, deciden seleccionar y poner en ejecución los procedimientos de recuperación, las primeras acciones a seguir son:

- Poner en marcha el árbol de llamadas

Figura 8. Árbol de llamadas

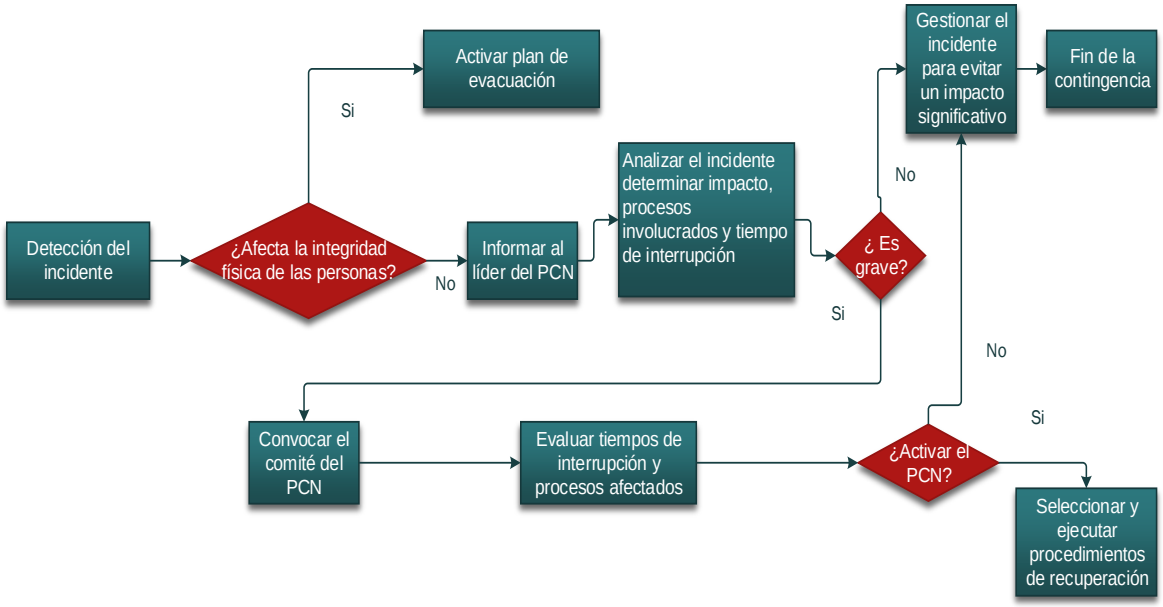


Fuente: http://www.criptored.upm.es/guiateoria/gt_m001r.htm

- Revisión del BIA
- Revisión de los niveles prioritarios de la infraestructura tecnológica
- Revisión de planes operativos existentes
- Personal disponible para el proceso de recuperación
- Revisión de los medios y recursos disponibles para la continuidad de los procesos críticos.

La figura 9, muestra brevemente una serie de actividades que la institución debe realizar una vez que se detecte un incidente que produzca una interrupción en uno o más de sus procesos críticos.

Figura 9. Secuencia de actividades en caso de una interrupción del SI



Fuente:http://ceeielche.emprenemjunts.es/descargando/1871_descarga.pdf

Entre los procedimientos de recuperación que la directiva de COOPSENA debe definir, planificar, coordinar, apoyar y asegurar para que el PCN tenga efectividad tenemos:

- Procedimiento para asegurar que todos los datos estén a salvo y que se pueda acceder a ellos
- Procedimiento de recuperación ante interrupción total del suministro eléctrico.
- Procedimiento de recuperación ante interrupción total de la conexión a internet o de la red del sistema de telecomunicaciones.
- Procedimiento de recuperación ante interrupción total de los servidores.
- Procedimiento de recuperación ante un ataque informático.
- Procedimiento de recuperación ante interrupción por fallas de hardware y/o software.
- Procedimiento de recuperación ante interrupción total o parcial por propagación de software malicioso.
- Procedimiento de continuidad ante interrupción por ausencia de personal
- Procedimiento de continuidad ante ausencia de suministro de servicios públicos.
- Procedimiento de recuperación ante interrupción total por un desastre natural (incendio, inundación, terremoto).

El último procedimiento enumerado, debe estar complementado por las acciones consistentes que se deben realizar antes, durante y después del desastre, tales como:

- Procedimiento de traslado de material, equipos y personas al sitio elegido como estrategia de recuperación.
- Procedimiento de puesta en marcha del sitio alterno de recuperación.
- Procedimiento de restauración del sistema informático y de los procesos críticos del negocio.
- Procedimiento de soporte y gestión de las áreas de procesos críticos.
- Procedimiento de gestión de seguridad de la información.

Fase VII: vuelta a la normalidad

Una vez recuperadas las funciones del sistema informático y/o de telecomunicaciones, que habían estado interrumpidas por el impacto del incidente y puestos en marcha los procesos críticos involucrados, el proceso a seguir es llevar a cabo las operaciones de recuperación normal y total del sistema junto con todos los demás procesos del negocio. Entre esas operaciones tenemos:

- Evaluación y análisis del impacto; esta actividad permite determinar que parte de la tecnología de la información fue averiada, si se puede reconstruir o por el contrario es necesario la obtención de equipos y materiales nuevos.
- Poner a prueba todo el sistema de tecnología de la información antes de reanudar todos los procesos y actividades productivas del negocio.
- Determinar que toda la documentación relevante de las funciones del sistema de tecnología de la información se encuentra disponible y actualizada.
- Actualizar el PCN y el plan de recuperación del sistema de tecnología de la información ante un futuro incidente.

Fase VIII: revisión y actualización del PCN

Revisión del PCN

Para que el PCN tenga validez y sea realmente efectivo ante una circunstancia que interrumpa los recursos informáticos de la empresa, esta debe contar con un plan de pruebas que simule la identificación y prevención de incidentes de seguridad, de tal manera que estos puedan ser gestionados y atendidos para saber cuán competente es el PCN en cuanto al restablecimiento de los procesos críticos del negocio según los objetivos establecidos, y de acuerdo a los resultados aprobar el plan, o dado el caso cambiar algunos aspectos para que dicho proceso adquiera solidez y esté disponible para una contingencia real.

Las pruebas deben ser realizadas con cierto grado de complejidad de tal forma que se aproximen a situaciones reales; por lo tanto, deben programarse con suficiente flexibilidad en cuanto a espacio y tiempo para que las operaciones normales de la institución sufran el mínimo impacto posible. En ese sentido, Del Pino Jiménez señala que, “Las pruebas de un Plan de Continuidad deben tener dos características principales: realismo y exposición mínima”[40].

[40] Del PINO JIMÉNEZ, Laura. Guía de desarrollo de un plan de continuidad de negocio. {En línea}. Julio de 2007. {Consultado en octubre de 2017}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Tabla 41. Tipos de pruebas del plan de continuidad del negocio

(-)

Complejidad

(+)

Tipo de prueba	Descripción
Test de consistencia	El plan de continuidad de negocio es distribuido a los departamentos y/o áreas funcionales implicadas para su revisión/actualización.
Test de validez	Representantes de cada departamento y/o área funcional implicada se reúnen para revisar y discutir el plan.
Test de simulación (simulacro)	Escenario ficticio de recuperación para verificar que el Plan de Continuidad contiene la información necesaria y suficiente.
Test actividades críticas	Recuperación real de una actividad crítica bajo un entorno controlado y sin poner en peligro la operativa usual/original.
Test completo	Interrupción real de las operaciones y recuperación de las mismas a través de los procedimientos del Plan de Continuidad.

Fuente: http://ceeielche.emprenemjunts.es/descargando/1871_descarga.pdf

Actualización del PCN

Teniendo en cuenta que un PCN, permite seguir brindando un buen servicio a los clientes y funcionarios de la organización, al sortear lo menos posible el impacto de un incidente que con relación al tiempo, ponga en riesgo las operaciones del sistema de tecnologías de la información del cual dependen procesos críticos, cuya inactividad generaría altas perdidas económicas; es imprescindible la planeación y gestión del mejoramiento continuo de dicho proceso con el fin de fortalecer su eficiencia, pues en resumidas cuentas, se trata de una estrategia clave y critica para la fiabilidad organizativa.

