DISEÑO DE UN MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO MEDIANTE LA NORMA ISO/IEC 27001:2013

MERCEDES SARRIA CUÉLLAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2015

DISEÑO DE UN MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO MEDIANTE LA NORMA ISO/IEC 27001:2013

MERCEDES SARRIA CUÉLLAR

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2015

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 31 de mayo de 2015

DEDICATORIA

A ti Padre Amado, tú quien nos da la oportunidad, de vivir pero también de crecer en el ámbito profesional y laboral; quien nos da sabiduría y nos guía hasta lograr cada una de las victorias en nuestras vidas y en cada de nuestras familias. A nuestros asesores por su disposición e incondicional apoyo para que lográramos este nuevo peldaño profesional.

Mercedes

AGRADECIMIENTOS

La autora expresa sus agradecimientos:

A Dios, por haberme regalado el más hermoso de los detalles la vida y una familia por quien luchar.

A mi familia, por darme la fortaleza y la valentía para seguir adelante.

A mis Asesores dela Monografía, por su integralidad en el proceso educativo y su permanente asesoría para la culminación de esta investigación.

A la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, por haberme prestado ayuda y orientación para la ejecución de la monografía. Y a todas aquellas personas que de una u otra forma colaboraron en la realización del presente trabajo.

CONTENIDO

Pág.

RESUMEN 14

INTRODUCCIÓN 15

1 PLANTEAMIENTO DEL PROBLEMA 16

1.1 FORMULACIÓN DEL PROBLEMA 17

2 JUSTIFICACIÓN 18

3 OBJETIVOS 19

3.1 OBJETIVO GENERAL 19

3.2 OBJETIVOS ESPECÍFICOS 19

4 MARCO REFERENCIA 20

4.1 ANTECEDENTES DE LA INVESTIGACIÓN 20

4.2 MARCO TEÓRICO 21

4.2.1 Iso 21

4.2.2 Norma ISO 27001 22

4.2.3 La Información 22

4.2.4 Seguridad Informática 22

4.2.5 Propósito de un sistema de gestión de la seguridad de la información. 23

4.2.6 Sistema de gestión de seguridad de la información. 23

4.2.7 Pilares de la seguridad informática. 24

4.2.8 Servicios de seguridad informática..... 25
4.2.9 Tipos de ataques internos o externos. 26
4.2.10 Buenas prácticas en seguridad informática..... 27
4.2.11 Identificación, clasificación y valoración de activos de información..... 28
4.2.12 Copias de seguridad. 29
4.2.13 Análisis del riesgo. 30
4.2.14 Gestión de riesgo. 31

4.3 MARCO LEGAL..... 32
4.3.1 Ley 1273 del 5 de enero de 2009 de delitos informáticos. 32
4.3.2 Ley estatutaria 1581 de 2012 Disposiciones Generales para la Protección de Datos Personales. 34

4.4 MARCO CONTEXTUAL 36
4.4.1 Marco institucional..... 36
4.4.2 Misión. 37
4.4.3 Visión. 38
4.4.4 Sedes de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.. 40
4.4.5 Sección servicios de consulta médica externa. 42
4.4.6 Sección de servicios de apoyo diagnóstico. 43
4.4.7 Sección de hospitalización, atención de urgencias y sala de parto..... 43
4.4.8 Sección de promoción de la salud prevención de la enfermedad. 44
4.4.9 Sección de telemedicina. 45
4.4.10 Sección de transporte. 46
4.4.11 Sección otros servicios..... 46
4.4.12 Organigrama de la Empresa Social del Estado Fabio Jaramillo Londoño. . 46
4.4.13 Estructura de la Red de la Empresa..... 47

4.4.14 Responsabilidades del personal de la Empresa Social del Estado Fabio Jaramillo Londoño. 50

5 METODOLOGÍA 51

5.1 EL CICLO PHVA (METODO GERENCIAL) 52

5.1.1 Planear. 53

5.1.2 Hacer 53

5.1.3 Verificar. 53

5.1.4 Actuar. 53

6 DESARROLLO DEL PROYECTO 54

6.1 ENCUESTA REALIZADA AL PERSONAL DE LA EMPRESA SOBRE LA SEGURIDAD DE LA INFORMACIÓN 54

6.1.1 Resultado de la Encuesta de Seguridad de la Información. 54

7 ANALISIS Y EVALUACION DEL RIESGO 64

7.1 DESCRIPCIÓN DE LOS ACTIVOS 64

7.2 INVENTARIO DE LOS ACTIVOS DE INFORMACIÓN 65

7.3 DIMENSIONES DE VALORACIÓN 66

7.4 IMPACTOS EN LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA DEL ESTADO FABIO JARAMILLO LONDOÑO 67

7.5 ANALISIS DE AMENAZAS POR ACTIVOS 68

7.5.1 Estimación del Impacto 71

7.5.2 Resumen del Análisis del Riesgos del Estado Actual de los Activos de Información de la Empresa Social del Estado Fabio Jaramillo Londoño. 72

8 DISEÑO DE UN MODELO GENERAL DE SEGURIDAD DE LA INFORMACIÓN SGSI 73

8.1 ANÁLISIS DETALLADO DEL ANEXO A ISO 27001:2013..... 74

9 DISEÑO DEL PLAN DE IMPLEMENTACIÓN DEL SGSI 113

9.1 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN..... 113

9.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN..... 116

9.3 SEGURIDAD DE LOS RECURSOS HUMANOS..... 120

9.4 GESTIÓN DE ACTVIOS..... 121

9.5 CONTROL DE ACCESO 122

9.6 CRIPTOGRAFÍA..... 128

9.7 SEGURIDAD FISICA Y DEL ENTORNO..... 129

9.8 SEGURIDAD DE LAS OPERACIONES..... 130

9.9 SEGURIDAD DE LAS COMUNICACIONES..... 132

9.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTMAS..... 133

9.11 RELACIONES CON LOS PROVEEDORES..... 135

9.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN .. 135

9.13 ASPECTOS DE SGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO 136

9.14 CUMPLIMIENTO 137

10 PLAN DE CONTINGENCIA INFORMATICO PARA LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO EN EL ÁREA DE SISTEMAS..... 139

11 CONCLUSIONES 161

RECOMENDACIONES 163

BIBLIOGRAFIA 164

LISTA DE FIGURAS

Pág.

Figura 1. Principio seguridad informática 23
Figura 2. Tipos ataques 27
Figura 3. Nuestra historia 37
Figura 4. Logo Empresa Social del Estado Fabio Jaramillo Londoño 38
Figura 5. Valores de la Empresa Social del Estado Fabio Jaramillo Londoño 39
Figura 6. Organigrama 47
Figura 7. Estructura de la red de la entidad 48
Figura 8. Actividad ciclo PHVA 52

LISTA DE TABLAS

Pág.

Tabla 1. Inventario de los activos de la información 65
Tabla 2. Escala porcentual de impactos 67
Tabla 3. Probabilidad de frecuencia (FREQ) 68
Tabla 4. Análisis de amenazas por activos 69
Tabla 5. Valores estimado de Impacto 71
Tabla 6. Resumen del Análisis de Riesgo 72
Tabla 7. Análisis detallado del Anexo A ISO 27001:2013 74

LISTA DE ANEXOS

Pág.

Anexo 1. Muestra Pregunta 1, de la encuesta de seguridad de la información. ...55

Anexo 2. Muestra Pregunta 2, de la encuesta de seguridad de la información 55

Anexo 3. Muestra Pregunta 3, de la encuesta de seguridad de la información 56

Anexo 4. Muestra Pregunta 4, de la encuesta de seguridad de la información. ...57

Anexo 5. Muestra Pregunta 5, de la encuesta de seguridad de la información. ...57

Anexo 6. Muestra Pregunta 6, de la encuesta de seguridad de la información. ...58

Anexo 7. Muestra Pregunta 7, de la encuesta de seguridad de la información 58

Anexo 8. Muestra Pregunta 8, de la encuesta de seguridad de la información 59

Anexo 9. Muestra Pregunta 9, de la encuesta de seguridad de la información 60

Anexo 10. Muestra Pregunta 10, de la encuesta de seguridad de la información 60

Anexo 11. Muestra Pregunta 11, de la encuesta de seguridad de la información 61

Anexo 12. Muestra Pregunta 12, de la encuesta de seguridad de la información 62

Anexo 13.Muestra Pregunta 13, de la encuesta de seguridad de la información .62

Anexo 14. Encuesta realizada al personal de la empresa sobre la Seguridad de la Información. 166

Anexo 15. Registró Fotográfico de visita 168

Anexo 16. Políticas de Seguridad de Uso Aceptable de los Recursos Informáticos 169

Anexo 17. Modelo plan maestro para la implementación de un sistema de gestión de seguridad de la información (SGSI) 173

RESUMEN

La presente investigación de esta monografía, se propone un diseño de un modelo de un sistema de gestión de seguridad de la información, el diseño del modelo se elaborará mediante la norma ISO/IEC 27001:2013, la cual implementa controles para el desarrollo de los pilares de seguridad de la información y los activos de información, se recomiendan mejoras y nuevas medidas de seguridad sobre los activos, los procesos y los sistemas que brindan servicios en la Empresa Social del Estado Fabio Jaramillo Londoño.

Igualmente, el diseño de un modelo de un sistema de gestión de seguridad de la información, proporciona las herramientas para que el área administrativa tome las decisiones y medidas pertinentes sobre la normatividad y la buena administración y tecnológicos en los recursos administrativos de la empresa, posibilitando mejores tiempos de respuestas, mitigando las amenazas existentes, se podrá valorar el estado de activo que es afectado sobre las dimensiones de seguridad de la metodología Magerit como la Disponibilidad, Integridad de los datos, Confidencialidad de la información, Autenticidad y Trazabilidad.

Palabras claves

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, DISEÑO, MODELO, ISO 27001: 2013, NORMAS, CONTROLES, PILARES, ACTIVOS DE INFORMACIÓN, SISTEMAS DE INFORMACIÓN, DISPONIBILIDAD, INTEGRIDAD DE LOS DATOS, CONFIDENCIALIDAD DE LA INFORMACIÓN, AUTENTICIDAD Y TRAZABILIDAD, VULNERABILIDADES, RIESGOS Y AMENAZAS.

INTRODUCCIÓN

Cuando hablamos de Informática nos referimos a todos los recursos que están relacionados con el manejo de la información y como esta llega a representar el motor en la era digital en la que nos estamos moviendo.

Las empresas hoy en día tienen que adaptar en todos sus procesos organizacionales y en sus estrategias de negocios directrices de seguridad de la información, debido a que los recursos informáticos están expuestos a sufrir diferentes daños los cuales pueden provenir tanto del interior como del exterior de la organización. Por ejemplo: Robo información, destrucción, uso no autorizado, acceso abusivo a los sistemas informáticos, ataque de denegación de servicio, entre muchos otros que pueden llegar a afectar la imagen y la operación normal de cualquier organización.

En el desarrollo de este proyecto se analizará el estado actual de los sistemas de información para determinar los riesgos a los cual se encuentran expuestos, se diseñaran los lineamientos de procedimientos para la implantación de un sistemas de gestión de seguridad de la información bajo la norma ISO 27001:2013, con el objetivo de que de alguna manera se realicen actividades de prevención, detección y corrección de cualquier problema con los recursos informáticos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, del Departamento del Caquetá.

Este diseño será entregado para uso de la empresa en mención, con el fin de fortalecer el buen manejo y seguridad de la información. Por lo tanto es una investigación de gran importancia para la misma.

1 PLANTEAMIENTO DEL PROBLEMA

La Empresa Social del Estado FABIO JARAMILLO LONDOÑO, es una empresa Social del Estado y constituye una categoría especial de entidad pública descentralizada del orden departamental, con personería jurídica, patrimonio propio y autonomía administrativa. Se ubica en la zona centro del departamento del Caquetá y presta los servicios de salud del primer nivel de complejidad, tienen una jurisdicción en los municipios de: Valparaíso, Solita, Milán y Solano. Municipios a orillas de los ríos Orteguaza y Caquetá, con sede Administrativa en el municipio de Florencia.

El problema de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, radica en la poca existencia de la infraestructura en el área de sistemas que brinde un soporte tecnológico que cumpla con los estándares y la normatividad vigente, aunque no existe un área de sistemas bien consolidada, ya que se trabaja de manera aislada, y los servicios y recursos como el internet, los recursos de computo los servidores y demás infraestructura tecnológica son en su mayoría un poco obsoletos y poco eficientes. No existen políticas sobre el manejo de equipos y software, no tiene un control adecuado en las directivas de usuarios donde se defina lo que los usuarios pueden y deben hacer para usar su red y equipos informáticos de la organización. Igualmente, no tiene definida las limitaciones a los usuarios para mantener la red segura de la empresa, como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que puede utilizar y cómo pueden acceder a los datos.

En el área de sistemas encontramos a nivel de infraestructura tecnológica, tecnologías y topologías de red construidas y que si bien cumplen con los estándares tecnológicos y de infraestructura de instalación y adecuación; no cumple con el aspecto de seguridad informática que nos atiende. En algunos casos estos equipos de red y relacionados, no cuentan con el suficiente nivel de administración, nivel de procedimiento y capacidad de expansión futura que requiere la Empresa Social del Estado FABIO JARAMILLO LONDOÑO dado que se encuentran dispositivos destinados a otro tipo de ambientes como lo es el hogar y no una red de computadores de nivel robusto. Actualmente los equipos no cuentan con contraseñas que restrinjan el acceso a nivel de cómputo a las máquinas y a la información y procedimientos que realizan.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede mitigar los riesgos para la protección de los sistemas y activos de información de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO?

2 JUSTIFICACIÓN

El diseño e implementación de este proyecto puede ofrecer grandes beneficios, a la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, para asegurar el manejo de la información permitiendo la autenticidad de los procesos llevados a cabo en la empresa, lo cual generará confianza en el manejo de la información y evitar riesgos que ponen en peligro la integridad de la información y el buen funcionamiento de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO de una manera adecuada.

Para cumplir con lo anterior, la organización debe establecer procedimientos adecuados e implementar controles de seguridad basados en la evaluación de los riesgos y la medición de su eficacia. Los riesgos provienen no solo desde el exterior de la red que conforma la organización, sino también desde el interior de la misma. Para poder trabajar en un entorno como este, de forma segura, las empresas pueden asegurar sus datos e información de valor con la ayuda de un SGSI (Sistema de Gestión de Seguridad de la Información).

Este proyecto también surge en respuesta a la Ley 872 de 2003, la cual establece que todas las entidades del estado deben adoptar el Sistema de Gestión de la Calidad, la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, en consecuencia al cumplimiento de su función constitucional, ha programado realizar un proceso metodológico con el fin de proponer un Sistema de Gestión de Seguridad Informática, ya que como investigadora no es factible implementar una solución macro a la red de hospitales de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, sino la de proporcionar las herramientas para que el área administrativa tome las decisiones y medias pertinentes sobre la normatividad y la buena administración de los recursos administrativos y tecnológicos de la empresa, posibilitando mejores tiempos de respuesta y acción a los procesos y procedimientos realizados por la misma.