La gestión de mejoramiento continuo de un PCN, no solamente prepara a la organización para superar factibles interrupciones de sus procesos importantes ante una contingencia, sino que también la acondiciona a los cambios organizacionales que generan la globalización de los mercados y el desarrollo constante de las tecnologías informáticas.

Fase IX. Capacitación y concienciación

Con el fin de complementar la formación y concienciación de los funcionarios, integrantes de los comités administrativos y del PCN, asociados, contratistas y proveedores; la conceptualización, normas, políticas, procedimientos y responsabilidades, relacionados al PCN, deben hacer parte del programa de sensibilización del SGSI propuesto durante el desarrollo del presente proyecto.

Ese programa de capacitación, permitirá resaltar la importancia y los beneficios que el PCN representa en primer lugar, para la conservación de la salud y la vida de las personas, en segundo lugar, garantizar la estabilidad de la institución en caso de presentarse algún incidente que ponga en riesgo sus procesos críticos, y en tercer lugar, mejorar la cultura y la eficiencia organizacional.

8. CONCLUSIONES

Un SGSI debe ser considerado por todo tipo de organizaciones como el proceso estratégico más importante a la hora de administrar los recursos de protección de la infraestructura tecnológica, especialmente cuando se trata de conseguir un nivel de garantía más eficiente y una mayor calidad de la seguridad de la información que es utilizada para el cumplimiento de los objetivos corporativos.

La implementación de esta norma en una organización, permite gestionar la seguridad de los sistemas de tecnología de la información de una forma altamente organizativa al considerar como primera medida, la existencia y valoración de los activos informáticos, como segunda medida, el análisis de amenazas y vulnerabilidades y por último, la gran posibilidad de contar con procedimientos y controles que permiten cuantificar la eficiencia de las disposiciones aceptadas con base en el ciclo de vida de la información y los dispositivos informáticos que la gestionan.

Estas acciones de tipo organizativo y técnico brindan niveles de protección adecuada a las organizaciones frente a las amenazas y riesgos cuyos resultados pueden afectar seriamente, la continuidad de una empresa. Por eso, la ISO/IEC 27001:2013 es uno de los estándares que más se ha fortalecido para dichos propósitos.

La metodología seleccionada para lleva a cabo la gestión de riesgos MAGERIT, cuyos procedimientos hacen parte de la etapa planificar del ciclo de Deming incluido en la norma ISO 27001, aporta grandes beneficios en las etapas de diseño e implementación de un SGSI al facilitar el proceso de gestión de riesgos, cuyos resultados oportunos, permiten optimizar el tiempo para establecer las salvaguardas destinadas a minimizarlos o a controlarlos y evitar un impacto potencial en el futuro.

Todos estos criterios han permitido una mejor visión sobre la importancia de diseñar y describir este proyecto investigativo y su posible implementación en el futuro, debido a las falencias que en materia de seguridad de la información, se pudieron identificar durante el desarrollo del mismo.

9. RECOMENDACIONES

Para que el presente proyecto cumpla en buena parte sus expectativas, se recomienda a la Dirección de la Cooperativa Multiactiva de Personal del SENA COOPSENA, tener en cuenta la temática que cubre su contenido sobre la importancia que implica el diseño y posible implementación de un SGSI bajo la norma ISO/IEC 27001:2013, cuya estructura se centra en establecer las políticas y procedimientos para gestionar los riesgos a los que está sometida la información, activo vital para el cumplimiento de los objetivos de negocio.

De igual manera, se recomienda la suscripción a un sitio web, entidad o comunidad que permita proveer información sobre seguridad informática, que apoye el uso instruido de técnicas tecnológicas de seguridad y la investigación innovadora con el fin de fortalecer los conocimientos y las buenas prácticas de la seguridad informática.

Es necesario que la dirección de la Cooperativa, tenga muy en cuenta los resultados obtenidos en la matriz de gestión de riesgos (Tabla 32), pues, aunque los promedios de magnitud de daño son de baja probabilidad e impacto bajo, siguen siendo riesgos; por lo tanto, no deben ser ignorados, sino que deben seguir siendo gestionados como riesgos, mediante un análisis cualitativo y documentado con el fin de mantener un control sobre los mismos.

Por eso, siendo el promedio más alto el correspondiente a la impericia y negligencia de usuarios/as, se recomienda crear un programa de seguridad informática que sea compatible con la cultura y la tecnología implementada en la entidad, que permita de tal forma encontrar soluciones a los aspectos negativos y aprovechar las fortalezas existentes para el mejoramiento progresivo de los procesos mediante una buena formación y concienciación sobre seguridad de la información.

9.1 PROGRAMA DE SENSIBILIZACION

La propuesta de este programa tiene como objetivo el de sensibilizar a los funcionarios, contratistas y usuarios externos de la entidad, en el buen uso y aprovechamiento de los recursos informáticos puestos bajo su responsabilidad para el debido cumplimiento de su deber, siguiendo los lineamientos del SGSI, también pretende capacitar a los administradores de sistemas, encargados de gestionar la seguridad de la información al interior de la entidad.

Para llevar a cabo dicho programa, se sugiere la ejecución de una campaña que permita divulgar y sensibilizar masivamente, a todos los usuarios que de manera directa o indirectamente, hacen parte del funcionamiento de la entidad para que acojan el Modelo de Seguridad de la Información, de tal forma que comprendan sus responsabilidades, cómo deben interactuar, orientarse y armonizar con el sistema de calidad (ISO 9001-2008), control interno y el SGSI bajo la norma ISO/IEC 27001:2013

Se propone que esta campaña de divulgación y sensibilización haga uso de los siguientes medios:

Medios impresos: afiches colocados en el interior de la oficina principal de la Cooperativa y en cada una de sus sedes a nivel nacional, y en las carteleras ubicadas en cada uno de los centros de formación del SENA, los cuales deben contener información resumida sobre las características y políticas del SGSI y como se puede colaborar a la entidad en la futura implementación y mejoramiento del SGSI.

Medios interactivos: Fondos de escritorio y protectores de pantalla con imágenes y videos con información relacionada al Modelo y políticas de seguridad de la información.

Recursos de Internet: publicación detallada de la información del SGSI en la página web de la entidad, www.coopsena.com.co

BIBLIOGRAFIA

LIZARAZO RUEDA, Javier Enrique. El ser humano: Factor clave en la seguridad de la información. {En línea}. Septiembre de 2012. {Consultado el 9 de octubre de 2016}. Disponible en: http://docplayer.es/1146750-El-ser-humano-factor-clave-en-la-seguridad-de-la-informacion.html

BANCO DE LA REPÚBLICA. Mecanismos de seguridad de los servicios informáticos. {En línea}. Junio de 2007. {Consultado en octubre de 2016}. Disponible en:
http://www.banrep.gov.co/economia/pli/Mecanismos_de_Seguridad_Informatica.pd

MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Elaboración de la política general de seguridad y privacidad de la información. {En línea}. 11 junio 2016. {Consultado en octubre de 2016}. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Informe final – modelo de seguridad de la información – sistema sansi - sgsi - modelo de seguridad de la información para la estrategia de gobierno en línea. {En línea}. Diciembre de 2008. {Consultado el 14 de octubre de 2016}. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf.