La razón académica que abriga esta investigación es la de aplicar los conocimientos adquiridos durante el proceso de especialización de seguridad informática; así mismo la razón social de este pretende dar un nueva visión a la forma en la que se están realizando los procesos tecnológicos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un modelo de un sistema de gestión de seguridad la información para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO bajo la norma ISO/IEC 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Recolectar información de las sedes que pertenecen a la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.
- Realizar encuestas al personal sobre los niveles de riesgo de los sistemas de información a su cargo.
- Describir el estado actual en el que se encuentran los sistemas de información de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.
- Proponer un diseño de un modelo general de procedimientos de seguridad de la información (SGSI).
- Establecer un plan de contingencia para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, en el área de sistemas.

4 MARCO REFERENCIA

4.1 ANTECEDENTES DE LA INVESTIGACIÓN

La Empresa Social del Estado Fabio Jaramillo Londoño ha ejercido sus funciones empleando herramientas de la informática donde la información que generaba administrativamente todos los procesos financieros, los cuales se elaboraban impresos y en medio magnéticos y teniendo en cuenta el avance día a día de la tecnología se crea la necesidad en el área de sistemas en la implementación de Sistema de Gestión Seguridad de Información, basándose en la norma ISO 27000, en sus estándares 27001 y enfocándose a las necesidades directas de la misma empresa, es un aporte que permite indagar y adentrarse en el manejo y la aplicabilidad de la norma ISO 27001, como base del diseño del modelo de un Sistema de Gestión de Seguridad de la Información, con todas sus recomendaciones y buenas practicas, para obtener a través de los análisis, el más adecuado resultado con la información de los riesgos encontrados y los controles que se puedan utilizar a estos.

Como resultados de la investigación de la implantación de un Sistema de Gestión Seguridad de Información por parte de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO vamos a obtener los siguientes beneficios.

En primer lugar, se obtendrá una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible o aceptable para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO. De este modo, si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada.

En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización.

En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

Por último, pero no por ello menos importante, la certificación del Sistema de Gestión de Seguridad de la Información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndolas más fiables e incrementando su prestigio.

Después de haber tomado las nociones iniciales y conocimientos básicos sobre los SGSI, procederemos a describir en el diseño del trabajo de los procesos y la posible adopción por parte de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, aunque no es un diseño de un modelo completo y exhaustiva si pretende dar a la dirección y administración las herramientas necesarias para la toma de decisiones en el ámbito de la seguridad informática.

4.2 MARCO TEÓRICO

4.2.1 Iso. (Internacional Organización for Standardization) Organización Internacional para la Estandarización, es una organismo que promueve el desarrollo de normas voluntarias internaciones de fabricación, comercio y comunicación para las ramas industriales. Ha definido el estándar ISO/27001 para la gestión de la seguridad de la información[1].

[1] COLLAZOS BALAGUER, Manuel “Colegio de Ingenieros del Peru” En línea 1962

4.2.2 Norma ISO 27001. Es la norma principal de la serie y se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad.

4.2.3 La Información. Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el cual puede equivocarse o no, o hacer el bien o el mal. La información tiene estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno**.**

4.2.4 Seguridad Informática. Es la que permite lograr que todos los sistemas informáticos utilizados en cualquier contexto, se encuentren seguro de cualquier daño o riesgos, ya sea por parte de personas ajenas que en forma voluntaria o involuntaria lo pueda hacer o de cualquier desastre natural. En este sentido, la protección de la información requiere de un conjunto de software o aplicativos diseñados, documentos estándares y metodologías existentes que permitan aplicar las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad. Se expresa control en la seguridad, porque se considera un tanto difícil garantizar la seguridad de la información en forma completa o llevada a un 100%, por cuanto intervienen diferentes amenazas a las que las organizaciones y/o personas se encuentran continuamente expuestas.

Figura 1. Principio seguridad informática

Fuente: Autor

4.2.5 Propósito de un sistema de gestión de la seguridad de la información. Es por tanto, garantizar 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.

4.2.6 Sistema de gestión de seguridad de la información. Es una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

Entre los muchos ejemplos de información que podemos encontrar en la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, están los correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos y un largo etcétera.

4.2.7 Pilares de la seguridad informática.

Son los que persigue proteger en gran escala la:

- **Confidencialidad**. La información sólo puede ser accedida y utilizada por el personal de la empresa que tiene la autorización para hacerlo. En este sentido se considera que este tipo de información no puede ser revelada a terceros, ni puede ser pública, por lo tanto debe ser protegida y es la que tiende a ser más amenazada por su característica.[2]

- **Integridad.** Se refiere al momento en que la información no ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino. Un ataque a la integridad de la información se puede presentar en archivos planos de bases de datos, información documental, registros de datos, etc.

- **Disponibilidad.** Se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para el procesamiento de la información, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean interrumpidos.

- **Autenticidad.** Este pilar se define aquella información legítima, que al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica.[3]

---

[2] SUAREZ SIERRA, Lorena Patricia, AMAYA TARAZONA, Carlos Alberto "Sistema de Gestión de la Seguridad de la información SGSI" En línea. Julio 2013. Recuperada 11-05-2015. Disponible: http://es.scribd.com/doc/202912531/Modulo-SGSI-233003-Listo#scribd

[3] SUAREZ SIERRA, Lorena Patricia "Sistema de Gestión de la Seguridad de la información SGSI" En línea. Julio 2013. Recuperada 11-05-2015. Disponible: http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

4.2.8 Servicios de seguridad informática.

- **Autenticación.** Este servicio es de mucha importancia ya que es necesario lograr que la información está siendo utilizada por la persona correcta, un ejemplo claro que se ve en las instituciones del estado del manejo de la información financiera por medio del certicamara “firma digital” de igual manera los bancos en la actualidad le brindan la facilidad a sus clientes de acceder a la firma digital para realizar transacciones seguras.

- **Disponibilidad**: la información debe encontrarse disponible en el momento que se necesite pero a su vez debe estar asegurada con el fin de que su integridad no sea violada**.**

- **Integridad.** La información debe de ser correcta y completa, además de esto únicamente debe ser modificada por la persona autorizada y de manera vigilada.

- **No repudio**. Cuando la información involucrada en un evento corresponde a quien par cipa, quien no podrá evadir su intervención en éste. Ejemplo: n emisor de un mensaje no puede negar que lo generó y viceversa, un receptor de un mensaje no puede negar que lo recibió.

- **Confidencialidad.** Cuando la información es solo accesible por aquellos a los cuales se ha autorizado a tener acceso. Un ejemplo de control para garantizar la confidencialidad son los mecanismos de encripción**.**

- **Vinculación.** Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado.

- **Cifrado.** Consiste en una transformación carácter por carácter o bit por bit, según el caso, sin importar la estructura lingüística ni el significado del mensaje.

- **Código.** Estaban definidos de tal forma que permitían cierto grado de detección y corrección de errores. Por este motivo se suele considerar a este código como el precursor de este tipo de prácticas. Podríamos considerar que traducir un documento a otro idioma es usar un código, el mensaje será comprensible sólo para los receptores que conozcan dicho código.

- **Estrategia.** A la hora de diseñar la estrategia actual y futura de la organización hay que tener en cuenta el potencial de las Seguridad

Informática. Los planes estratégicos de las TI deben recoger y satisfacer las necesidades estratégicas de negocio de la organización**.**

- **Responsabilidad.** Deben establecerse las responsabilidades de cada individuo o grupo de personas dentro de la organización las en relación con la Seguridad Informática. Cada uno debe aceptar y ejercer su responsabilidad y aquellos a los que se le asigne una responsabilidad deberá tener dicha responsabilidad.

4.2.9 Tipos de ataques internos o externos.

- **Ataque SYN.** Este tipo busca explotar una debilidad en el protocolo TCP/ IP. Cuando se establece una conexión a través de TCP / IP, se trata de un mecanismo de toma de contacto, que consiste en el intercambio de mensajes.

- **Ataque Smurf.** Esta es una forma de paralizar una red desde el interior. El mecanismo de un ataque Smurf es más sofisticado y la parte crítica es descubrir un servidor de emisión. Cuando un hacker conoce los servidores de difusión en una red, él o ella envían una solicitud de ping. La dirección IP de origen en la solicitud de ping es falso y parece como si el ping viene de dentro de la red.

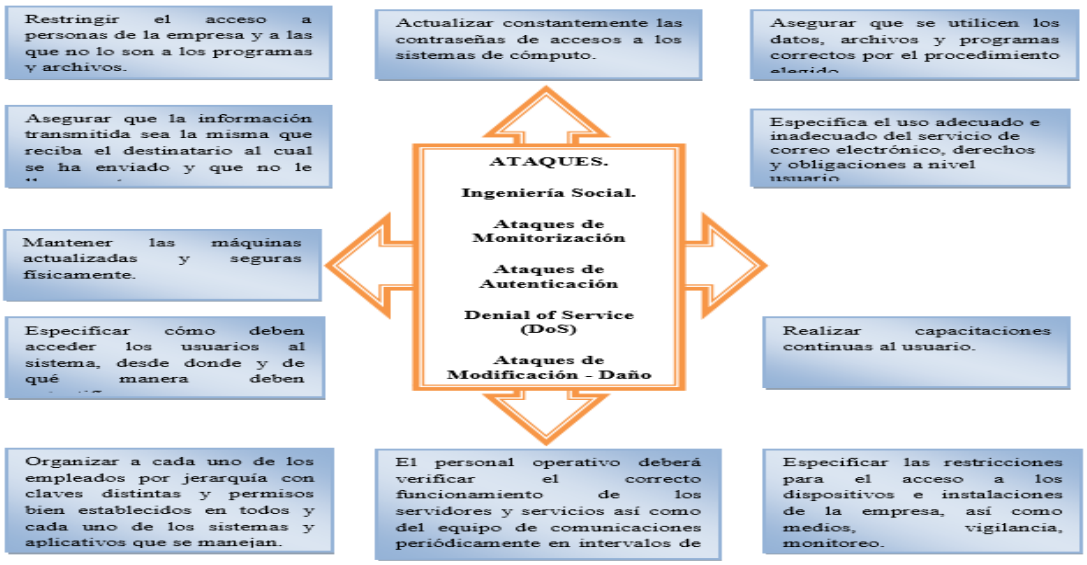
- **Ataque Teardrop.** Este implica el envío de paquetes IP dañados, cuyo objetivo es confundir y potencialmente bloquear el sistema de recepción. Al igual que el ataque Ping de la muerte, los ataques teardrop**.**

- **Ataque de inundación.** Este es la primera forma conocida de un ataque DoS. El mecanismo de un ataque de inundación es simple - los atacantes envían más tráfico a un servidor del que puede manejar. Si el ancho de banda de la víctima es bueno, un ataque de inundación tiene una oportunidad de tener éxito sólo si se trata de un ataque DDoS.

- **Ataque por fuerza bruta.** No es necesariamente un procedimiento que se deba realizar por procesos informáticos, aunque este sistema ahorraría tiempos, energía y esfuerzos. El sistema de ataque por fuerza bruta, trata de recuperar una clave probando todas las combinaciones posibles hasta

encontrar aquella que se busca, y que permite el acceso al sistema, programa o archivo en estudio.[4]

Figura 2. Tipos ataques



Fuente: Autor

El objetivo de las políticas de seguridad es definir qué están haciendo los usuarios con la información de la empresa, se deberá hacer un buen uso de los recursos de hardware y software y por supuesto eficientizar los costos. Política que debe implementar el departamento de sistemas informáticos para prevenir estos posibles ataques.

4.2.10 Buenas prácticas en seguridad informática. Según el European Microfinance network, define las Buenas Prácticas alcanzan las estrategias, formas, tácticas, proceso, pruebas, metodologías, actividades y enfoques que se evidencian, y están accesibles, son eficaces, aceptados y pertinentes desarrollados por la organizaciones y

[4] MONOGRAFIA.COM, Índice de seguridad tecnologías de información. {En línea}: 2013. Recuperado 09-05-2015. Disponible: http://www.monografias.com/trabajos16/tecnologias-informacion/tecnologias-informacion.shtml

profesionales idóneos realizados por un personal altamente capacitado. Las Buenas Prácticas de Seguridad Informática figuran:[5]

- Configurar el sistema operativo con todas sus normas de seguridad.
- Mantener actualizado el sistema operativo y sus aplicaciones.
- Protección en el correo electrónico, configuración de protección anti spam
- Conocimiento y protocolos para ingresar a aplicaciones externas que puedan ser objeto de Pishing.
- Seguridad en la navegación, configuración del Firewall, proxys, tiempos de navegación, bloqueo a ciertas aplicaciones que se consideren expuestas.

4.2.11 Identificación, clasificación y valoración de activos de información.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen.

- Las características de inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Oficina Asesora de Sistemas brinda herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

- La red de datos de la Empresa Social del Estado Fabio Jaramillo Londoño, en coordinación de la División de Recursos Físicos y la Sección de Almacén tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la empresa.

[5] BORBÓN Sanabria, J. {2011}: Buenas prácticas, estándares y normas. REVISTA. SEGURIDAD, DEFENSA DIGITAL. {En línea}: 11-05-2015. Disponible:http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-%20est%C3%A1ndares-y-normas.

4.2.12 Copias de seguridad. Toda información que pertenezca a la matriz de activos de información de la Empresa o que sea de interés para el proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros[6].

- Las dependencias de la Empresa Social del Estado Fabio Jaramillo Londoño, deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

- Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. La Oficina Asesora de Sistemas debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorias aleatorias que permitan determinar el correcto funcionamiento de los procesos de copias de seguridad.

- Las copias de seguridad de información crítica debe ser mantenida de acuerdo a cronogramas definidos y publicados por la Oficina Asesor de Sistemas en conjunto con la Red de Datos de la Empresa Social del Estado Fabio Jaramillo Londoño.

- La creación de copias de seguridad de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad

[6] UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS. “Seguridad de la Información SGSI” {En línea}. Recuperado el 24-05-2015. Disponible: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

4.2.13 Análisis del riesgo. La administratición del riesgo es utilizado para minimizar el riesgo aplicado efectivamente medidas de seguridad según las:

- Amenazas
- Vulnerabilidades y
- El valor de los activos a ser protegidos

El análisis es el método para:

- Identificar los riesgos
- Evaluar el posible daño que estos puedan causar a una empresa
- Justificar las medidas de seguridad que deben implementar en la misma

a. Objetivos del análisis del riesgo

El objetivo principal del análisis de riesgo es:

- Cuantificar el impacto de las amenazas potenciales.
- Asignar un precio o valor del costo de la pérdida de un negocio por la manifestación de un riesgo:
- Incluye la identificación de los riesgos y
- El costo/beneficio que justifica la seguridad y control, lo cual es de vital importancia de la creación de una arquitectura de seguridad que mitiga los riesgos de un negocio.

b. Características del análisis de riesgo.