ARRIETA, Álvaro. Políticas y normas de seguridad informática. {En línea}. 2011. {Consultado el 12 de septiembre de 2016}. Disponible en, http://www.cvs.gov.co/jupgrade/images/stories/docs/Alertas/Politicas_de_Seguridad_Informatica_CVS_2011-.pdf

CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL. Lineamientos de política para ciberseguridad y ciberdefensa. {En línea}. 14 de junio de 2011. {Consultado en septiembre de 2016}. Disponible en, http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

EL TIEMPO. El hacker Andrés Sepúlveda es enviado a la cárcel. El tiempo. {En línea}. 7 de mayo de 2014. {Consultado en septiembre de 2016}. Disponible en: http://www.eltiempo.com/archivo/documento/CMS-13950196

EL PAIS. En Colombia las cifras de delitos informáticos van en aumento. {En línea}. Diciembre 31 de 2012. {Consultado en septiembre de 2016}.Disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento

RAMIÓ AGUIRRE, Jorge. Libro Electrónico de Seguridad Informática y Criptografía. Introducción a la seguridad informática. {En línea}. 01 marzo 2006. {Consultado en septiembre de 2016}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001a.htm

BARRY M. Leiner, VINTON G. CERF, David D. CLARK, Robert E. KAHN, Leonard, KLEINROCK, Daniel C. LYNCH, Jon Postel, LARRY G. Roberts, WOLFF Stephen. Breve historia de internet. {En línea}. {Consultado en septiembre de 2016} Disponible en: http://www.internetsociety.org/es/breve-historia-de-internet

MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Día de la Seguridad Informática. {En línea}. 12 de septiembre de 2012. {Consultado en septiembre de 2016}. Disponible en: http://www.enticconfio.gov.co/dia-de-la-seguridad-informatica

CAROLINACOLS. Fundamentos de seguridad informática. {En línea}. {Consultado en septiembre de 2016}. Disponible en: https://carolinacols.files.wordpress.com/2012/03/fundamentos-bc3a1sicos-de-seguridad-informc3a1tica.pdf

INTENSAS.COM. Infraestructura tecnológica. {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.intensas.com/infraestructura-tecnologica/

UOC.EDU. Infraestructura tecnológica. {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/serveis/index.html

SUAREZ SIERRA, Lorena Patricia. Sistema de Gestión de la Seguridad de la Información (SGSI). {En línea}. Julio de 2013. {Consultado en octubre de 2016}.Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-SGSI-233003.pdf

ISO 27000.ES. El portal de ISO 27001 en español. {En línea}. {Consultado en octubre de 2016}. Disponible en: http://www.iso27000.es

INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION. Implantación de un SGSI en la empresa. {En línea}. {Consultado en octubre de 2016}. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27000. ES. Sistema de Gestión de Seguridad de la Información. {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISACA. Cobit 5. Resumen ejecutivo. {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://www.google.com.co/#q=mantener+un+equilibrio+entre+la+realizaci%C3%B3n+de+beneficios+y+la+optimizaci%C3%B3n+de+los+niveles+de+riesgo+y+utilizaci%C3%B3n+de+los+recursos

NIST. Risk Management Guide for Information Technology Systems Julio de 2002. {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

DUQUE OCHOA Blanca Rubiela. Metodologías de gestión de riesgos. {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

FRANCABILLA, Carlos. Como aporta COBIT 5 y gobernanza de TI a la gobernanza empresarial {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014-COBIT%20y%20Gobernanza%20de%20TI.pdf

ESPINOSA T Diego, MARTÍNEZ P Juan, AMADOR D Siler. Gestión del riesgo en la seguridad de la información con base en la norma iso/iec 27005 de 2011, proponiendo una adaptación de la metodología octave-s. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control académico (darca) de la universidad del cauca. Febrero de 2014. {En línea}. {Consultado en noviembre de 2016}.disponible en: http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

Auditoria en Informática CUN. Distribución de los dominios y procesos de COBIT. {En línea}. {Consultado en noviembre de 2016}. Disponible en: https://sites.google.com/site/auditoriaeninformaticacun/cobit/dominios-y-procesos

OLMO PARRA, Antonio Santos; SÁNCHEZ CRESPO, Luis Enrique; MEDINA PATÓN, Eduardo Fernández; PIATTINI VELTHUIS, Mario. Métricas de seguridad en los SGSI, para conocer el nivel de seguridad de lo SSOO y de los SGBD. {En línea}. {Consultado en noviembre de 2016. Disponible en: http://www.criptored.upm.es/cibsi/cibsi2011/info/Ponencias/6.%20M%C3%A9tricas%20de%20seguridad%20en%20los%20SGSIs,%20para%20conocer%20el%20nivel%20de%20seguridad%20de%20los%20SSOO%20y%20de%20los%20SGBD.pdf

INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION. Guía avanzada de gestión de riesgos. {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://www.ficad.org/lecturas/adicional_uno_tercera_unidad_soma.pdf

INSTITUTO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Magerit-versión 3.0, Metodología de análisis y gestión de riesgos de los sistemas de información. {En línea}. Octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WABC-cmdDIU

ADVISERA.COM. ¿Qué es ISO 27001? {En línea}. {Consultado en noviembre de 2016}. Disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Norma Técnica Colombiana NTC-ISO/IEC 27001. Marzo de 2006. {En línea}. {Consultado en noviembre de 2016}. Disponible en:

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

CONGRESO DE COLOMBIA. Ley 1273 de enero 05 de 2009. {En línea}. Enero 05 de 2009. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

CONGRESO DE COLOMBIA. Ley 1341 del 30 de julio de 2009. {En línea}. 30 de julio de 2009. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles 3707_documento.pdf

CONGRESO DE COLOMBIA. Ley estatutaria 1581 del 17 de octubre de 2012. {En línea}.17 de octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf

MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO. Decreto 1377 del 27 de junio de 2013. {En línea}. 27 de junio de 2013. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos; BAPTISTA LUCIO, Pilar. Metodología de la investigación. {En línea}. Enero de 1997. {Consultado en octubre de 2016}.Disponible en: http://www.derechoshumanos.unlp.edu.ar/assets/files/documentos/metodologia-de-la-investigacion.pdf

COOPSENA. Quienes somos. {En línea}. {Consultado en noviembre de 2016}.Disponible en: http://www.coopsena.com.co/html/somos.html

SOTELO BEDÓN Marcos; TORRES UTRILLA José; RIVERA ORTEGA Juan. Un Proceso Práctico de Análisis de Riesgos de Activos de Información. {En línea}. {Consultado en marzo de 2017}. Disponible en: http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

APEC. Guía para desarrollar un plan de continuidad de negocios. {En línea}. {Consultado en octubre de 2017}. Disponible en: https://apecmsmemarketplace.com/sites/default/files/doc/bcp_guidebook_abridged_version_spanish_20140829.pdf

Del PINO JIMÉNEZ, Laura. Guía de desarrollo de un plan de continuidad de negocio. {En línea}. Julio de 2007. {Consultado en octubre de 2017}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001r.htm

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR. Manual de administración del plan de continuidad de negocios. {En línea}. Mayo de 2013. {Consultado en octubre de 2017}. Disponible en: https://portal.icetex.gov.co/Portal/docs/default-source/documentos-el-icetex/biblioteca/manuales-de-la-entidad/manual_de_administraci%C3%B3n_del_plan_de_continuidad_del_negocio.pdf?sfvrsn=2

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Plan de contingencia y continuidad de negocio. {En línea}. {Consultado en octubre de 2017}. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Octubre

de 2010. {En línea}. {Consultado en octubre de 2017}.Disponible en:http://ceeielche.emprenemjunts.es/descargando/1871_descarga.pdf

MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Guía para realizar el Análisis de Impacto de Negocios BIA. . {En línea}. Mayo 05 de 2015. {Consultado en octubre de 2015}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

OSORIO MONTOYA, Andrés Mauricio. Plan de continuidad del negocio una perspectiva preventiva para evitar impactos potenciales caso PREBEL, S. A. {En línea}. 2011. {Consultado en octubre de 2017}. Disponible en: https://repository.eafit.edu.co/xmlui/bitstream/handle/10784/1574/OsorioMontoya_AndresMauricio_2011.pdf?sequence=1&isAllowed=y

FERRER, Rodrigo. Plan de continuidad del negocio. {En línea}. Febrero 16 de 2010. {Consultado en octubre de 2017}. Disponible en: http://www.sisteseg.com/files/DocumentometodologiaBCPyDRP.pdf