- Permite considerar el costo de los sistemas automatizados y controles; respecto al impacto de la pérdida o modificación de los recursos e información de manera inadecuada, asociándolo a su vez al impacto en la empresa.
- Permite establecer un método por el cual las vulnerabilidades individuales se comparan para identificar escenarios actuales de amenazas de la seguridad y determinar la probabilidad en la que compromete la información protegida.
- Permite definir e implementar requerimientos de seguridad.
- Evaluación de las amenazar y vulnerabilidades conocidas y postuladas, con la finalidad de determinar la pérdida esperada y establecer el grado de aceptabilidad para la operación de sistemas.

Bajo este contexto, el analisis de riesgos es entonces una herramienta que permite ayudar a los directivos de negocio a obtener un entendimiento de los riesgos y las vunerabilidades asociadas a la información y la tecnologia que la habilita y apartir de ello establecer una arquitectura que reduzca el nivel del riesgo; ya que las tecnicas disponibles son dificiles de entender, producen resultados que son inciertos y requieren de personal altamente capacitado y experiencia que es dificil de entcontrar.

4.2.14 Gestión de riesgo. Para que gestionar un riesgo, se puede tomar varias alternativas.

- Aceptarlo
- Transferirlo
- Mitigarlo (Implementar políticas de seguridad)

Evitarlo (eventualmente)

4.3 MARCO LEGAL

4.3.1 Ley 1273 del 5 de enero de 2009 de delitos informáticos.

- **Artículo 69A**: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de los acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

- **Artículo 269B:** Obstaculización ilegítima de sistemas informáticos o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

- **Artículo 269C:** Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de una sistema informático que los trasporte.

- **Artículo 269D:** Daños informáticos. El que, sin estar facultado para ello, destruya**,** dañe, borra, altere o suprime datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

- **Artículo 269E**: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

- **Artículo 269F:** Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile,

sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

- **Artículo 269G:** Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

- **Artículo 269 H:** Circunstancias de agravación punitiva. Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere.[7]

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.

[7] Secretaria General de la Alcaldía Mayor de Bogotá, D.C.” Ley 1273 del 2009” En línea: Enero 5 de 2009. Recuperado el 11-05-2015. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información.

4.3.2 Ley estatutaria 1581 de 2012 Disposiciones Generales para la Protección de Datos Personales.

- **Artículo 1**°. Objeto. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.[8]

- **Artículo 2°.** Tratamiento de datos en el ámbito personal o doméstico. De conformidad con lo dispuesto en el literal a) del artículo 2° de la Ley 1581 de 2012, se exceptúan de la aplicación de dicha ley y del presente decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.

- **Artículo 3°.** Definiciones. Además de las definiciones establecidas en el artículo 3°. de la Ley 1581 de 2012, para los efectos del presente decreto se entenderá por:

- **Aviso de privacidad.** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las

[8] Secretaria General de la Alcaldía Mayor de Bogotá, D.C.” Decreto 1377 del 2013” {En línea}. Junio 27 de 2013. Recuperado el 11-05- 2015. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

políticas de Tratamiento de información que le serán se pretende dar a los datos personales.

- **Dato público.** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos sensibles.** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Transferencia.** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión**. Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de

Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

4.4 MARCO CONTEXTUAL

4.4.1 Marco institucional. La Empresa Social del Estado FABIO JARAMILLO LONDOÑO, es una empresa Social del Estado y constituye una categoría especial de Entidad Pública descentralizada del Orden Departamental, con personería jurídica, Patrimonio Propio y autonomía administrativa. Se ubica en la zona centro del Departamento del Caquetá y presta los servicios del Primer Nivel de Complejidad.

Fue creada mediante ordenanza No. 000914 del 29 de abril de 2005 y modificada por el Decreto No. 00781 de 28 de mayo de 2007, tienen una jurisdicción en los municipios de: Valparaíso, Solita, Milán y Solano. Municipios a orillas de los ríos Orteguaza y Caquetá, con sede Administrativa en el municipio de Florencia.

Figura 3. Nuestra historia

RAZON SOCIAL	E.S.E. Fabio Jaramillo Londoño
DIRECCION SEDE ADMINISTRATIVA	CARRERA 12 No 9B - 06 BARRIO JUAN XXIII Florencia – Caquetá.
NUMEROS TELEFONICOS	434 56 73 435 77 23
FAX	434 5673 Ext. 102
CORREO ELECTRONICO	esefabiojaramillo@hotmail.com
NIT	900.211.468 – 3
ACTIVIDAD ECONOMICA	Prestación de Servicios de Salud de Baja Complejidad
REPRESENTANTE LEGAL	Martha Patricia Ortiz Vega
DECRETOS DE CREACION	No. 000914 del 28 de Abril del 2005 No. 000781 del 28 de mayo de 2007, modifica el artículo 3, 4, 7 y 11 del Decreto No. 000914 del 2005

Fuente: Documento oficina Administrativa

4.4.2 Misión. Seremos en el año 2016 una Empresa Social del Estado, solida financieramente, competitiva y reconocida a Nivel Regional por la Prestación de Servicios de Salud de Baja complejidad, con Estándares de Calidad para nuestros usuarios.

4.4.3 Visión. Somos una Empresa Social del Estado FABIO JARAMILLO LONDOÑO, con sedes de atención en los municipios de: Milán, Solano, Solita y Valparaíso, que presta servicios de salud de baja Complejidad; con niveles de calidad centrados en la Seguridad del Paciente y la Participación Social, a través de una Gestión Financiera eficiente, con un Equipo Humano calificado, comprometido con actitud de servicio; contribuyendo al mejoramiento de la calidad de vida de nuestros usuarios.

Figura 4. Logo Empresa Social del Estado Fabio Jaramillo Londoño

Fuente: Documento oficina Administrativa

Nuestro Propósito. Prestar los servicios de salud de manera ejemplar, sin distingos de raza, credo o convicción política, dando lo mejor de cada uno de los funcionarios que integran nuestro equipo, para alcanzar la mayor satisfacción de nuestros usuarios.

- Políticas de Seguridad**.** En la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, estamos comprometidos a mejorar continuamente nuestro proceso en las áreas asistenciales, operativas y administrativas, para preservar la vida y salud de nuestra comunidad, brindando servicios de salud de calidad.

- Valores Corporativos. Nuestra cultura organizacional está orientada con valores corporativos que enmarcan el direccionamiento de la EMPRESA SOCIAL DEL ESTADO. Todos interiorizamos estos valores y los practicamos porque hacen parte de nuestras vidas e interactúan en los contextos en que nos desenvolvemos.

Figura 5. Valores de la Empresa Social del Estado Fabio Jaramillo Londoño

Fuente: Documento oficina Administrativa

- Respeto: Es reconocer los limites existentes entre las personas, aceptando y comprendiendo las particularidades de cada uno. El respeto nace hacia nosotros mismos y debe ser permanente con nuestros compañeros y la sociedad.

- Tolerancia: Es el dominio propio o control de sí mismo, respecto la dignidad y diferencia entre los seres, su relación y aceptación con diferentes personas y las distintas culturas, aceptando su actuar e incluyendo su derecho a expresarlo.

- Honestidad: El servidor público y/o contratista actuara con pudor, decoro y recato, tendrá responsabilidad consigo mismo y con los demás, en relación con la calidad de su trabajo, el compromiso con la empresa y el desarrollo de sus funciones, dando ejemplo de rectitud ante los demás servidores públicos y la comunidad en general.

- Principios Corporativos. Son el conjunto de los principales valores, creencias y normas éticas que rigen y regulan la vida de la empresa y constituyen la base de la cultura organizacional.

- Justicia: Actuar de manera razonable, mediante el reconocimiento de los deberes y derechos que toda persona demanda y posee, otorgándole a quien lo que le corresponde.

- Servicio: Brindar ayuda de manera espontánea en los detalles más pequeños, habla del alto sentido de colaboración para facilitar el acceso a los servicios ofertados.

- Responsabilidad: Cumplir debidamente con la Misión Institucional y asumir las consecuencias de las decisiones con la empresa y con la comunidad.

- Eficiencia: Es el mejor aprovechamiento de los recursos disponibles, para el logro de los objetivos y metas institucionales (Visión)

Políticas Institucionales

- Calidad: Mejoramiento continuamente de los procesos en las áreas asistenciales, operativas y administrativas, para preservar la vida y fomentar la salud de nuestra comunidad brindando servicios de salud de calidad.

- Seguridad del Paciente: Conjunto de acciones y estrategias que ofrece el sistema de garantía de calidad, para proteger al paciente de riesgos evitables que se deriven de la atención en salud.

- Usuarios: Usuarios activos para garantizar el derecho a salud

- Financiera: Empresa viable y sostenible financieramente.

- Sistema de Información: La información generada en los procesos de la ESE, debe ser confiable, oportuna, veraz, de calidad, cuantificable y comparable que permita el seguimiento y mejoramiento de los procesos.

- Talento Humano: Cliente interno y con niveles de bienestar físico y social.

4.4.4 Sedes de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

Está constituida por cinco (5) hospitales conformados por IPS Valparaíso, IPS de Solita, IPS de Solano, IPS Milán con su sede en la Inspección de Policía de San

Antonio de Getucha y su sede administrativa en Florencia, ubicada en la dirección Carrera 12 No. 9B-06 Barrio Juan XXIII.

- Sección Talento Humano: Integrantes:
- 1 gerente
- 1 Subgerente Administrativo
- 1 Subgerente de Servicios de Salud
- 3 Directores
- 12 Médicos Generales S.S.O
- 1 Auditor de Servicios de Salud
- 5 Odontología S.S.O
- 4 Bacteriólogos
- 4 Enfermeros Profesionales
- 3 Técnicos de Saneamiento
- 41 Auxiliares de Enfermería
- 1 Auxiliar de Laboratorio Clínico
- 1 Auxiliar de Higiene Oral
- 26 Promotores de Salud
- 5 Conductores de Ambulancia
- 1 Vigilante

4.4.5 Sección servicios de consulta médica externa.

La Empresa Social del Estado FABIO JARAMILLO LONDOÑO, cuenta con consultorios para la atención a la Salud del paciente ambulatorio, donde se ofrece orientación, diagnóstico y tratamiento médico a toda la comunidad, en las cinco (5) IPS Valparaíso, IPS de Solita, IPS de Solano, IPS Milán con su sede en la Inspección de Policía de San Antonio de Getucha.

- Sección Servicio de Odontología General
- Servicios odontológicos asistenciales:
- Un Consultorio Odontológico en cada una de nuestras Sedes
- Examen clínico de primera vez
- Consulta de Urgencias
- Obturación de superficies con amalgama
- Obturación de superficies con resina
- Exodoncia permanente
- Exodoncia en temporales
- Endodoncia
- Restauraciones en Ionómero de Vidrio
- Actividades de promoción y prevención en odontología
- Consulta de Primera vez
- Educación en salud oral
- Topicación con flúor
- Control de placa bacteriana
- Aplicación de sellantes de foto curado
- Detartraje Supra gingival
- Consulta de la Mujer Gestante

- Profilaxis

4.4.6 Sección de servicios de apoyo diagnóstico.

Contamos con el servicio de Imagen logia en las IPS de Solano, Solita y Valparaíso, el cual ofrece ayuda diagnosticas de Radiologías convencionales a los pacientes atendidos por: Consulta Externa, Hospitalizaciones y Urgencias, en forma permanente, eficiente y oportuna. Igualmente contamos con Laboratorio Clínico: De toma y procesamiento de muestras de laboratorio del primer nivel de atención, en las aéreas de:

- Hematología
- Microbiología
- Parasitología
- Química Sanguínea
- Serología o Inmunología

4.4.7 Sección de hospitalización, atención de urgencias y sala de parto.

- Hospitalización: Contamos con áreas destinadas al internamiento de los pacientes ara su diagnóstico, recuperación y/o tratamiento; así: Hospitalización adultos 27 camas, Hospitalización Pediátrica 17 camas, Obstetricia 9 camas.

- Atención de Urgencia**:** Prestamos el servicio de Primer Nivel de Complejidad, las 24 horas de día en Medicina General, con atención inmediata y estabilización del paciente; Consultorios Médicos, valoración y tratamiento inicial de urgencias, sala de procedimientos y sala de sutura.

- Sala de Partos: Nuestras salas están dotados de equipos básicos, para la atención de partos de baja complejidad y la atención de Adaptación Neonatal.

Estos servicios cuentan con la dotación y personal Asistencial comprometido con la misión de nuestra Empresa.

4.4.8 Sección de promoción de la salud prevención de la enfermedad.

Con el propósito de mejorar y mantener la salud y la calidad de vida de nuestros usuarios. La Empresa Social del Estado FABIO JARAMILLO LONDOÑO desarrolla los programas de Promoción y Prevención de acuerdo con los requerimientos en cada una de las etapas de ciclo vital (Niño, Adolescente, Mujer, Hombre, Adulto)

Con estos programas se busca que los individuos y familia en conjunto con La Empresa Social del Estado FABIO JARAMILLO LONDOÑ, desarrollen acciones tendientes a mejorar los comportamientos, prácticas y actitudes personales y colectivas duraderas, que mejoren su bienestar y calidad de vida.

- Programas de Promoción y Prevención
- Programa Ampliado de Inmunización PAI
- Planificación familiar
- Atención de Parto
- Atención de Recién Nacido
- Salud Preventiva Oral
- Detención Temprana de las alternativas del Crecimiento y Desarrollo del menor de 10 años
- Detección temprana de las alteraciones del Joven

- Detección temprana de las alteraciones del Adulto
- Detección temprana de las alteraciones del Embarazo
- Detección temprana del Cáncer de cuello Uterino
- Detección temprana de las alteraciones de la Agudeza Visual

4.4.9 Sección de telemedicina. La Empresa Social del Estado FABIO JARAMILLO LONDOÑO tiene la posibilidad de proveer servicios de salud a distancia, en los componentes de promoción y prevención, diagnóstico, tratamiento o rehabilitación, por profesionales de la salud que utilizan tecnologías de la información y la computación, que les permiten intercambiar datos con el propósito de facilitar el acceso de la población a servicios que presentan limitaciones de oferta, de acceso a los servicios o de ambos en su área geográfica.

La Empresa Social del Estado FABIO JARAMILLO LONDOÑO desarrolla esta modalidad en convenio con la Facultad de Medicina de la Universidad Nacional de Colombia y el Ministerio de la Protección Social. Ofrece las siguientes especialidades:

- Cardiología
- Ginecobstetricia
- Infecto logia
- Ortopedia y Traumatología
- Medicina Interna
- Dermatología

4.4.10 Sección de transporte.

La Empresa Social del Estado FABIO JARAMILLO LONDOÑO presta el servicio las 24 horas para el transporte de pacientes dentro del sistema de referencia y contra referencia hacia hospitales de mayor nivel de complejidad.

La Empresa Social del Estado FABIO JARAMILLO LONDOÑO, dispone de 6 ambulancias terrestres tipo T.A.B y cuatro Ambulancias fluviales.

4.4.11 Sección otros servicios. La Empresa Social del Estado FABIO JARAMILLO LONDOÑO cuenta con los recursos físicos, humanos y tecnológicos, dispuestos a trabajar directamente con la familiar y comunidad, acercando los servicios de salud e interviniendo en donde transcurre su cotidianidad, actuando como agente de cambio a nivel comunitario, dinamizando los procesos en torno a la salud.