ANEXOS

Anexo A. Dominios y controles de la ISO/IEC 27001:2013

Tabla 42. ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD. **5.1 Directrices de la Dirección en seguridad de la información.** 5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información. 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC. **6.1 Organización interna.** 6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. **6.2 Dispositivos para movilidad y teletrabajo.** 6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo. 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. **7.1 Antes de la contratación.** 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. **7.2 Durante la contratación.** 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario. **7.3 Cese o cambio de puesto de trabajo.** 7.3.1 Cese o cambio de puesto de trabajo. 8. GESTIÓN DE ACTIVOS. **8.1 Responsabilidad sobre los activos.** 8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. **8.2 Clasificación de la información.** 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. **8.3 Manejo de los soportes de almacenamiento.** 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 9. CONTROL DE ACCESOS. **9.1 Requisitos de negocio para el control de accesos.** 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. **9.2 Gestión de acceso de usuario.**	10. CIFRADO. **10.1 Controles criptográficos.** 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves. 11. SEGURIDAD FÍSICA Y AMBIENTAL. **11.1 Áreas seguras.** 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. **11.2 Seguridad de los equipos.** 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. 12. SEGURIDAD EN LA OPERATIVA. **12.1 Responsabilidades y procedimientos de operación.** 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. **12.2 Protección contra código malicioso.** 12.2.1 Controles contra el código malicioso. **12.3 Copias de seguridad.** 12.3.1 Copias de seguridad de la información. **12.4 Registro de actividad y supervisión.** 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. **12.5 Control del software en explotación.** 12.5.1 Instalación del software en sistemas en producción. **12.6 Gestión de la vulnerabilidad técnica.** 12.6.1 Gestión de las vulnerabilidades técnicas.	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. **14.1 Requisitos de seguridad de los sistemas de información.** 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes Públicas. 14.1.3 Protección de las transacciones por redes telemáticas. **14.2 Seguridad en los procesos de desarrollo y soporte.** 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.7 Externalización del desarrollo de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación. **14.3 Datos de prueba.** 14.3.1 Protección de los datos utilizados en pruebas. 15. RELACIONES CON SUMINISTRADORES. **15.1 Seguridad de la información en las relaciones con suministradores.** 15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. **15.2 Gestión de la prestación del servicio por suministradores.** 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. **16.1 Gestión de incidentes de seguridad de la información y mejoras.** 16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información.

9.2.1 Gestión de altas/bajas en el registro de usuarios. **9.2.2 Gestión de los derechos de acceso asignados a usuarios.** **9.2.3 Gestión de los derechos de acceso con privilegios especiales.** **9.2.4 Gestión de información confidencial de autenticación de usuarios.** **9.2.5 Revisión de los derechos de acceso de los usuarios.** **9.2.6 Retirada o adaptación de los derechos de acceso** **9.3 Responsabilidades del usuario.** **9.3.1 Uso de información confidencial para la autenticación.** **9.4 Control de acceso a sistemas y aplicaciones.** **9.4.1 Restricción del acceso a la información.** **9.4.2 Procedimientos seguros de inicio de sesión.** **9.4.3 Gestión de contraseñas de usuario.** **9.4.4 Uso de herramientas de administración de sistemas.** **9.4.5 Control de acceso al código fuente de los programas.**	**12.6.2 Restricciones en la instalación de software.** **12.7 Consideraciones de las auditorías de los sistemas de información.** **12.7.1 Controles de auditoría de los sistemas de información.** 13. SEGURIDAD EN LAS TELECOMUNICACIONES. **13.1 Gestión de la seguridad en las redes.** **13.1.1 Controles de red.** **13.1.2 Mecanismos de seguridad asociados a servicios en red.** **13.1.3 Segregación de redes.** **13.2 Intercambio de información con partes externas.** **13.2.1 Políticas y procedimientos de intercambio de información.** **13.2.2 Acuerdos de intercambio.** **13.2.3 Mensajería electrónica.** **13.2.4 Acuerdos de confidencialidad y secreto.** ISO27002.es PATROCINADO POR: 	**16.1.3 Notificación de puntos débiles de la seguridad.** **16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.** **16.1.5 Respuesta a los incidentes de seguridad.** **16.1.6 Aprendizaje de los incidentes de seguridad de la información.** **16.1.7 Recopilación de evidencias.** 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. **17.1 Continuidad de la seguridad de la información.** **17.1.1 Planificación de la continuidad de la seguridad de la información.** **17.1.2 Implantación de la continuidad de la seguridad de la información.** **17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.** **17.2 Redundancias.** **17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.** 18. CUMPLIMIENTO. **18.1 Cumplimiento de los requisitos legales y contractuales.** **18.1.1 Identificación de la legislación aplicable.** **18.1.2 Derechos de propiedad intelectual (DPI).** **18.1.3 Protección de los registros de la organización.** **18.1.4 Protección de datos y privacidad de la información personal.** **18.1.5 Regulación de los controles criptográficos.** **18.2 Revisiones de la seguridad de la información.** **18.2.1 Revisión independiente de la seguridad de la información.** **18.2.2 Cumplimiento de las políticas y normas de seguridad.** **18.2.3 Comprobación del cumplimiento.**

Fuente: http://iso27000.es/download/ControlesISO27002-2013.pdf

Anexo B. Lista de chequeo

Lista de chequeo basada en el estándar ISO/IEC 27002:2013 para verificar la existencia de controles de seguridad en ocho (8) de los catorce (14) dominios evaluados dentro de la empresa COOPSENA. Este procedimiento, está basado en la encuesta realizada a 7 (siete) empleados seleccionado de la Cooperativa, ellos son: Carlos Javier Garzón Lasprilla (Jefe de servicio al cliente), María Esnedy Arango González (Tesorera), Ingrid Gómez Suárez (Asistente de cartera), Aureliana Gutiérrez Chávez (Asistente de cobranzas), Juan Pablo Rodríguez Mojica (Auxiliar de archivos) y Angélica Godoy Gutiérrez (Promotora de servicios).

Tabla 43. Cuestionario 01

Lista de chequeo: Infraestructura tecnológica		COOPSENA		
Cuestionario de control		C.C.01		
DOMINIO	5. POLÍTICAS DE SEGURIDAD			
Objetivo de control	5.1 Directrices de la Dirección en seguridad de la información.			
Control	5.1.1 Conjunto de políticas para la seguridad de la información.			
Preguntas		Si	No	N/A
¿Usted conoce cuales son objetivos y la importancia de la seguridad informática?			x	
¿La Cooperativa si cumple con los requisitos legislativos, reglamentarios y de contratación para el manejo de la información?		x		
¿Conoce usted las consecuencias que acarrea la violación de las normas que conforman la política de seguridad informática?		x		
¿La cooperativa cuenta con un programa de formación y concienciación sobre seguridad informática?			x	
¿La entidad cuenta con un plan de contingencia en caso de presentarse fallas en el sistema informático?		x		
Control	5.1.2 Revisión de las políticas para la seguridad de la información.			

Preguntas	Si	No	N/A
¿La entidad cuenta con un plan de revisión de la política de seguridad, dada una determinada circunstancia o situación que cambie el enfoque de la misma?	x		
¿La entidad reporta los incidentes de seguridad presentados a las autoridades pertinentes?	x		
¿La entidad asigna los recursos necesarios para mejorar la gestión de la seguridad informática y sus procesos?	x		

Fuente: el autor Tabla 43. (Continuación)

Tabla 44. Cuestionario 02

Cuestionario de control		C.C.02		
DOMINIO	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.			
Objetivo de control	6.1 Organización interna.			
Control	6.1.1 Asignación de responsabilidades para la seguridad de la información.			
Preguntas		Si	No	N/A
¿Los activos informáticos y los procedimientos de seguridad asociados a los mismos se pueden identificar y están definidos de manera precisa?		x		
¿Se asignan las responsabilidades para el uso de cada activo, y estas se documentan?		x		
¿Los privilegios para el uso o acceso al sistema de información se encuentran documentados?		x		
Control	6.1.3 Contacto con las autoridades.			
Preguntas		Si	No	N/A
¿Existe un conducto regular documentado para notificar, aprobar o buscar apoyo ante acciones o situaciones de seguridad u otro servicio por parte de las autoridades pertinentes?		x		

Control	6.1.4 Contacto con grupos de interés especial.		
Preguntas	Si	No	N/A
¿Existen acciones para el mejoramiento de las prácticas y actualización de conocimientos en seguridad informática?		x	
¿La entidad cuenta con el apoyo de alguna organización especializada en seguridad de la información?	X		
¿En la entidad se tiene conocimiento sobre productos de nueva tecnología o sobre las amenazas, riesgos y vulnerabilidades de la actualidad?		x	

Fuente: el autor Tabla 44. (Continuación)

Tabla 45. Cuestionario 03

Cuestionario de control	C.C.03		
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		
Objetivo de control	7.2 Durante la contratación.		
Control	7.2.1 Responsabilidades de gestión.		
Preguntas	Si	No	N/A
¿Sabía usted cuáles eran sus funciones y sus responsabilidades respecto a la política de seguridad de la información antes de hacer uso de los recursos informáticos de la entidad?	x		
¿La entidad tiene normas establecidas para regular las funciones de los funcionarios con relación a la seguridad de la información?	x		
¿Está usted consciente sobre los lineamientos de seguridad de la información para el buen desempeño de sus funciones?	x		
¿Está usted de acuerdo con las normas, condiciones y métodos de trabajo que se rigen a través de la política de seguridad de la información?	x		
Control	7.2.2 Concienciación, educación y capacitación en seguridad de la información		

Preguntas	Si	No	N/A
¿La entidad forma y concientiza regularmente a sus contratistas y demás personas externas sobre seguridad de la información antes de tener autorización para realizar actividades dentro de la entidad?		x	
¿Tiene usted conocimiento sobre las amenazas que a diario impactan sistemas informáticos?		x	

Fuente: el autor Tabla 45. (Continuación)

Tabla 46. Cuestionario 04

Cuestionario de control		C.C.03		
DOMINIO	**8. GESTIÓN DE ACTIVOS.**			
Objetivo de control	8.1 Responsabilidad sobre los activos.			
Control	8.1.1 Inventario de activos.			
Preguntas		Si	No	N/A
¿La organización cuenta con un inventario que especifique y relacione los equipos informáticos existentes?		x		
¿Existe una planificación para realizar la revisión del inventario?		x		
¿Existe un procedimiento para la relación de inventarios a cuentadantes, como tomas físicas, fecha de asignación, etc.?			x	
¿El inventario de equipos informáticos se actualiza cada vez que se presenta alguno de los siguientes eventos (Retiro y Adquisición o reemplazo) y por lo menos una vez al año?		x		
¿La organización cuenta con alguna herramienta tecnológica para controlar y administrar el inventario de activos informáticos?		x		
Control	8.1.2 Propiedad de los activos.			
Preguntas		Si	No	N/A
¿La adquisición o disposición de activos informáticos es aprobada por la junta directiva?		x		

¿La adquisición de equipos informáticos se documenta previamente, mediante cotización y factura para luego realizar el registro en el sistema?	x		
¿Se identifican los equipos informáticos que son adquiridos por la organización mediante un sello, etiqueta o placa permanente para mantener su control de inventario?	x		
¿Existen registros que permitan verificar a tiempo y correctamente, la adquisición y disposición de los equipos tecnológicos?	x		
¿Se cuenta con el procedimiento y registros contables de depreciación de los equipos informáticos?	x		
¿Se verifica que las pérdidas o daños en la disposición de los equipos informáticos sean mínimas y se contabilizan debidamente?		x	
Control	8.1.3 Uso aceptable de los activos.		
Preguntas	Si	No	N/A
¿Existe una política que establezca la responsabilidad, el cumplimiento y el uso aceptable, racional y eficiente de los equipos informáticos que son asignados a los empleados?	x		
¿Existen documentos de responsabilidad firmadas por cada empleado respecto al uso adecuado y daños causados en los equipos informáticos?	x		
¿Existen acciones o medidas disciplinarias y/o legales relacionadas al mal uso de los dispositivos informáticos?	x		
¿La entidad cuenta con un plan de concienciación sobre buenas prácticas y uso aceptable de los dispositivos informáticos para el cumplimiento de sus funciones?		x	
¿Existe un código de conducta mediante el cual los empleados asumen su responsabilidad sobre el uso correcto y legal de los equipos informáticos y de toda la infraestructura tecnológica complementaria puesto a su disposición?		x	
Control	8.1.4 Devolución de activos.		

Tabla 46. (Continuación)

Preguntas	Si	No	N/A
¿Existe un procedimiento organizacional para la devolución de los equipos informáticos que ya no son utilizados por los empleados?	x		
¿Existe un conducto regular para la entrega, recepción y disposición final (donación, venta a empleados, venta a terceros, eliminación definitiva por daño o deterioro, perdida o hurto) de los equipos informáticos?	x		
¿Se cuenta con un funcionario profesional en TI, responsable de diagnosticar la viabilidad devolutiva de un equipo informático?		x	
¿Existe un procedimiento para la cuantificación del valor del activo informático y su remplazo inmediato en caso de diagnosticarse como inservible, obsoleto o perdido?			
¿Existe un funcionario profesional asignado para adelantar investigación administrativa, dado el caso, del hurto de un equipo informático?	x		
Objetivo de control	8.2 Clasificación de la información		
Control	8.2.1 Directrices de clasificación.		
Preguntas	Si	No	N/A
¿La información que utiliza la organización se clasifica de acuerdo a los requisitos legislativos, como el nivel de riesgo, valor, criticidad, sensibilidad, divulgación o modificación no autorizada?	x		
¿Todos los empleados de la organización conocen la clasificación de la información y los niveles de protección que se deben mantener para su respectivo aseguramiento?	x		
¿Cada funcionario conoce los controles que se utilizan para proteger la Información, sin importar el medio, formato o lugar donde se encuentre?	x		

Tabla 46. (Continuación)

¿Existe una política para el seguimiento y cumplimiento de la confidencialidad de la información que es entregada a los proveedores, asociados, contratistas y terceros para la gestión y efectos organizativos?		x		
¿Existe una metodología aprobada por el funcionario responsable de la seguridad del sistema informático para la destrucción de la información que ya no es utilizada en la organización?		x		
Control	8.2.2 Etiquetado y manipulado de la información.			
Preguntas		Si	No	N/A
¿El rotulado de la información se realiza de acuerdo a su clasificación?		x		
¿Existe un formato o tabla de retención documental para cada tipo o formato de documento?		x		
¿Se aplica alguna técnica de etiquetado como cintas adhesivas, marcas de agua, placas, etc. De acuerdo al formato y elemento de almacenamiento de la información?		x		
Control	8.2.3 Manipulación de activos.			
Preguntas		Si	No	N/A
¿Los equipos informáticos y demás recursos tecnológicos son asignados bajo responsabilidad a cada funcionario, por lo cual se compromete a manipular adecuada y eficientemente dicho recurso?		x		
¿Los movimientos de equipos informáticos son gestionados por cada departamento y controlados por la gerencia administrativa?		x		
¿Existe una metodología de control para el uso y manipulación de los equipos informáticos que son entregados a los funcionarios?		x		
¿Existen métodos de borrado remoto de la información contenida en elementos informáticos en caso de pérdida o hurto?		x		
¿El manejo de los equipos informáticos es controlado permanentemente y está debidamente sistematizado?			x	
Objetivo de control	8.3 Manejo de los soportes de almacenamiento			

Tabla 46. (Continuación)

Control	8.3.1 Gestión de soportes extraíbles			
Preguntas				
¿Los dispositivos de almacenamiento externo, tienen constantemente, habilitado el escaneo automático de virus?		x		
¿El antivirus institucional mantiene configurado el bloqueo de reproducción automática de archivos ejecutables?		x		
¿Existen lineamientos que permitan a los usuarios disponer de forma segura de los dispositivos de almacenamiento extraíble?		x		
Control	8.3.2 Eliminación de soportes			
Preguntas		Si	No	N/A
¿Para los procesos de eliminación de dispositivos de almacenamiento, se tienen en cuenta los niveles de seguridad de la información que estos almacenan?		x		
¿La organización cuenta con el procedimiento y las técnicas adecuadas de eliminación de la información de forma segura y la reutilización de los dispositivos que se utilizan para su almacenamiento?		x		
¿Las actividades de eliminación, limpieza o destrucción de los dispositivos de almacenamiento de la información son registradas en los inventarios de activos gestionados por cada área de la organización?		x		
Control	8.3.3 Soportes físicos en tránsito.			
Preguntas		Si	No	N/A
¿Se aplican técnicas como el encriptado, contraseñas o aplicativos utilizados para proteger los dispositivos que contienen información contra acceso no autorizado?		x		
¿Para el traslado de dispositivos o elementos que contienen información se gestionan documentos de autorizaciones, confidencialidad y responsabilidad?		x		

Fuente: el autor Tabla 46. (Continuación)