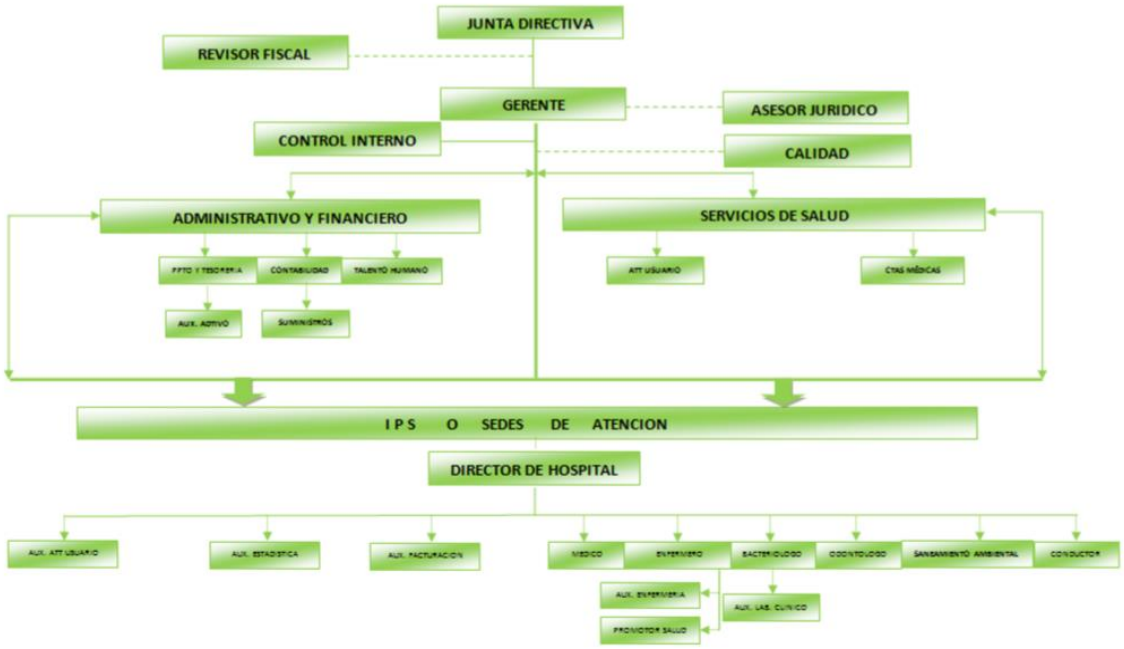
Además de los servicios que presta en sus sedes de atención, ofrecemos los servicios de:

- Psicología
- Salud Ocupacional
- Nutrición y Dietética

4.4.12 Organigrama de la Empresa Social del Estado Fabio Jaramillo Londoño.

Cuenta con una estructura establecida de acuerdo a los lineamientos de la administración pública, en la figura 6 se detalla el organigrama de la Empresa.

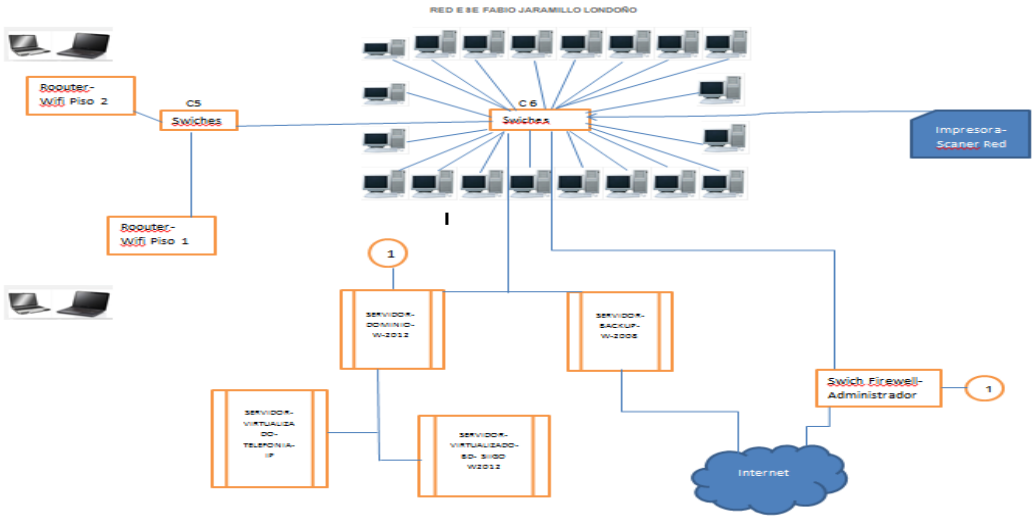
Figura 6. Organigrama



Fuente: Documento oficina Administrativa

4.4.13 Estructura de la Red de la Empresa. La Empresa Social del Estado Fabio Jaramillo Londoño, no cuenta con un centro de cómputo para la infraestructura tecnológica y maneja una red WAN, es una red en su topología estrella, la cual suministra múltiples servicios mediante la transmisión por fibra óptica servicios de voz y datos. (Ver Figura 7)

Figura 7. Estructura de la red de la entidad



Fuente: Autor

La topología de red construida que interconecta a las computadores entre sí en algunas de las sedes se encuentran habilitados los servicios de DHCP (Dynamic Host Configuration Protocolo) que entrega toda la información de conectividad y comunicación de manera automática a cualquier atacante externo que tenga acceso a un punto y cable de red, podrá husmear a merced propia toda la red.

Algunos de estos sitios de conectividad que forman parte de la red la Empresa Social del Estado FABIO JARAMILLO LONDOÑO cuentan con conectividad wifi, si bien es cierto ahorran mucho tiempo de instalación y adecuación, esta no cuenta con las medidas de seguridad necesarias para bloquear conexiones no deseadas que puedan esnifar la red y permita obtener acceso a documentos de nivel crítico. Este tipo de comunicación inalámbrica se encuentra protegida con una débil y sencilla contraseña de red, que puede ser vulnerable a las herramientas y algoritmos de cifrado actuales para romper este tipo de contraseñas.

Algunos de estos puntos de las sedes de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO cuentan con el servicio de conectividad a internet por distintos medios, comprendidos entre conexiones satelitales y en algunos casos

internet 3g y conmutado. A nivel de red no encontramos sistemas protección que bloqueen a atacantes externos desde la WAN o ajenos a la red. No se cuenta con dispositivos de firewall/corta fuegos de red que es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los equipos de cómputo, en su mayoría no cuenta con un software antivirus que proteja a las máquinas de amenazas como virus, adware, malware, phishing, entre otras amenazas. Muchas de las versiones de software antivirus que se encontró en estas equipos son versiones gratuitas que se pueden descargar libremente de la red, que si bien es cierto ofrecen una mediana o baja protecciones frente a esta problemática, no cuentan con la tecnología y los márgenes de detección adecuados para brindar una protección de alto nivel.

Los usuarios tienen acceso total a los equipos de cómputo y todas las funciones que estos ofrecen tales como poder conectar dispositivos periféricos externos ajenos a la Empresa Social del Estado FABIO JARAMILLO LONDOÑO como memorias USB y discos duros externos; posibilitando de esta manera la duplicidad y manipulación de información o el robo no autorizado de la misma por parte del mismo personal que es usuario de las maquinas.

Esto ha traído consigo problemas de seguridad en la información de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, por medio de acceso no deseados de intrusos, los cuales acceden a datos confidenciales, robos o alteran información valiosa, deniegan el acceso al servicio. Igualmente, existen riesgos físicos no controlables tales como incendios, inundaciones, terremotos o vandalismo que pueden afectar la disponibilidad de nuestra información y recursos. Haciendo inviable la continuidad de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, si no se está preparado para afrontarlos.

Si la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, no implementa mecanismos de seguridad en los sistemas de información, tanto a requerimientos tecnológicos y de manejo del personal en lo que se refiere a la manipulación de la información, que permitan mitigar o restringir los riesgos de acceso a sus datos de forma adecuada, la conllevará a un total fracaso para la empresa pues ya no tendría la privacidad de sus documentos, fichas y demás.

4.4.14 Responsabilidades del personal de la Empresa Social del Estado Fabio Jaramillo Londoño.

Todo el personal de la Empresa Social del Estado Fabio Jaramillo Londoño, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información de la empresa.

- Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la Oficina Asesora de sistemas, en cuanto a la información y la Red de Datos de la Empresa Social del Estado Fabio Jaramillo Londoño, en cuanto a los dispositivos hardware y los elementos software.

- La Empresa y el empleado deben contemplar procesos y sanciones disciplinarias para los casos en que se presente uso de información y TI que violen los términos y condiciones.

5 METODOLOGÍA

Se realiza una investigación viable, en el diseño de un modelo de un sistema de gestión de seguridad de la información, para la Empresa Social del Estado Fabio Jaramillo Londoño, basado en estándares y las normas internacionales, manejando la metodología de Margerit para la realización del análisis del riesgo de la seguridad informática, el cual tiene por objeto facilitar la identificación, análisis y evaluación de los factores que pueden influir en la manifestación del riesgo en la Organización, con la finalidad de que con la información obtenida se pueda evaluar la clase y dimensión de ese riesgo para cuantificarlo, contrarrestarlo o asumirlo. El análisis de riesgos de TI es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

Una de las principales características que debe poseer un empresa que busque establecer un SGSI es un enfoque por procesos, la norma ISO 27001 promueve la adopción del ciclo (Planear – Hacer – Verificar – Actuar) PHVA, para la definición de los procesos relacionados en el SGSI, aunque no es parte del alcance de presente documento el establecer una metodología para las organizaciones de cómo adquirir un enfoque por procesos, se darán una recomendaciones generales que ayudaran el lector a definir los procesos que intervendrán en el SGSI.

Fases de la realización.

1. Establecer el equipo
2. Definir el Servicio/sistema
3. Describir las funciones o componentes que lo integran
4. Listar modos de fallos potenciales de cada uno de ello
5. Definir los efectos de los modos de fallo
6. Describir las causas que podrían originar dichos fallos
7. Listar controles que permitan detectar cada modo del fallo

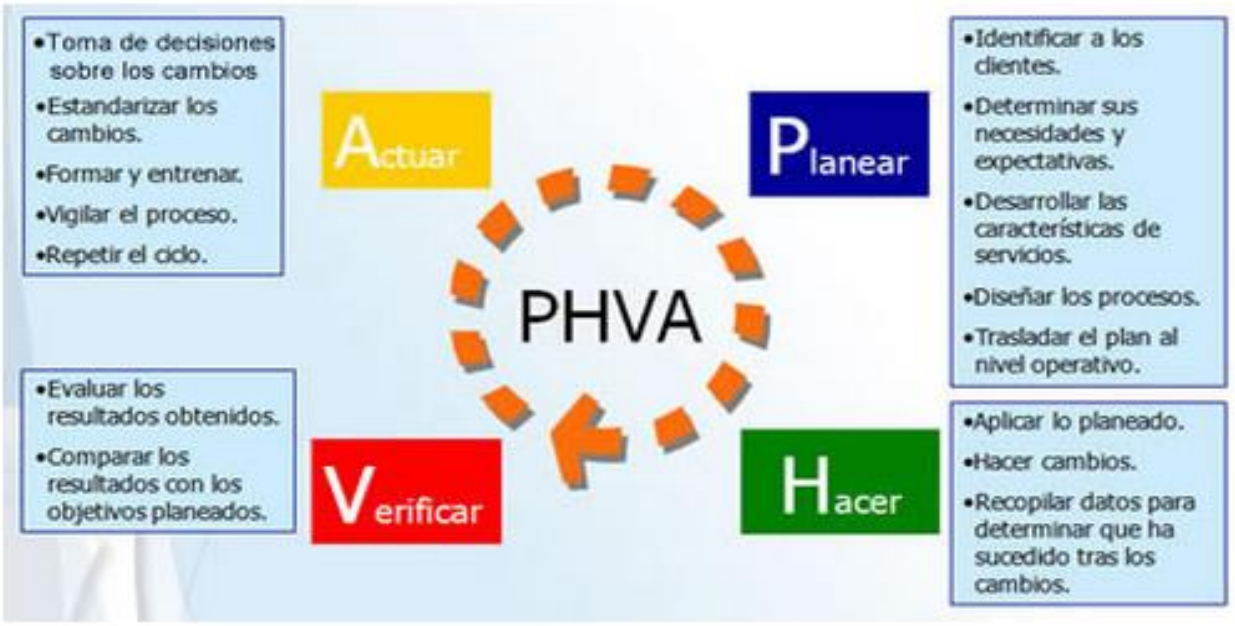
8. Calcular prioridades (impacto de cada riesgo)
9. Implantar acciones de mejora para prevenirlos

5.1 EL CICLO PHVA (METODO GERENCIAL)

El “control de proceso”, se establece a través del ciclo PHVA (Planear, hacer, verificar, actuar) compuesto por las cuatro fases básicas del control: [9]

- Planificar
- Ejecutar
- Verificar
- Actuar correctivamente.
-

Figura 8. Actividad ciclo PHVA



Fuente: Tomado de Implementación SIG[10]

[9] Gerencia de Calidad - Gerencia de Procesos. “Método de Control de Procesos” {En línea}. Junio 27 de 2013. Recuperado el 24-05- 2015. Disponible: http://www.unalmed.edu.co/josemaya/Ing_prod/Control%20de%20Proceso-%20Metodo.pdf

Los términos usados en el ciclo PHVA, tienen el siguiente significado:

5.1.1 Planear. Consiste en: Establecer metas para los indicadores de resultado y establecer la manera (el camino, el método) para alcanzar las metas propuestas.

5.1.2 Hacer. Ejecución de las tareas exactamente de la forma prevista en el plan y en la recolección de datos para la verificación del proceso. En esta etapa es esencial el entrenamiento en el trabajo resultante de la fase de planeamiento.

5.1.3 Verificar. Tomando como base los datos recolectados durante la ejecución, se compara el resultado obtenido con la meta planificada.

5.1.4 Actuar. Esta es la etapa en la cual el usuario detectó desvíos y actuará de modo que el problema no se repita nunca más.

[10] Implementación SIG. {2014}. El ciclo de Deming. {En línea}. {11 de mayo del 2015}.Disponible en http://www.implementacionsig.com/indez.php/generalidades-sig/55-ciclo-de

6 DESARROLLO DEL PROYECTO

Para dar cumplimiento al objetivo: Realizar encuestas al personal sobre los niveles de riesgo de los sistemas de información a su cargo, recomiendo lo siguiente:

A través de diferentes encuestas se analizó los problemas de seguridad de la información de la Empresa la Empresa Social del Estado Fabio Jaramillo Londoño, para poder así tomar decisiones, diseñar lineamientos de seguridad, analizar los riesgos y proponer el diseño del sistema de gestión de seguridad de la información.