Tabla 47. Cuestionario 05

Cuestionario de control		C.C.05		
DOMINIO	9. CONTROL DE ACCESOS			
Objetivo de control	9.1 Requisitos de negocio para el control de accesos			
Control	9.1.1 Política de control de accesos			
Preguntas		Si	No	N/A
¿Existen políticas de controles de acceso a las TIC?		x		
¿Están definidas, asignadas y aceptadas las responsabilidades de acceso y usos de las TIC y los controles sobre las mismas?		x		
¿La organización cuenta con controles o registros de acceso en entradas y salidas de usuarios en las diferentes áreas y especialmente, en los centros de cómputo?		x		
¿Se aplican técnicas de identificación y autenticación como claves secretas de acceso, tarjetas magnéticas, huellas digitales, reconocimiento de voz o firmas digitales?			x	
¿Existen técnicas o procedimientos para asegurar lógica y físicamente los equipos y herramientas de la infraestructura de TI?		x		
¿Existen algún procedimiento de análisis de cuentas y contraseñas de usuarios para buscar periodos de inactividad u otro aspecto que permita redefinir necesidades de acceso al sistema?		x		
¿Existe algún procedimiento de mantenimiento y actualización de permisos de acceso al SI?		x		
¿La anulación de permisos de acceso a personal desvinculado de la empresa se realiza de manera inmediata?		x		
¿Los funcionarios o terceros que cuentan con un usuario en la plataforma TIC, conocen y cumplen la política de acceso, derechos y deberes con respecto al uso adecuado del SI?		x		

Tabla 47. (Continuación)

Control	9.1.2 Control de acceso a las redes y servicios asociados		
Preguntas	Si	No	N/A
¿La organización cuenta con normas y procedimientos específicos de control y autorización de acceso entre redes?	x		
¿Existen mecanismos para controlar, identificar y proteger las redes y servicios a los cuales se permite el acceso tanto interna como externamente?	x		
¿El sistema de seguridad informática contempla servicios de conexiones externas SSL, VPN y primarios para los usuarios que requieran conexión remota a la red institucional?		x	
¿Existen procedimientos documentados para la autenticación de servicios VPN para los usuarios con conexiones externas?		x	
¿Existen mecanismos de identificación de equipos conectados a la red institucional como controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI?	x		
¿El área de soporte de TIC cuenta con una política de control remoto de los equipos de los usuarios finales sin que estos los desatiendan?	x		
¿Existen mecanismos de seguridad como firewalls que permitan controlar el acceso entre las redes corporativas?	x		
¿Existe una política que establezca la capacidad de descarga de archivos para cada usuario?		x	
¿La organización cuenta con el estándar WPA2 o superior como medida de seguridad de las conexiones Wi-Fi?	x		
¿Existen controles para restringir el acceso a servicios de la red como mensajería instantánea, telefonía a través de internet, acceso a sitios recreativos, etc.?		x	
Objetivo de control	9.2 Gestión de acceso de usuario.		
Control	9.2.1 Gestión de altas/bajas en el registro de usuarios**.**		

Tabla 47. (Continuación)

Preguntas		Si	No	N/A
¿La organización cuenta con procedimientos claros para el registro y cancelación de usuarios?		x		
¿Los privilegios de acceso de los usuarios son controlados para evitar accesos o usos no autorizados de la información y de los sistemas que la soporta?		x		
¿Los privilegios de acceso de los usuarios, tanto internos como externos, son revisados contantemente y siempre que existen cambios en las funciones o tareas corporativas?		x		
Control	9.2.2 Gestión de los derechos de acceso asignados a usuarios			
Preguntas		Si	No	N/A
¿Existe una implementación de perfiles de usuario que garantice un acceso normal para todo tipo de usuarios y en todos los sistemas y servicios?		x		
¿Existe una metodología de revisión constante de los derechos de acceso de los usuarios externos e internos a la entidad?		x		
Control	9.2.3 Gestión de los derechos de acceso con privilegios especiales.			
Preguntas		Si	No	N/A
¿Existe una metodología para controlar, restringir o gestionar el acceso al sistema por parte de los usuarios con privilegios especiales?		x		
¿El uso de las claves de usuarios administrativos, tales como: “root”, “admin” y “system”, entre otros, son controladas y protegidas acorde con los lineamientos de la política de seguridad?		x		
Control	9.2.4 Gestión de información confidencial de autenticación de usuarios.			
Preguntas		Si	No	N/A
¿La información confidencial se controla a través de un proceso de seguridad y de acuerdo a la clasificación dada a los activos por parte de los usuarios?		x		

Tabla 47. (Continuación)

¿Todos los funcionarios cambiar su contraseña de acceso a los diferentes sistemas de información por lo menos cada tres meses?		x		
¿Existe un mecanismo de control que bloqueé a los usuarios, el acceso al sistema de información luego de 3 intentos fallidos de autenticación?		x		
Control	9.2.5 Revisión de los derechos de acceso de los usuarios.			
Preguntas		Si	No	N/A
¿Existe un método de revisión a los privilegios de acceso de los usuarios en un intervalo de tiempo?		x		
¿Cuándo hay una desviación de acceso, esta es tratada como un incidente en seguridad de la información?		x		
¿El responsable deja trazas del incidente realizado para ser revisado por depto. de seguridad de la organización?		x		
Control	9.2.6 Retirada o adaptación de los derechos de acceso			
Preguntas		Si	No	N/A
¿Existe una metodología para gestionar el retiro de los derechos de acceso de todo funcionario y/o contratistas del sistema de información e instalaciones informáticas en el momento de su retiro y/o terminación de contrato?		x		
Objetivo de control	9.3 Responsabilidades del usuario.			
Control	9.3.1 Uso de información confidencial para la autenticación.			
Preguntas		Si	No	N/A
¿Existe una política o documento de control que exija a los usuarios del sistema que cumplan con las prácticas sobre el buen uso de la información que es autenticada?		x		
Objetivo de control	9.4 Control de acceso a sistemas y aplicaciones.			

Tabla 47. (Continuación)

Control	9.4.1 Restricción del acceso a la información.			
Preguntas				
¿Existe una política para restringir el acceso a la información, a las funciones y aplicaciones del sistema informático?		x		
Control	9.4.2 Procedimientos seguros de inicio de sesión.			
Preguntas		Si	No	N/A
¿Existen mecanismos de seguridad para regular el acceso y/o conexión segura a las aplicaciones y sistemas de información?		x		
Control	9.4.3 Gestión de contraseñas de usuario			
Preguntas		Si	No	N/A
¿Los usuarios que adquieren cuentas y contraseñas de acceso al sistema son obligados a realizar el cambio de las mismas como medida de garantía, responsabilidad y único conocimiento sobre la misma?		x		
¿Existe una política que regule las características de las contraseñas como longitud mínima, uso de caracteres alfanuméricos, no utilización de nombres propios, no utilizar fechas de nacimiento o cualquier otra expresión de fácil identificación?		x		
¿Existe un mecanismo de control y un periodo de tiempo recomendable para realizar el cambio de contraseñas?		x		
¿Existe un mecanismo de control y una política para bloquear el acceso de un usuario al sistema después de cierto número (mínimo 3) intentos fallidos y solicitar el desbloqueo al dpto. de TI, respectivamente?		x		
¿La organización cuenta con una política para regular y gestionar el buen uso de las contraseñas las cuales son de carácter personal e intransferible?		x		
Control	9.4.4 Uso de herramientas de administración de sistemas.			

Tabla 47. (Continuación)

Preguntas		Si	No	N/A
¿La organización cuenta con mecanismos de control para restringir y bloquear el uso de aplicaciones privilegiadas como programas de utilidad que podrían ser capaces de anular o desconfigurar el sistema?		x		
Control	9.4.5 Control de acceso al código fuente de los programas			
Preguntas		Si	No	N/A
¿Existe una política y/o un mecanismo de control para limitar o bloquear el acceso al código fuente de los programas o aplicaciones legalmente licenciados?		x		

Fuente: el autor Tabla 47. (Continuación)

Tabla 48. Cuestionario 06

Cuestionario de control		C.C 06		
DOMINIO	10. CIFRADO.			
Objetivo de control	10.1 Controles criptográficos.			
Control	10.1.1 Política de uso de los controles criptográficos.			
Preguntas		Si	No	N/A
¿Conoce usted la política que regula el uso de las claves públicas?		x		
¿Sabe cuál es la función de una clave pública?		x		
¿Sabe usted cuales son los objetivos de una clave pública?		x		
¿La entidad cuenta con un plan de recuperación de la información cifrada en caso de daño o perdida de las claves públicas?		x		
Control	10.1.2 Gestión de claves.			
Preguntas		Si	No	N/A
¿La entidad cuenta con un programa de capacitación sobre como adquirir los certificados digitales de claves públicas?		x		
¿La entidad cuenta con un sistema de seguridad para el almacenamiento de claves públicas?		x		
¿Sabe usted cuando y como cambiar una clave pública?		x		

¿Sabe usted cual es el procedimiento en caso de pérdida de sus claves públicas?	x		

Fuente: el autor Tabla 48. (Continuación)

Tabla 49. Cuestionario 07

Cuestionario de control		C.C 07		
DOMINIO	13. SEGURIDAD EN LAS TELECOMUNICACIONES.			
Objetivo de control	13.1 Gestión de la seguridad en las redes.			
Control	13.1.1 Controles de red.			
Preguntas		Si	No	N/A
¿Existen controles destinados a proteger la información que es transmitida entre la intranet de la empresa - red pública y viceversa?		x		
¿La entidad cuenta con sistema de monitoreo para el registro de actividad log?		x		
¿El acceso al cuarto de equipos de sistemas y de redes es permitido solamente a personas autorizadas?		x		
¿La entidad cuenta con sistema biométrico de autenticación de ingreso al cuarto de sistemas y otras instalaciones de alto nivel de criticidad?			x	
Control	13.1.3 Segregación de redes.			
Preguntas		Si	No	N/A
¿El sistema de redes de la entidad está dividida en dominios lógicos tanto interno como externo?		x		
¿Cada dominio tiene sus propios controles de seguridad?		x		
¿El flujo de información entre los dominios configurados es controlado por el sistema de seguridad?		x		
¿Los grupos de usuarios de la entidad, utilizan redes privadas virtuales VPN?			x	

Objetivo de control	13.2 Intercambio de información con partes externas.			
Control	13.2.1 Políticas y procedimientos de intercambio de información.			
Preguntas		Si	No	N/A
¿El intercambio de información a través de la red es protegido y controlado por mecanismos de seguridad?		x		
¿La red cuenta con mecanismos de prevención y detección de intrusos?		x		
¿Existen controles y restricciones para el uso del correo electrónico y las llamadas telefónicas?		x		
¿Sabe usted que es la ingeniería social?			x	
Control	13.2.2 Acuerdos de intercambio.			
Preguntas				
¿Conoce usted la norma de control para el envío y recepción de datos?		x		
¿Los funcionarios saben cuál es su responsabilidad y el procedimiento a seguir en caso de cometer un incidente de seguridad?		x		
Control	13.2.3 Mensajería electrónica.			
Preguntas		Si	No	N/A
¿Existen procedimientos para evitar el re-encaminamiento de datos por parte de los usuarios del sistema?		x		
¿El servicio de mensajería esta siempre disponible?				
Control	13.2.4 Acuerdos de confidencialidad y secreto.			
Preguntas		Si	No	N/A
¿Existen compromisos documentados sobre el uso responsable y confidencial de los datos utilizados en las tareas de mensajería electrónica?		x		

Fuente: el autor Tabla 49. (Continuación)

Tabla 50. Cuestionario 08

Cuestionario de control		C.C 08		
DOMINIO	18. CUMPLIMIENTO.			
Objetivo de control	18.1 Cumplimiento de los requisitos legales y contractuales.			
Control	18.1.1 Identificación de la legislación aplicable.			
Preguntas		Si	No	N/A
¿Los controles y compromisos de confidencialidad individual para el uso de los recursos informáticos están completamente documentados?		x		
Control	18.1.2 Derechos de propiedad intelectual (DPI).			
¿La entidad da a conocer a sus funcionarios las normas de cumplimiento en el uso de la propiedad intelectual y legal del software y de otros elementos de tecnología?		x		
¿La entidad cuenta con proveedores autorizados para adquirir software u otros elementos tecnológicos?		x		
¿Existen acciones disciplinarias ante la violación de los derechos de propiedad intelectual en el uso del software u otras aplicaciones?		x		
Control	18.1.3 Protección de los registros de la organización.			
Preguntas		Si	No	N/A
¿Los funcionarios conocen la norma que establece los procedimientos de edición, almacenamiento, retención y eliminación de datos e información?		x		
¿Existe un inventario de relación de las fuentes de información crítica?		x		
¿Las fuentes de información cuentan con un sistema de seguridad?				
Control	18.1.4 Protección de datos y privacidad de la información personal.			
Preguntas		Si	No	N/A
¿La entidad cuenta con una política compuesta por procedimientos técnicos y organizaciones para la seguridad y privacidad de los datos?		x		
¿Los funcionarios conocen la política de seguridad y privacidad de los datos?		x		
Control	18.1.5 Regulación de los controles criptográficos.			

¿La entidad cuenta con una política debidamente implementada para el uso de los controles y claves de criptografía?		x		
¿Está restringido el uso de los recursos criptográficos?		x		
Objetivo de control	18.2 Revisiones de la seguridad de la información.			
Control	18.2.1 Revisión independiente de la seguridad de la información.			
Preguntas		Si	No	N/A
¿La gerencia evalúa las oportunidades de mejoramiento y requisitos de cambios en el sistema de seguridad, implicando la política y los objetivos de control?		x		
¿La revisión del sistema de seguridad de la información es realizada por personal especializado externo a la entidad?		x		
¿Los resultados de la revisión son documentados y reportados a la gerencia?		x		
¿Si el reporte indica que el sistema de seguridad de la información es inapropiado, la gerencia asume las correcciones respectivas?		x		
Control	18.2.2 Cumplimiento de las políticas y normas de seguridad.			
Preguntas		Si	No	N/A
¿Si se presentan violaciones a la política y normas de seguridad, la gerencia investiga sus causas?		x		
¿Se aplican las correcciones y sanciones de acuerdo a la política para evitar futuros incumplimientos?		x		
¿Se evalúan las correcciones realizadas?		x		
Control	18.2.3 Comprobación del cumplimiento.			
Preguntas		Si	No	N/A
¿La comprobación del cumplimiento de la política de seguridad de la información es realizada por personal especializado?		x		
¿La gerencia autoriza realizar pruebas de penetración durante la comprobación del cumplimiento?			x	

Fuente: el autor Tabla 50. (Continuación)

Anexo C. Resumen Analítico Especializado (RAE)

Título de Documento.	DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTA
Autor	RUIZ PEÑA Jose Higinio.
Palabras Claves	SGSI, Estándar, Arquetipo, Infraestructura tecnológica, Riesgo, Amenaza, Vulnerabilidad, Gestión de riesgos, Degradación, Impacto residual, Riesgo residual, salvaguarda, Declaración de aplicabilidad.
Descripción El trabajo investigativo presenta, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo a la norma ISO/IEC 27001:2013 como modelo estratégico de protección para la infraestructura tecnológica de la Cooperativa Multiactiva del Personal del SENA, COOPSENA, y cubre desde el estado actual de la seguridad del sistema informático de la entidad, nivel de concientización de los funcionarios, análisis y gestión de riesgos, identificación de salvaguardas a implantar, las fases de preparación que la entidad debe gestionar para una futura implementación del SGSI, y el plan de continuidad del negocio como estrategia de preparación y reacción apropiada ante un desastre.	
Fuentes Bibliográficas	El desarrollo del proyecto referencia 45 fuentes bibliográficas, algunas de las cuales hacen mayor énfasis en el análisis e implementación de sistemas de Gestión de Seguridad de la Información (SGSI), otras que son especializadas en el análisis y gestión de riesgos, otras que se enfocan en el estudio de los riesgos y amenazas más significativos de la actualidad, las que se especializan en la seguridad, desde el punto ético y legislativo, las que se enfocan en el plan de continuidad de negocios TIC; y por supuesto, las que aportan conocimientos solidos de cómo se debe llevar a cabo un trabajo investigativo. Todos estos documentos, la mayoría de ellos recuperados de internet, son el soporte y el aporte de personas mejores conocedoras del tema para llevar a buen término este trabajo investigativo, con el fin de acceder al título como Especialista en Seguridad Informática. Entre las fuentes más relevantes tenemos: MINISTERIO NACIONAL DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Informe final – modelo de seguridad de la información – sistema sansi - sgsi - modelo de seguridad de la información para la estrategia de

	gobierno en línea. {En línea}. Diciembre de 2008. {Consultado el 14 de octubre de 2016}. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf. CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL. Lineamientos de política para ciberseguridad y ciberdefensa. {En línea}. 14 de junio de 2011. {Consultado en septiembre de 2016}. Disponible en, http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION. Implantación de un SGSI en la empresa. {En línea}. {Consultado en octubre de 2016}. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/ Guia_apoyo_SGSI.pdf INSTITUTO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Magerit-versión 3.0, Metodología de análisis y gestión de riesgos de los sistemas de información. {En línea}. Octubre de 2012. {Consultado en noviembre de 2016}. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WABC-cmdDIU CONGRESO DE COLOMBIA. Ley 1273 de enero 05 de 2009. {En línea}. Enero 05 de 2009. {Consultado en noviembre de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf Del PINO JIMÉNEZ, Laura. Guía de desarrollo de un plan de continuidad de negocio. {En línea}. Julio de 2007. {Consultado en octubre de 2017}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001r.htm INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Octubre de 2010. {En línea}. {Consultado en octubre de 2017}.Disponible en:http://ceeielche.emprenemjunts.es/descargando/1871_descarga.pdf
CONTENIDO: Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la cooperativa multiactiva del personal del SENA,	

en Bogotá.