6.1 ENCUESTA REALIZADA AL PERSONAL DE LA EMPRESA SOBRE LA SEGURIDAD DE LA INFORMACIÓN

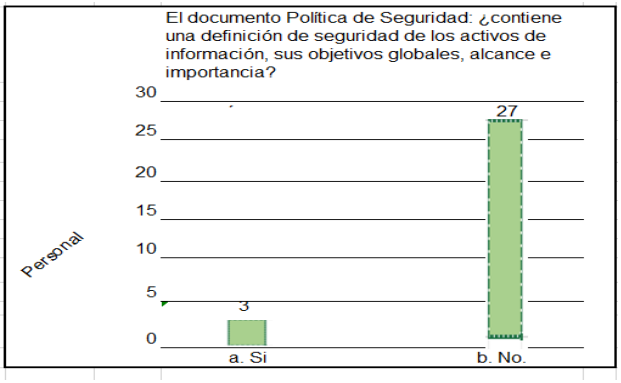
A algunos empleados de las dependencias de Administrativo y Financiero, servicios de salud y de la sala de sistemas de la Empresa Social del Estado Fabio Jaramillo Londoño, se le realizó una encuesta sobre la seguridad de la Información, para establecer y conocen Política de Seguridad, responsabilidad administrativa por los activos de información, si se identifican los activos de información y si se elabora un inventario de ellos, normas para transmisión por correo electrónico. (Ver Anexo 14). En cuesta realizada al personal de la empresa sobre seguridad de la información.

6.1.1 Resultado de la Encuesta de Seguridad de la Información.

A continuación el análisis del resultado de la encuesta.

- Pregunta 1 ”El documento Política de Seguridad: ¿contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia?“ (Ver Anexo 1)

Anexo 1. Muestra Pregunta 1, de la encuesta de seguridad de la información.

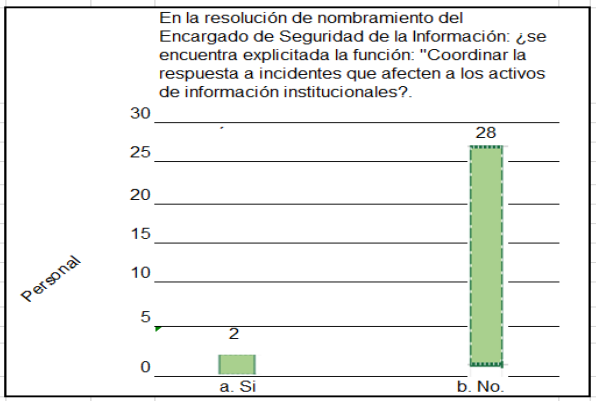


Fuente Autor

Se evidencia que el documento de políticas de seguridad de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, ya que desconocen el objetivo, alcance e importancia de la seguridad de la información.

- Pregunta 2 ”En la resolución de nombramiento del encargado de seguridad de la información: ¿se encuentra explicitada la función: "Coordinar la respuesta a incidentes que afecten a los activos de información institucionales?” (ver Anexo 2)

Anexo 2. Muestra Pregunta 2, de la encuesta de seguridad de la información

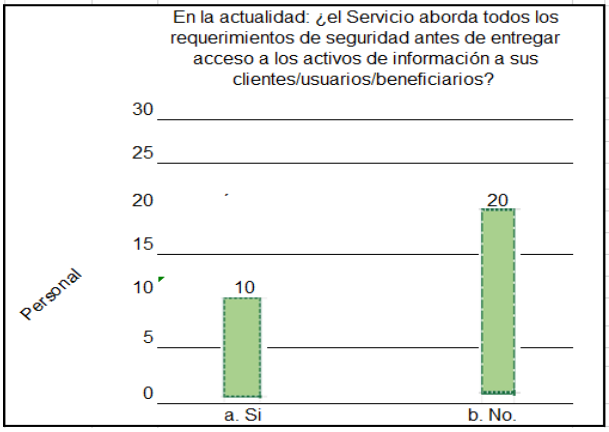


Fuente Autor

Se evidencia que en la Resolución de nombramiento del encargado de seguridad de la información de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, ya que desconocen los incidentes que afectan a los activos de información de la institución.

- Pregunta 3 ”En la actualidad: ¿el servicio aborda todos los requerimientos de seguridad antes de entregar acceso a los activos de información a sus clientes/usuarios/beneficiarios?“ (Ver Anexo 3)

Anexo 3. Muestra Pregunta 3, de la encuesta de seguridad de la información

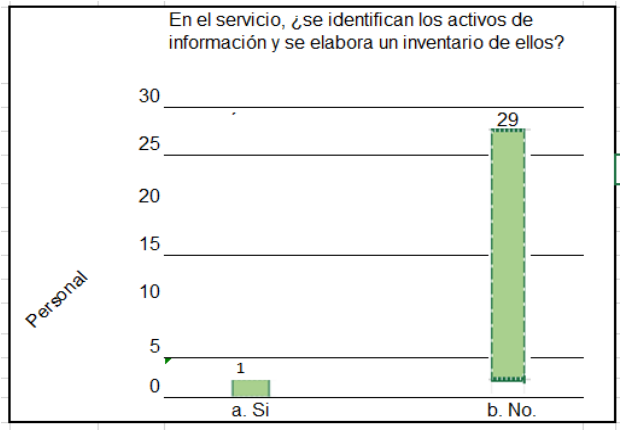


Fuente Autor

Se evidencia que en la actualidad en la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, los requerimientos de seguridad del acceso a los activos de información a los clientes/usuarios/beneficiarios, la cual la desconocen.

- Pregunta 4” En el servicio, ¿se identifican los activos de información y se elabora un inventario de ellos? “(Ver Anexo 4)

Anexo 4. Muestra Pregunta 4, de la encuesta de seguridad de la información.

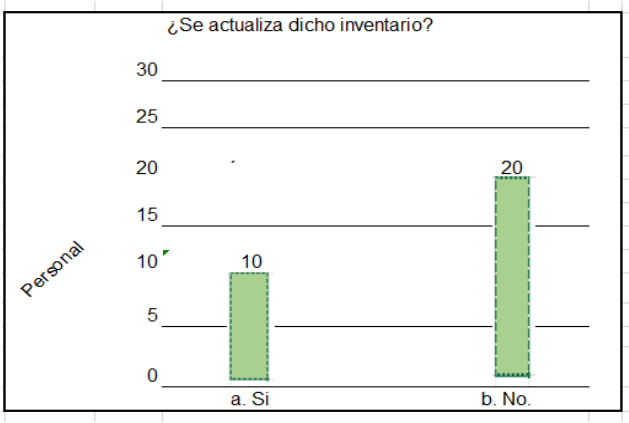


Fuente Autor

Se evidencia que en el servicio de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, la identificación de los activos de información y que debe existir un inventario de ellos.

- Pregunta 5 ”¿se actualiza dicho inventario?“ (Ver Anexo 5)

Anexo 5. Muestra Pregunta 5, de la encuesta de seguridad de la información.

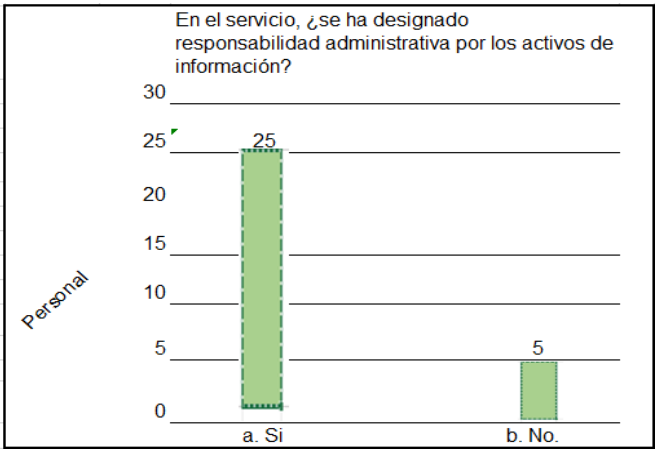


Fuente Autor

Se evidencia en la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, que los inventarios de los activos de información deben estar actualizados.

- Pregunta 6” En el servicio, ¿se ha designado responsabilidad administrativa por los activos de información? “(Ver Anexo 6)

Anexo 6. Muestra Pregunta 6, de la encuesta de seguridad de la información.

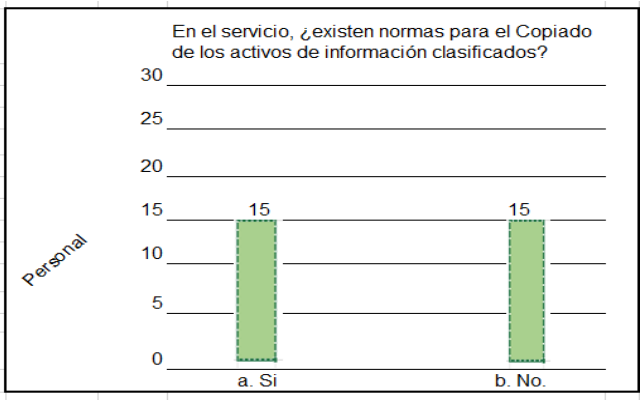


Fuente Autor

Se evidencia que en el servicio en la Empresa Social del Estado Fabio Jaramillo Londoño no se ha designado responsabilidad administrativas por los activos de información, ni han sido divulgados a todos los funcionarios de la organización.

- Pregunta 7 ”En el servicio, ¿existen normas para el copiado de los activos de información clasificados?“ (Ver Anexo 7)

Anexo 7. Muestra Pregunta 7, de la encuesta de seguridad de la información

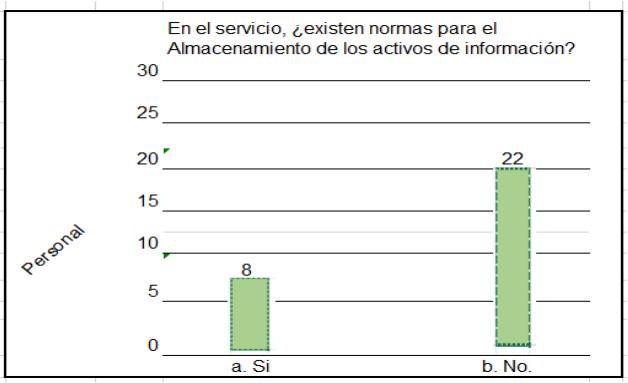


Fuente Autor

Se evidencia que el servicio de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, las normas para el copiado de los activos de información clasificado, las cuales se desconocen.

- Pregunta 8 ”En el servicio, ¿existen normas para el almacenamiento de los activos de información clasificados? “ (Ver Anexo 8)

Anexo 8. Muestra Pregunta 8, de la encuesta de seguridad de la información

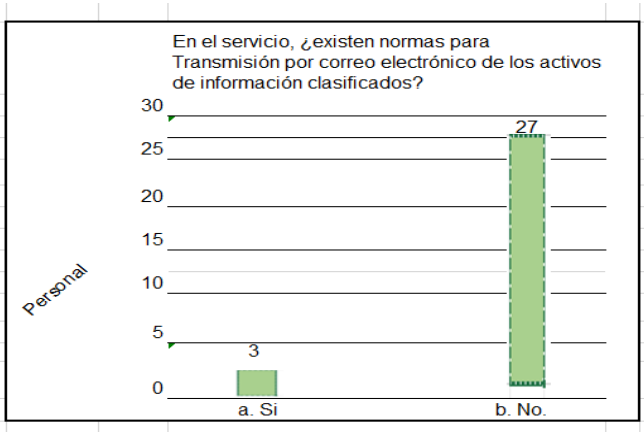


Fuente Autor

Se evidencia que el servicio en la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, las normas que existen para el almacenamiento de los activos de información clasificado, ya que desconocen.

- Pregunta 9” En el servicio, ¿existen normas para transmisión por correo electrónico de los activos de información clasificados?“ (Ver Anexo 9)

Anexo 9. Muestra Pregunta 9, de la encuesta de seguridad de la información

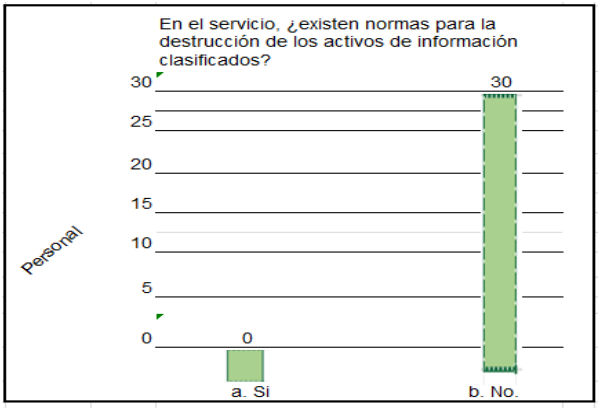


Fuente Autor

Se evidencia que el servicio en la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, las normas que existen para transmisión por correo electrónico de los activos de información clasificado, ya que desconocen.

- Pregunta 10 ”En el servicio, ¿existen normas para la destrucción de los activos de información clasificados?“ (Ver Anexo 10)

Anexo 10. Muestra Pregunta 10, de la encuesta de seguridad de la información



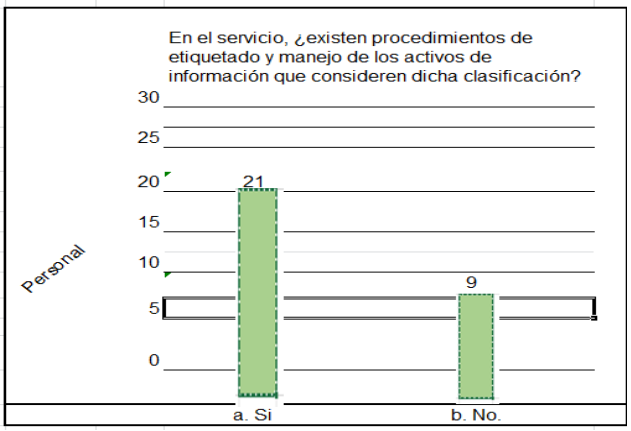
Fuente Autor

Se evidencia que en el servicio de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, ya que

desconocen que existen normas para la destrucción de los activos de información clasificados.

- Pregunta 11 ”En el servicio, ¿existen procedimientos de etiquetado y manejo de los activos de información que consideren dicha clasificación?“ (Ver Anexo 11)

Anexo 11. Muestra Pregunta 11, de la encuesta de seguridad de la información

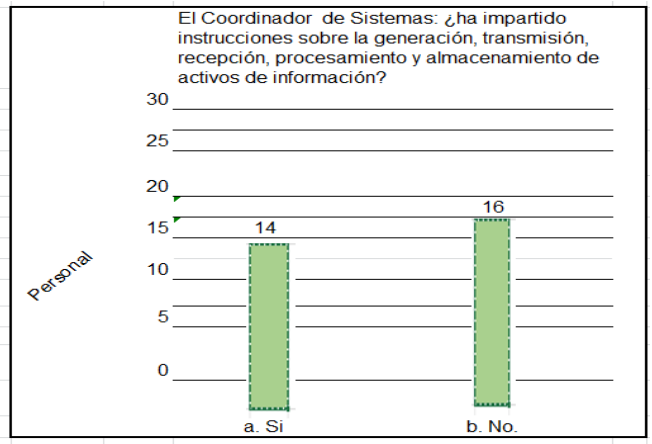


Fuente Autor

Se evidencia que en el servicio de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, ya que desconocen que existen procedimientos de etiquetado y manejo de los activos de información que consideren dicha clasificación.