OBJETIVO GENERAL.

Proponer el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO/IEC 27001:2013 en COOPSENA, de tal manera que permita mejorar los niveles de seguridad de su sistema informático.

OBJETIVOS ESPECÍFICOS.

- Realizar el levantamiento de la información del estado actual del sistema informático corporativo, las metodologías de la gestión de riesgos, la legislación y normatividad, y los controles que conforman un SGSI.

- Definir la metodología a utilizar para la gestión de riesgos con el fin de identificar las vulnerabilidades y amenazas de seguridad que se presentan en los activos informáticos de la Cooperativa.

- Establecer los controles apropiados y proponer la implementación planificada.

- Contribuir con conocimientos y buenas prácticas al fortalecimiento de la seguridad de la información en los funcionarios de la organización

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

En este estudio investigativo, es notorio que los riesgos y las amenazas a los que constantemente están sometidos los sistemas informáticos, se han convertido en un problema potencial para el cumplimiento de los objetivos organizacionales.

Por tanto, para gestionar entornos organizativos más viables y seguros, las empresas deben asegurar la información que es el activo más importante para llevar a cabo los diferentes procesos comerciales, productivos, económicos y sociales, mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

A lo largo del contenido del documento, se detallan los beneficios y las ventajas que una organización obtiene cuando implementa este tipo de sistema y la forma como se debe hacer. Allí se define, que un Sistema de Gestión de Seguridad de la Información, es una moderna metodología que permite analizar, conocer, gestionar, reducir o eliminar los riesgos probables que pueden impactar y degradar los activos informáticos de una empresa, y dar cumplimiento a las normas legislativas.

Por ello, se deben gestionar ordenadamente, las fases o procesos que conforman un SGSI, como p.e, el de la ISO 27001:2013 cuyo modelo se basa en el ciclo de Deming, PDCA (Plan-Do-Check-Act) o Planificar, Hacer, verificar y Actuar. Para el desarrollo de este proyecto se tomó como referencia la etapa Planificar, pues su implementación de la cual hacen parte las otras tres etapas, se ha dejado a criterio de los dirigentes de la entidad sobre la cual se realizó este estudio investigativo.

La etapa en mención, es importante no solo por ser la primera, sino porque además permite;

Primero: analizar y ordenar adecuadamente, los diferentes activos que conforman la infraestructura tecnológica de la organización.

Segundo: realizar el análisis y gestión de riesgos

Tercero: seleccionar los controles que se deben implementar en la organización.

Cuarto: crear las normas o políticas de seguridad

La implementación de un SGSI, va a conformar un velador potente para la organización frente a los continuos riesgos y amenazas que pueden impactar negativamente, la competitividad, viabilidad y continuidad de una empresa en el mercado.

Para el análisis y tratamiento de riesgos, la ISO 27001 recomienda definir una metodología especializada para gestionar este proceso, el cual permite garantizar la confidencialidad, integridad, disponibilidad y el no repudio de la información.

Existen varias metodologías para llevar a cabo un proceso gestión de riesgos, y aunque todas persiguen el mismo objetivo, se diferencian en la forma como presentan los resultados, algunas se caracterizan por la sencillez para llevar a cabo el proceso mientras que otras son complicadas y unas son más costosas que otras, por lo tanto, es importante conocer sus estructuras, características, ventajas y desventajas para escoger la que más se adapte a las necesidades de la organización.

Para el caso de este proyecto, la metodología elegida fue MAGERIT, por su flexibilidad y la forma como describe los pasos que se deben seguir para gestionar los riesgos, detalla una a una las tareas que se deben ejecutar de tal manera que el proceso este siempre bajo control, teniendo en cuenta aspectos prácticos para que la gestión de los riesgos sea realmente efectiva como es el caso de las valoraciones cualitativas y cuantitativas de activos informáticos y de los riesgos en sí. Además, es una metodología de carácter público, no requiere autorización para utilizarla y

tiene un alto porcentaje de buenas referencias en su aplicación, y por demás, se adapta muy bien a los lineamientos y requerimientos del estándar ISO 27001.

METODOLOGÍA DE DESARROLLO

Para este proyecto investigativo se utilizan metodologías relacionadas al método científico como la de enfoque mixto, debido a la recolección de datos cuantitativos y cualitativos, de enfoque descriptivo y explicativo, así como las técnicas utilizadas para la investigación de campo y documental que conllevaron a las decisiones, fases y actividades para la consecución de los resultados esperados como lo son:

- Modelo del SGSI bajo la norma ISO/IEC 27001:2013.
- Alcance del Sistema de Gestión de Seguridad de la Información
- Políticas de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Tabla de inventario de activos
- Matriz de valoración de activos
- Tabla de identificación y valoración de amenazas
- Matriz de análisis de riesgos
- Lista de chequeo
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos, entre otros.

Conclusiones

- Prácticamente, todas las empresas, independientemente de su tamaño, actividad económica y función social, dependen más cada día de las tecnologías de la información y las comunicaciones (TIC), y de los diferentes servicios que brinda el escalable conjunto de redes interconectadas , recursos que representan un alto beneficio para las diferentes objetivos de negocio; pero también, están expuestas a un gran número de riesgos y amenazas que deben gestionarse con procedimientos, mecanismos y políticas de seguridad para fortalecer la confianza de los usuarios y la protección de los diferentes sistemas de información. Por eso, se han creado diferentes Sistemas de Gestión de Seguridad de la Información (SGSI) cuyo propósito es garantizar la confianza de los sistemas informáticos y mejorar los niveles de competencia, fiabilidad de clientes y prestigio en el mercado.

- El análisis y gestión de riesgos, es el proceso más importante sobre el que se apoya un sistema de gestión de seguridad de la información (SGSI), pues sus procedimientos permiten detectar, controlar, eliminar, asumir, trasferir o mitigar los riesgos; por eso, una organización debe valerse de una

metodología que facilite la toma de decisiones y una mejor orientación sobre las medidas de control que se deben implantar para salvaguardar los activos informáticos, y en especial, la información que es utilizada para sus objetivos de negocio.

Anexo D. Carta de aceptación de COOPSENA para el desarrollo del proyecto

COOPSENA
Cooperativa Multiactiva del Personal del Sena
NIT 860.014.871-1

GER – 0021

Bogotá D.C., Marzo 22 de 2017

Señor
JOSE HIGINIO RUIZ PEÑA
Ciudad

Respetado señor Ruíz:

En respuesta a su solicitud para llevar a cabo el desarrollo del proyecto de investigación titulada: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI), BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA "COOPSENA", en ésta ciudad; nos permitimos manifestarle nuestro interés y estamos dispuestos a participar en el proceso, ofreciendo la información y el apoyo necesario para el complimiento de las actividades correspondientes al desarrollo de dicho proyecto.

Cualquier inquietud con mucho gusto será atendida.

Cordial saludo,

EDGAR EDWIN POLANCO BOTELLO
Representante Legal

Vigilada por la Superintendencia de la Economía Solidaria - Intendencia para el Sector Real

Calle 57 No. 24-11 • PBX 805 16 60 • www.coopsena.com.co • E-mail: gerencia@coopsena.com.co • Bogotá D.C.