- Pregunta 12 ”El coordinador de sistemas: ¿ha impartido instrucciones sobre la generación, transmisión, recepción, procesamiento y almacenamiento de activos de información? “ (Ver Anexo 12)

Anexo 12. Muestra Pregunta 12, de la encuesta de seguridad de la información

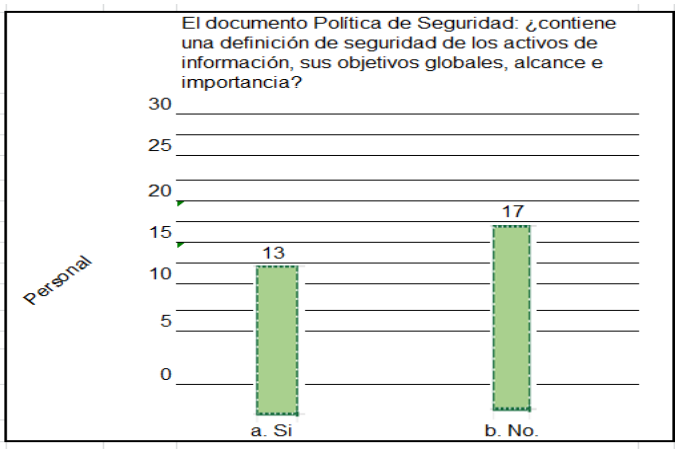


Fuente Autor

Se evidencia que el coordinador de sistemas de la Empresa Social del Estado Fabio Jaramillo Londoño, no ha dado a conocer las instrucciones a todos los funcionarios de la organización sobre la generación, transmisión, recepción, procesamiento y almacenamiento de activos de información, ya que desconocen

- Pregunta 13 ” El documento Política de Seguridad: ¿contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia? “ (Ver Anexo 13)

Anexo 13.Muestra Pregunta 13, de la encuesta de seguridad de la información



Fuente Autor

Se evidencia que el documento Política de Seguridad de la Empresa Social del Estado Fabio Jaramillo Londoño no ha sido divulgado a todos los funcionarios de la organización, ya que desconocen que contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia.

7 ANALISIS Y EVALUACION DEL RIESGO

7.1 DESCRIPCIÓN DE LOS ACTIVOS

Cada uno de los elementos que la entidad tiene para el procedimiento de la información (sistemas, soportes, edificios, personas) que tenga valor para la empresa. Para la realización del analisis del riesgo tenemos:

- Personal: Todo el personal interno y externo que manipulan la información en los sistemas de información. Auxiliares, Médicos , Técnicos de Saneamiento, Promotores de Salud, Administradores del Sisitema, Desarrolladores, personal de mantenimiento, contratistas y proveedores.

- Equipos informaticos: Equipos de oficina (portatiles, servidores,pc de escritorios, dispositivos moviles) Hay tres: Servidor WED IIS7, servidor de DOMINIOS DNS y Servidor de BD.

- Datos/Información: Son la información que se realiza en cada dependencia de la empresa y sus servicios que presta al usuario: Bases de datos del SIIGO

- Software/Aplicativos: Sistemas desarrollados para el manejo de la información, como el portal de la Página Web, Bases de Datos SIIGO, MYSQL, POSTGRES, SQLSERVER, para la generación de archivos planos RIPS, y captura de historias clínicas programa SGIS, digitalización de historias.

- Soporte almacenamiento de la información: Todos los elementos que sirven para guardar la información generada en la empresa o que se encuentra esa información, como discos extrahibles, cd y memorias USB.

7.2 INVENTARIO DE LOS ACTIVOS DE INFORMACIÓN

Tabla 1. Inventario de los activos de la información

INVENTARIO DE LOS ACTIVOS DE LA INFORMACIÓN				
RECURSO	**ITEM**	**TIPO**	**SOFTWARE**	**CANTIDAD**
Datos/Información	Activo 1	Bases de Datos MYSQL	Windows server 2012	1
	Activo 2	Bases de Datos POSTGRES	Windows server 2012	1
	Activo 3	Bases de Datos SQLSERVER	Windows server 2012	1
	Activo 4	Bases de Datos SIIGO,	Windows server 2012	1
Equipos informaticos	Activo 5	Equipos de Cómputo Escritorio	Windows XP, 2008 y 2012	15
	Activo 6	Equipos Portátiles	Windows 7 y Windows 2008	5
	Activo 7	Routers WIFI 4 PORT LAN 1 WAN 3G	N/A	2
	Activo 8	Servidores WED IIS7, DOMINIOS DNS y Backup.	Windows server 2008 y 2012	3
	Activo 9	Switches X 24	N/A	3
Personal	Activo 10	Personal Técnico, Administradores del Sisitema	N/A	1
	Activo 11	Personal de mantenimiento de los Sistemas de Información	N/A	2
	Activo 12	Antivirus	Licencia ESET Nod.32	10
	Activo 13	El Portal Web	Windows server 2012	1

Tabla 1. (Continuación)

INVENTARIO DE LOS ACTIVOS DE LA INFORMACIÓN				
RECURSO	**ITEM**	**TIPO**	**SOFTWARE**	**CANTIDAD**
Software/ Aplicativos	Activo 14	Programa Captura de Historias Clínicas programa SGIS	Windows server 2012	1
	Activo 15	Programa Generación Archivos Planos RIPS	Windows server 2012	1
Soporte almacenamiento de la información	Activo 16	Disco Duro HDD 1TRB SATA	N/A	6

Fuente Autor del Proyecto

7.3 DIMENSIONES DE VALORACIÓN

Son las características o atributos que hacen valioso un activo, estas se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.[11]

[D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

[11] PORTAL ADMINISTRACIÓN ELECTRÓNICA. {Madrid, octubre de 2012}. {En línea}." Magerit v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información". Recuperado el 05 de junio de 2015. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_cat%C3%A1logo%20de%20elementos_es_NIPO_630-12-171-8.pdf

[I] Integridad de los datos: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

[C] Confidencialidad de la información: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

[A] Autenticidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

[T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Para cada una de las dimensiones se establecerá un valor en escala porcentual, el cual medirá el impacto que causaría si se llegara a materializar cada una de las amenazas por activos.

7.4 IMPACTOS EN LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO

Para la Empresa Social del Estado Fabio Jaramillo Londoño, se tiene en cuenta los efectos de la ejecución de las distintas amenazas y los daños que éstas puedan causar. Son muchas las pérdidas que se pueden generar tecnológicas, financieras, físicas. (“Ver Tabla 3”). Igualmente se tiene en cuenta la Probabilidad de Frecuencia (FREQ) (Ver Tabla 4)

Tabla 2. Escala porcentual de impactos

Porcentaje	Criterio
90%-100%	Muy alto
75%-89%	Alto

50%-74%	Medio
20%-49%	Bajo
0%-19%	Muy bajo

Fuente: Autor del proyecto

Tabla 3. Probabilidad de frecuencia (FREQ)

Valor	**Criterio**	
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años
1/100	Muy poco frecuente	Siglos

Fuente: Magerit – versión 3.0 Libro I – Método

7.5 ANALISIS DE AMENAZAS POR ACTIVOS

El análisis de las amenazas por activos de la seguridad informática está enfocada en el análisis de vulnerabilidades con el fin de explicar y recomendar las cusas que generan el problema y la importancia de implementar controles en los sistemas de información en el área de sistemas de la Empresa Social del Estado Jaramillo Londoño, para mitigar las amenazas existentes. Igualmente, se podrá valorar el estado de activo que es afectado sobre las dimensiones de seguridad de la metodología Magerit como la [D] Disponibilidad, [I] Integridad de los datos, [C] Confidencialidad de la información, [A] Autenticidad y [T] Trazabilidad. (Ver Tabla 4).

Tabla 4. Análisis de amenazas por activos

AMENAZAS POR ACTIVO			FREQ	[D]	[I]	[C]	[A]	[T]
	Activo 1	**Bases de Datos MYSQL**		50%	100%	100%	100%	
		[E.1] Errores de los usuarios	10	10%	10%	10%		
		[E.2] Errores del administrador	1	50%	20%	20%		
		[A.5] Suplantación de la identidad del usuario	10		10%	50%	100%	
		[A.11] Acceso no autorizado	100		100%	100%		
	Activo 2	**Bases de Datos POSTGRES**		100%	100%	100%		
		[E.4] Errores de configuración	10	100%	100%	100%		
Datos/		[A.14] Interceptación de información (escucha)	100			80%		
Información		[E.1] Errores de los usuarios	10	10%	10%	10%		
	Activo 3	**Bases de Datos SQLSERVER**		1%	100%	100%		
		[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
		[A.11] Acceso no autorizado	100		100%	100%		
	Activo 4	**Bases de Datos SIIGO**		50%	20%	100%	100%	
		[E.2] Errores del administrador	1	50%	20%	20%		
		[A.5] Suplantación de la identidad del usuario	10		10%	50%	100%	
		[A.19] Revelación de información	10			100%		
	Activo 5	**Equipos de Cómputo Escritorio**		1%	1%			
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	1%	1%			

Tabla 4. (Continuación)

AMENAZAS POR ACTIVO			REQ	[D]	[I]	[C]	[A]	[T]
	Activo 6	**Equipos Portátiles**		1%	1%			
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	1%	1%			
Equipos informaticos	**Activo 7**	**Routers WIFI 4 PORT LAN 1 WAN 3G**		1%	10%	50%		
		[A.7] Uso no previsto	10	1%	10%	50%		
	Activo 8	**Servidores WED IIS7, DOMINIOS DNS y Backup.**		100%	100%	100%		
		[E.4] Errores de configuración	10	100%	100%	100%		
		[E.14] Escapes de información	1		100%	100%		
		[A.4] Manipulación de la configuración	1	100%				
	Activo 9	**Switches X 24**		100%	20%	50%		
		[E.2] Errores del administrador	1	100%	20%	50%		
	Activo 10	**Personal Técnico, Administradores del Sisitema**		50%	100%	100%		
Personal		[A.30] Ingeniería social (picaresca)	1	50%	100%	100%		
	Activo 11	**Personal de mantenimiento de los Sistemas de Información**		10%				
		[A.28] Indisponibilidad del personal	1	10%				
		Antivirus		50%	10%			
Software/	**Activo 12**	[E.21] Errores de mantenimiento / actualización de programas (software)	1	50%	10%			
Aplicativos								
	Activo 13	**El Portal Web**		50%	20%	50%		
		[E.8] Difusión de software dañino	1/10	50%	20%	50%		
	Activo 14	**Programa Captura de Historias Clínicas programa SGIS**		1%	20%	20%		
		[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%		

Tabla 4. (Continuación)

			FREQ	[D]	[I]	[C]	[A]	[T]
	Activo 15	**Programa Generación Archivos Planos RIPS**		50%	100%	100%		
		[E.1] Errores de los usuarios	10	10%	10%	10%		
		[A.22] Manipulación de programas	1	50%	100%	100%		
Soporte almacenamiento de la información		**Disco Duro HDD 1TRB SATA**		100%				
	Activo 16							
		[A.18] Destrucción de información	10	100%				

Fuente: Autor del proyecto

7.5.1 Estimación del Impacto

En el análisis del impacto se evidencia el daño que se origina en el activo producido de la realización de una amenaza. Con la obtención de los valores de los activos y el porcentaje de la degradación que originan las amenazas se proviene el impacto que tienen sobre los activos de la Empresa (Ver Tabla 5).

Tabla 5. Valores estimado de Impacto

Degradación						
IMPACTO		1%	10%	50%	80%	100%
	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	B	MB	MB	MB	MB	MB

Fuente: Magerit – versión 3.0 Libro I – Método

7.5.2 Resumen del Análisis del Riesgos del Estado Actual de los Activos de Información de la Empresa Social del Estado Fabio Jaramillo Londoño.

Tabla 6. Resumen del Análisis de Riesgo

Resumen del Análisis de Riesgos del Estado Actual de los Activos de Información de la Empresa Social del Estado Fabio Jaramillo Londoño	FREQ	[D]	[I]	[C]	[A]	[T]
[**Activo 1**] **Bases de Datos MYSQL**		50%	100%	100%	100%	
[**Activo 2**] **Bases de Datos POSTGRES**		100%	100%	100%		
[**Activo 4**] **Bases de Datos SIIGO**		50%	20%	100%	100%	
[**Activo 8**] **Servidores WED IIS7, DOMINIOS DNS y Backup.**		100%	100%	100%		
[**Activo 9**] **Switches X 24**		100%	20%	50%		
[**Activo 10**] **Personal Técnico, Administradores del Sisitema**		50%	100%	100%		
[**Activo 13**] **El Portal Web**		50%	20%	50%		
[**Activo 15**] **Programa Generación Archivos Planos RIPS**		50%	100%	100%		
[**Activo 16**] **Disco Duro HDD 1TRB SATA**		100%	100%	100%		

Fuente: Autor del proyecto

8 DISEÑO DE UN MODELO GENERAL DE SEGURIDAD DE LA INFORMACIÓN SGSI

Con el análisis de los controles del anexo A de la norma ISO 27001: 2013, los pilares de seguridad de la información y los activos de información se recomiendan mejoras, implementar y nuevas medidas de seguridad sobre los activos, los procesos y los sistemas que brindan servicios en la Empresa Social del Estado Fabio Jaramillo Londoño.

La versión 2013 de la norma ISO 27001: 2013 incluye los siguientes catorce controles principales:

1. **DOMINIO A5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**
2. **DOMINIO A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
3. **DOMINIO A7. SEGURIDAD DE LOS RECURSOS HUMANOS**
4. **DOMINIO A8. GESTIÓN DE ACTIVOS**
5. **DOMINIO A9. CONTROL DE ACCESO**
6. **DOMINIO A10. CRIPTOGRAFÍA**
7. **DOMINIO A11. SEGURIDAD FISICA Y DEL ENTORNO**
8. **DOMINIO A12. SEGURIDA DE LAS OPERACIONES**
9. **DOMINIO A13. SEGURIDAD DE LAS COMUNICACIONES**
10. **DOMINIO A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
11. **DOMINIO A15. RELACIONES CON LOS PROVEEDORES**
12. **DOMINIO A16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
13. **DOMINIO A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**
14. **DOMINIO A18. CUMPLIMIENTO**

8.1 ANÁLISIS DETALLADO DEL ANEXO A ISO 27001:2013

Tabla 7. Análisis detallado del Anexo A ISO 27001:2013

CHECK LIST DE LA NORMA 27001-2013 EN LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO					
REQUISITO	**4 CONTEXTO DE LA ORGANIZACIÓN**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
4.1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO		X		Implementar políticas de seguridad de la información, dar a conocemos los objetivos generales, alcance, importancia, referencias a documentos de soporte, responsabilidades, explicación de normas sus requisitos legales, contractuales, aplicabilidad de la ética profesional y ética de la información para los programadores.
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS		X		La necesidad de la implementación de unas políticas de seguridad de los sistemas de información y de un sistema de gestión de seguridad de la información.
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		X		Al implementar un sistema de gestión de seguridad para la empresa ayuda a mitigar los riesgos
4.4	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		X		Elaborar un diseño de un Sistema de Gestión de Seguridad de la Información, que garantice la disponibilidad eficaz de la información y el cumplimiento de normas y estándares internacionales.

REQUISITO	5 LIDERAZGO	Cumple	no cumple	que se tiene	Recomendaciones a implementar
5.1	LIDERAZGO Y COMPROMISO	X		La Dirección de la empresa lidera todo el proceso, ya que es la que conoce los riesgos del negocio y las obligaciones con sus clientes y accionistas mejor que nadie.	
5.2	POLÍTICA		X	Políticas de Seguridad: Estamos comprometidos a mejorar continuamente nuestro proceso en las áreas asistenciales, operativas y administrativas, para preservar la vida y salud de nuestra comunidad, brindando servicios de salud de calidad	Implementar políticas de seguridad de la información conocemos los objetivos generales, alcance, importancia- declaración de intención, referencias a documentos de soporte, responsabilidades, explicación normas- leyes: requisitos legales- contractuales, formación, Gestión de Continuidad de Negocio, consecuencias de violación.
5.3	ROLES, RESPONSABILIDADES. Y AUTORIDADES EN LA ORGANIZACIÓN		X		Implementar las responsables de procesos de seguridad y de activos, definir niveles de autorización sobre estos activos e información. Empleados, contratistas y usuarios terceras partes: Cumplir política, proteger activos, ejecutar procesos, informar eventos.

REQUISITO	6 PLANIFICACIÓN	Cumple	no cumple	que se tiene	Recomendaciones a implementar
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES		X	Cuenta con auditoria interna, MECI, pero esto no abarca los sistemas de información.	Si la empresa, no implementa mecanismos de seguridad en los sistemas de información, control Interno Informático, tanto a requerimientos tecnológicos y de manejo del personal en lo que se refiere a la manipulación de la información, que permitan mitigar o restringir los riesgos de acceso a sus datos de forma adecuada, la conllevará a un total fracaso para la empresa pues ya no tendría la privacidad de sus documentos, fichas y demás.
6.1.1	Generalidades		X		Establecer un plan de contingencia para la parte Administrativa en el área de sistemas
6.1.2	Valoración de riesgos de la seguridad de la información		X		Como la Empresa no cuenta con el levantamiento físico de los activos de la información ni los inventarios de los mismos, se recomienda realizarlos y documentarlos.
6.1.3	Tratamiento de los riesgos de seguridad de la información	X		A través de la oficina de Control Interno, y aplicando MECI, se hace verificación en el uso de los software existentes en la empresa. La actualización permanente a los sistemas de los procesos Institucionales.	Se de implementar planes de seguimiento y mejora en los sistemas de información.

6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLO		X		La realización de auditorías a los sistemas; tienen por objetivo ayudar a las instituciones a identificar su situación actual respecto a las vulnerabilidades de la red de datos y a la vez optar por la implementación de un Sistema de Gestión de Seguridad de la Información, que garantice la disponibilidad eficaz de la información y el cumplimiento de normas y estándares internacionales.
REQUISITO	**7 SOPORTE**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
7.1	RECURSOS		X	Cuenta con los recursos físicos, humanos y tecnológicos, dispuestos a trabajar.	A pesar que cuenta con recursos físicos, humanos y tecnológicos, esto no es suficiente ya que en cuanto a infraestructura no existe una sala de sistemas adecuación, los medios tecnológicos con que cuenta muchos de ellos son obsoletos y en cuanto al talento humano, no se ha capacitado en el tema de la seguridad de la información, políticas de seguridad.
7.2	COMPETENCIA	X		Son empleados bien calificados, idóneos, con ética profesional.	
7.3	TOMA DE CONCIENCIA		X		La empresa cuenta con personal contratista esto hace que no tomen concientización, esto es un factor en algunos escenarios de riesgo y adicional a esto la no presentación o divulgación de los deberes y responsabilidades de los empleados.
7.4	COMUNICACIÓN		X		Deben de tener una comunicación asertiva y estable con todos los miembros de la empresa.
7.5	INFORMACIÓN DOCUMENTADA	X		Tienen plantillas para para la elaboración de las actas, formatos, las cuales son Clasificadas y controladas.	

7.5.1	Generalidades		X		Implementación de las salvaguardas, actúan reduciendo la probabilidad de las amenazas y Limitando el daño causado.
7.5.2	Creación y actualización	X		En el desarrollo del software, en este se diseña, implementa y mantiene para protegerse contra el acceso no autorizado. Se realizan actuales a los mismos.	
7.5.3	Control de la información documentada	X		Se hace a través de internet, ya que los proveedores son de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.	
REQUISITO	**8 OPERACIÓN**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL	X		Los resultados de la Gestión de la Oficina de Control Interno, se dan a conocer a la Gerencia y a las Subgerencias de la Empresa.	
8.2	VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		X		Si la empresa no realiza seguimientos, análisis del riesgo e implementa un Sistema de Gestión de Seguridad de la Información, no podrá saber su valor en caso de una perdida de información, cuanto le costaría no tener asegurado sus datos de información.
8.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		X		Estar preparados, se debe realizar y tener presente en caso de presentarse un inconveniente, el tratamiento a seguir.

REQUISITO	9 EVALUACIÓN DEL DESEMPEÑO	Cumple	no cumple	que se tiene	Recomendaciones a implementar
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	X		La Oficina de Control Interno, en desarrollo de su gestión continua con la ejecución del Plan de acción y de Auditorias planeadas para la vigencia.	Ejecutar los planes de mejoramiento en la empresa y realizar los seguimientos necesarios para verificar el cumplimiento a las acciones de mejora y demás compromisos adquiridos al interior de la empresa y con entes de control.
9.2	AUDITORIA INTERNA	X		Cuenta con la oficina de Control Interno, y aplicando MECI, el uso de los softwares existentes en la empresa permite el procedimiento inmediato de la información, como herramienta eficaz para la toma de decisiones por parte de la gerencia. La actualización permanente a los sistemas de los procesos Institucionales.	Desarrollar a través de control interno auditorias especialmente a los sistemas, para que se verifiquen los filtros, de confiabilidad de los sistemas de información. Igualmente, a través de las recomendaciones ejecutadas para adecuación del centro de cómputo para la Empresa.
9.3	REVISIÓN POR LA DIRECCIÓN	X		La alta dirección de la empresa brinda total apoyo a la oficina de Control Interno; lo cual ha permitido mantener el modelo MECI, demostrado con el resultado alcanzado en la Evaluación del Modelo Estándar de	Se debe implementar un seguimiento de revisión por la Dirección, para la mejora continua, educar y entrenar a los usuarios.

				Control Interno su estado de Madurez para la vigencia, con una calificación Satisfactoria.	
REQUISITO	**10 MEJORA**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
10.1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS		X		Al no existir auditorías a los sistemas ni una política de seguridad, no se han ejecutado no conformidades ni acciones correctivas
10.2	MEJORA CONTINUA	X		Se da continuidad a la socialización del proceso de planeación de seguridad del paciente con la aplicabilidad del ciclo PHVA, siguiendo con la trazabilidad con la documentación institucional de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, Culminar la actualización del mapa de riesgos en los procesos Institucionales, revisar en forma periódica su estado de tal forma que permita establecer puntos de control adecuado, acorde al desarrollo de la Empresa Social del	Continuar con la actualización de forma permanente de la página Web de la ESE, donde se comunique a la comunidad sobre los eventos y procesos que se adelantan en la misma. Igualmente, continuar con la Implementación del Software de Facturación y de Historias Clínicas en la IPS.

				Estado FABIO JARAMILLO LONDOÑO.	

ANEXO A (OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA)					
DOMINIO A5:	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A5.1	Orientación de la dirección para la Gestión de la seguridad de la información				
Objetivo	Brindar soporte y orientación por parte de la dirección.				
Numeral	**Controles**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A5.1.1	Políticas para la seguridad de la información		X		Es una necesidad primaria que se debe abordar y poner en conocimiento la responsabilidad de la Dirección.
A.5.1.2	Revisión de las políticas para la seguridad de la información		X		Implementar auditorías a los sistemas de información.
DOMINIO A6:	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.6.1	Organización interna				
Objetivo	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización				
Numeral	**Controles**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.6.1.1	Roles y Responsabilidad		X		Al personal se le debe asignar de acuerdo a sus funciones roles y responsabilidades con el resguardo de la información. Dar a

	es para la seguridad de la información.				conocer a los empleados sobre la Ética profesional.
A.6.1.2	Separación de deberes	X		Cada empleado tiene sus propios deberes y acceso a la misma.	Gestionar la viabilidad de la implementación de políticas de seguridad y darlas a conocer a todo el personal.
A.6.1.3	Contacto con las autoridades	X		La autoridad está en cabeza de cada jede de Sección. El proceso es reportar incidentes por incumplimiento de la ley (policía, bomberos)	Se debe tener buena relaciones, con los superiores, demás organismos del estado y acatar órdenes, en cuanto al cuidado y tratamiento de la información.
A.6.1.4	Contacto con grupos de interés especial		X		Consultar a Especialistas de la seguridad para ejecutarla en toda las oficinas.
A.6.1.5	Seguridad de la información en la gestión de proyectos	X		Por parte de control interno se hace auditoria en cuanto a la gestión, cuentan con plan de desarrollo y plan estratégico.	Es deber de la dirección apoyar en la evaluación periódicamente de la seguridad de la información de cualquier proyecto implementado o a desarrollar.
A.6.2	**Dispositivos móviles y teletrabajo**				
Objetivo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A.6.2.1	Política para dispositivos		X		Implementar seguridad de telefonía móvil, restricciones al ingreso a internet, encriptar la información. Controlar, bloquear, encriptar

	móviles				códigos móviles.
A.6.2.2	Teletrabajo	X		La Gerencia es la permite que se realicen trabajos fuera de la empresa y esta les exige a los empleados que se cumplan con las mismas seguridades que se tiene en la empresa. El servicio de Internet a través de telefonía móvil y otros servicios de comunicación en los municipios donde la empresa hace presencia, continua afectando el proceso de la implementación de sistemas informáticos (software) en línea y la ejecución de los diferentes	Si la información de hace física, tener el envío con empresas con seguridad y reservado. Igualmente, se debe desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

				procesos de la empresa.	
DOMINIO A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.7.1	**Antes de asumir el empleo**				
Objetivo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que consideren				
A.7.1.1	Selección	X		Los empleados son contratados de acuerdo a su perfil.	Al usuario se le debe exponer con claridad los cuidados a que tiene con la empresa, en cuanto a la información que va a manejar.
A.7.1.2	Términos y condiciones del empleo	X		Cada funcionario resguarda la información de su labor diaria, teniendo una clave de acceso.	Capacitar al personal sobre seguridad de la información sobre las amenazas, riesgos y vulnerabilidades, así como socializar el manual de funciones.
A.7.2	**Durante la ejecución del empleo**				
Objetivo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan				

A.7.2.1	Responsabilidades		X		Establecer primero que todo las políticas de seguridad en la empresa, para ser difundida y concientizar a los empleados, de la importancia de la seguridad de la información. Dar a conocer los reglamentos de ética profesional. La empresa tiene que ofrecer unos planes de formación continua, promoviendo el desarrollo de una carrera profesional de sus empleados. Estos planes de formación han de incluir todos los temas básicos para el desarrollo de su trabajo (leyes aplicables, seguridad, prevención de riesgos laborales, metodologías, tecnologías y conocimientos funcionales).
A.7.2.2	Toma de conciencia educación y formación en la seguridad de la información.		X		La falta de concientización de los usuarios, esto no es diferente de otras plataformas, sin embargo, un factor en algunos escenarios de riesgo. Por ejemplo, la divulgación no intencional de datos a menudo se basa en la falta de conciencia de los usuarios de las implicaciones que trae el consentimiento a la divulgación de datos.
A.7.2.3	Proceso disciplinario	X		Por medio de oficina de Control Interno, se hace seguimiento a los procesos. Establecer un proceso disciplinario formal a la violación a la seguridad.	Se debe dar a conocer a los usuarios internos de la legislación sobre los delitos informáticos y sus las penalidades en caso de fraude, robo o fuga de información, daño o sabotaje informático.

A.7.3	**Terminación y cambio de empleo**				
Objetivo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	X		La Dirección con apoyo proceso de MCI, hacer saber al empleado del recibo de bienes y funciones. Procedimientos retiro de derechos- políticas, responsabilidad después de terminación contrato.	Debe existir, documentación, actas tanto para la entrega y/o recibo de bines de la empresa, se debe hacer la inducción al puesto de trabajo a cada empleado.
DOMINIO A.8	**GESTIÓN DE ACTIVOS**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.8.1	**Responsabilidad por los activos**				
Objetivo	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.				
A.8.1.1	Inventario de activos		X		Por parte del encargado Área de Sistemas, se debe ejecutar el levantamiento total de inventarios de los activos que cuenta la

					empresa, clasificándolos por niveles, manteniendo un inventario de activos definidos, relación de los riesgos con tipo de activos, mantener registros de personas con sus capacitaciones y realizar las hojas de vida de cada elemento de cómputo.
A.8.1.2	Propiedad de los activos		X		Por parte del contratado para el Área de Sistemas, se debe realizar la individualización de los activos físicas y dejando soporte de los mismos. Al igual de las responsabilidades del cuidado de los mismos.
A.8.1.3	Uso aceptable de los activos		X		Implementar reglas para el uso aceptable de los activos informáticos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, implica la aceptación por parte de los usuarios, de las normas, políticas y estándares establecidos para garantizar la seguridad informática.
A.8.1.4	Devolución de activos	X		Se tiene diseñado un formato de Paz y Salvo, por parte de la Almacenista para la entrega de los bienes, en el programa SIIGO. Procedimientos – políticas de devolución de activos información a la entidad. Si utiliza equipo propio debe transferir informando a la institución y hacer eliminación-documentar.	Este trámite de sebe estandarizar según las normas de calidad, para el cuidado, buen manejo y entrega definitiva de los activos.

A.8.2	**Clasificación de la Información**				
Objetivo	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la Información	X		Cuenta con su calificación de la información pública la que se publica en la página WEB y privada, las Historias Clínicas, solo con una Orden Judicial se entregaran.	Estandarizar en el documento impreso, en la plantilla membretado de la Empresa lo que sea secreto o reservado
A.8.2.2	Etiqueta de la información	X		La información que se envía electrónicamente es encriptada	Establecer Normas y Política del Ministerio del Interior sobre seguridad y uso de los sistemas de tratamiento de información, de las redes y del correo electrónico, secreto o reservado.
A.8.2.3	Manejo de Activos		X		Implementar política y gestión para el manejo de Activos Fijos.
A.8.3	**Manejo de Medios**				
Objetivo	Evitar la divulgación, la momificación, el retiro o la destrucción no autorizados de la información almacenada en los medios				
A.8.3.1	Gestión de medios removibles		X		Diligenciar la información que se solicita en el formato del equipo usado antes de realizar el borrado, verificar en la hoja de vida que se solicita en este formato es el mismo de la placa que determine en el PC.
A.8.3.2	Disposición de los medios	X		Se diligencia el acta de respaldo de la información y borrado seguro.	Es responsabilidad del Área de Tecnología e Informática disponer de medios seguros para que los funcionarios que posean notebooks accedan a la información.
A.8.3.2	Transferencia medios físicos	X		El administrador, ejecuta el	Implementar políticas de usuario.

				archivo bat, para configuración de reglas en el firewall. (usuario de autenticación)- Usar transporte confiable, embalaje, varias rutas.	
DOMINIO A.9	**CONTROL DE ACCESO**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.9.1	**Requisitos del negocio para control de acceso**				
Objetivo	Limitar el acceso a información y a instalaciones de procesamiento de información.				
A.9.1.1	Política de control de acceso		X		Desarrollar e implementar política de control de acceso de la Seguridad informática y atendiendo la legislación aplicable: Para así asegurar que en la empresa, la información está protegida contra divulgación a usuarios no autorizados (confidencialidad), modificación inapropiada (integridad) y al no acceso cuando se requiere (disponibilidad). Asimismo establecer, documentación y revisar reglas y derechos de cada usuario int/ext en servicios y sistemas. Requisitos de seguridad de software.
A.9.1.2	Acceso a redes y a servicios en red		X		Los primeros elementos que se deben definir son las políticas relacionadas con el uso y manejo y de sus datos. Esto le ayudara a determinar las medidas y procedimientos de defensa.

					– procesos de autorización uso de redes y servicios. - Crear políticas de Directivas de usuario. Definir lo que los usuarios pueden y deben hacer para usar su red y equipos informáticos de la organización. Definir los limitaciones a los usuarios mantener la red segura como; Como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que pueden utilizar, y cómo pueden acceder a los datos.
A.9.2	**Gestión de acceso de usuario**				
Objetivo	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A.9.2.1	Registro y cancelación registro de usuario.		X		Se debe crear la directiva de usuarios, para por intermedio de ello se pueda realizar los permiso a los empleados de acurdo a sus cargos y cuando sean tengan cualquier novedad, como vacaciones, licencias, cambio de funciones o retiro, estos sean bloqueados mientras sean reintegrados a sus labor, esto lo realiza el administrador. Procedimiento de registro/cancelación de usuarios para sistemas y servicios, autorización, verificación, dar a usuario declaración escrita de sus derechos.
A.9.2.2	Suministro de acceso de usuarios	X		El administrador del sistema asigna claves a los usuarios de acuerdo al programa que manejan.	Establecer los permisos de acceso a las aplicaciones informáticas existentes en una organización. Garantizar la operación continua de los sistemas informáticos en cualquier organización.
A.9.2.3	Gestión de derechos de acceso privilegiado	X		Se tiene establecido un formato F-SAF-01 Versión 1, de solicitud acceso servicios	

				informáticos.	
A.9.2.4	Gestión de información de autenticación secreta	X		Se Utiliza enviar toda información que transita por las redes en códigos, encriptación, el cual solo el emisor y receptor conocen la llave.	Implementar la clasificación de la documentación y por qué medio es más seguro la entrega.
A.9.2.5	Revisión de los derechos de acceso de usuarios	X		Se realiza el procedimiento de revisión/reasignación de contraseña- cambio contrato laboral - Se está prohibido el acceso, modificaciones o alteraciones no autorizada de componentes, datos o información de los activos informáticos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.	Estas reglas hay de documentarlas y firmadas por la dirección para que sea publicada a todo el personal de la empresa.

				Igualmente El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización del administrador del sistemas.	
A.9.2.6	Retiro o ajuste de los derechos de acceso		X		Se debe implementar y soportar todo proceso que se haga cuando un empleado se retire de la empresa o cualquier cambio.
A.9.3	**Responsabilidades de los usuarios**				
Objetivo	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A.9.3.1	Uso de información de autenticación secreta.	X		Casi toda la información que se envía a través de internet o correos electrónicos, se envía encriptada.	Implementar que uso del servicio de internet puede ser utilizado solamente con fines autorizados y legales. Que se prohíba toda transmisión, difusión, distribución o almacenamiento de cualquier material digital o impreso en violación de cualquier ley o regulación aplicable, estos incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio, o que constituya una amenaza ilegal.

A.9.4	**Control de acceso a sistemas y aplicaciones**				
Objetivo	Evitar el acceso no autorizado a sistemas y aplicaciones				
A.9.4.1	Restricción de acceso a la información.		X		Implementar políticas de control de acceso, prohibir a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios, aun con la autorización expresa del usuario propietario de la misma. De acuerdo a la política de control de acceso para usuarios y personal de soporte. Leer, escribir, eliminar y ejecutar.
A.9.4.2	Procedimiento ingreso seguro	X		El usuario de sistemas operativos y aplicaciones que maneja la entidad, lo hacen desde sitios seguros y sus propias estaciones de trabajo.	Implantar el no compartir sus contraseñas, poner en el sistemas de políticas de bloqueo cuando se intente acceder varia veces realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo informático.
A.9.4.3	Sistema de gestión de contraseñas	X		Se tiene implementado el uso de las contraseñas, firmas digitales o dispositivos de autenticación.	Implementar buenas practicas-uso de contraseñas, las Directivas de Contraseña: Esta política es para ayudar a mantener las cuentas de usuario seguras. Se define la frecuencia con los usuarios deben cambiar sus contraseñas, el tiempo que ha de ser, las reglas de complejidad (tipos de caracteres utilizados como letras minúsculas, mayúsculas, números y caracteres especiales), y otros artículos. Que el sistema a determinado tiempo le pida cambio de su contraseña y que esta no se repita durante unos meses.

A.9.4.4	Uso de programas utilitarios privilegios	X		Se asigna a cada usuario claves de acceso a cada módulo de los programas que se manejan.	Implementar los privilegios de los usuarios que no se asignen más de dos perfiles o permisos de los diferentes sistemas o programas, y nunca dejarlo como administrador del equipo, para que no pueda ingresar o manejar todo el sistema.
A.9.4.5	Control de acceso a códigos fuentes de programas		X		Restringir y asegurar el acceso a los códigos fuentes ya que cualquier personal, sin mucha experiencia puede llegar a dañarla información, para eso se deben hacer pruebas con el VPN y el uso de sistema de usuario remoto (acceso remoto): debe ser revisado en busca de virus /troyanos / puertas traseras. Se debe tener firewall. Control, procedimiento de control de cambio.
DOMINIO A.10	**CRIPTOGRAFÍA**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.10.1	**Controles criptográfico**				
Objetivo	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.				
A.10.1.1	Política sobre el uso de controles criptográficos	X		Se implementó la encriptación por medio de PGP, para toda la información	Implementar políticas de encriptación en medios móviles, claves, recuperación, responsabilidades.

				enviada por internet, correos electrónicos.	
A.10.1.2	Gestión de llaves	X		Se ésta periódicamente cambiando las claves y llaves de la información encriptada pública y privada.	Proteger las claves criptográficas por modificación, pérdida, destrucción. Registro y auditoria de claves.
DOMINIO A.11	**SEGURIDAD FISICA Y DEL ENTORNO**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.11.1	**Áreas seguras**				
Objetivo:	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A.11.1.1	Perímetro de seguridad	X		Se tiene definido perímetro, recepción, puertas, alarmas, separación física.	
A.11.1.2	Controles de acceso físicos	X		Se desarrolla un control al acceso a las instalaciones e información vital de los sistemas de Información de la organización.	Implementar protección física adecuada.
A.11.1.3	Seguridad de oficinas, recintos	X		Se aplica a todos los	Implementar normas de seguridad y salud, no acceso de instalaciones claves-estrategia, señales, alarmas, detectores de

	e instalaciones			recursos físicos de los Sistemas de Información: Se Protege la infraestructura del sistema de información, ubicándolos en áreas adecuadas con medidas de seguridad y controles de acceso apropiado.	humo, incendios u otro sistema.
A.11.1.4	Protección contra amenazas externas y ambientales	X		Se tiene un plan de contingencia para controlar causas ambientales que podrían alterar el buen funcionamiento de la infraestructura Informática que contiene la información de la organización.	Definir las limitaciones a los usuarios mantener la red segura como; Como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que pueden utilizar, y como pueden acceder a los datos.
A.11.1.5	Trabajo en áreas seguras	X		Se protege la infraestructura del sistema de información, ubicándolos en áreas	

				adecuadas con medidas de seguridad y controles de acceso apropiados.	
A.11.1.6	Áreas de despacho y carga	X		Se implementó acceso restringido a personal no autorizado y está definido un perímetro, recepción, puertas, alarmas, separación física.	Habilitar el área de Almacén. Separar envíos entrantes/salientes.
A.11.2	**Equipos**				
Objetivo	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección de los equipos		X		Escoger ubicación, directrices protección de no comer, beber. Medir Temperatura y humedad, pararrayo. Reducir riesgo de visual.
A.11.2.2	Servicios de suministro		X		Establecer revisión de servicios, tener UPS, planta, agua, luz, aire acondicionado, iluminación de emergencia. Hacer pruebas,
A.11.2.3	Seguridad del cableado		X		Proteger interrupciones y daños, separar cables de comunicación, rotular, tener plano del cableado.
A.11.2.4	Mantenimiento de equipos	X		Se desarrolla el plan de mantenimiento, procedimiento de realización, registro de fallas-comunicación de incidentes.	
A.11.2.5	Retiro de activos	X		Formato de autorización	

				para retirar equipos, informáticos software y su registro de T. al devolverlo identificar quienes están autorizados.	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		X		Implementar políticas para retirar portátil, PC, celulares, cámaras. Autorizar uso fuera.
A.11.2.7	Disposición segura o reutilización de equipos		X		Establecer política y procedimiento borrar información y software.
A.11.2.8	Equipos de usuario desatendido		X		Implementar protección como protector de pantalla, logout, apagar, bloqueo-contraseña.
A.11.2.9	Política e escritorio limpio y pantalla limpia		X		Implementar que toda documentación no debe estar expuesta hay que tenerla guardada en gabinetes, cerrar sesión, puntos de escritorio, correo, uso no autorizado de fotocopiadora-scanner, cámaras.
DOMINIO A.12	**SEGURIDA DE LAS OPERACIONES**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.12.1	**Procedimientos operacionales y responsabilidades**				
Objetivos	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información				
A.12.1.1	Procedimientos de operación documentados.		X		Tener procedimientos de copias, mantenimiento, manejo de información, informes especiales, manejo de medios, requisitos de programación, manejo de errores, lista de contacto de cada sistema, mantenimiento y sw, de recuperación y reinicio, eliminación segura. Gestión de registros de auditoria y del sistema.
A.12.1.2	Gestión de		X		De sistemas y servicios, TR, Identificar y registrar cambios,

	cambios				planificación, pruebas, evaluación de impacto, seguridad, aprobación de cambios. Comunicarlo. Controlar cambios en equipos, software y procedimiento. Actualización de software implica información adicional, costo, soporte, costos de mantenimiento.
A.12.1.3	Gestión de capacidad		X		Seguimiento y adaptaciones del uso de los recursos, actualizaciones, proyecciones.-capacidad futura. Para cada actividad, requisitos, negocios nuevos, tendencias
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	X		El desarrollo es responsabilidad del respectivo Jefe de Proyecto solicitar la habilitación y acceso a los distintos ambientes, mediante formulario de solicitud de Housing y Virtualización, en el Desarrollo, se dispone de herramientas como Eclipse, Java empresarial, Visual Studio. Net, Bases de datos, login, Control de versiones autorizados, Build Management,	

				administrador de código fuente, como se cuenta con un solo desarrollador se hace en el computador, son similares a los ambientes de prueba y producción.	
A.12.2	**Protección contra códigos maliciosos**				
Objetivo:	Asegúrese de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos malicioso.				
A.12.2 .1	Controles contra códigos maliciosos	X		Se tiene instalado en todas las máquinas de cómputo software antivirus, para detección y prevención para protegerse de códigos malicioso. - política de prohibición de sw pirata, procedimientos de concientización , controles de detección, prevención, recuperación.	Se tiene de establecer que se adquirirá y utilizará software únicamente de fuentes confiables y en caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

				Revisar red, correos, PC, servidores, página Web.	
A.12.3	**Copias de respaldo**				
Objetivo:	Proteger contra la pérdida de datos				
A.12.3 .1	Respaldo de la información	X		Se hacen los Bakups de la información de las estaciones de trabajo. La mayoría de la información se maneja en los softwares y en línea.	Desarrollar los procedimientos de backup y respaldo. Llevar a otro sitio, almacenamiento. Protección física, probar, encriptar.
A.12.4	**Registro y seguimiento**				
Objetivo:	Registrar eventos y generar evidencia				
A.12.4.1	Registro de eventos		X		El administrador del sistema debe de llevar una bitácora de todos los registro de los eventos presentados en los sistemas, errores y fallas.
A.12.4.2	Protección de la información de registro		X		Proteger estos registros-cambios.
A.12.4.3	Registros del administrador y del operador		X		Registro de auditoria de operador, administrador del sistema.
A.12.4.4	Sincronización de relojes		X		Tiempo Coordinado Universal (UTC). Procedimiento para verificar y corregir.
A.12.5	**Control de software operacional**				
Objetivo:	Asegurarse de la integridad de los sistemas operacionales.				
A.12.5.1	Instalación de software en sistemas operativos	X		Procedimientos instalación en SO con autorización. Sistema de Control de	Utilizar Aplicaciones de seguridad, atributos para los datos del Usuario, en los sistemas operativos, actualizaciones de los mismos.

				Configuración, política de restaurar estado anterior, registro de auditoria de actualizaciones , monitorear proveedor.	
A.12.6	**Gestión de la vulnerabilidad técnica**				
Objetivo:	Prevenir el aprovechamiento de las vulnerabilidades técnicas.				
A.12.6.1	Gestión de las vulnerabilidades técnicas		X		Implementar proceso= identificar vulnerabilidades de sistemas en uso, instalar parches.
A.12.6.2	Restricciones sobre la instalación de software	X		Esta labor solo lo hace el perfil del administrador.	Contratar para instalar programa estándar de actualizaciones.
A.12.7	**Consideraciones sobre auditorías de sistemas de información**				
Objetivo:	Minimizar el impacto de las actividades de auditorías sobre los sistemas operativos.				
A.12.7	Controles de auditorías de sistemas de información		X		Proteger el sistema operativo, documentar procedimiento.
DOMINIO A.13	**SEGURIDAD DE LAS COMUNICACIONES**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.13.1	Gestión de la seguridad de las redes				
Objetivo:	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A.13.1.1	Controles de redes	X		Utiliza el firewall, detecta los ataques a los sistemas, el servidor solo tiene abierto el puerto 80 y el	Las políticas de firewall -¿Qué puertos se deben bloquear o permitir, la forma de interactuar con ella o es propietario de ella, quien tiene acceso a la consola de control. * Inalámbrica, VPN, router y conmutador de seguridad, la retención de correo electrónico, auto remitido política de correo electrónico, la capacidad de TI para auditar y realizar la evaluación de riesgos, los algoritmos de cifrado aceptables. Igualmente no utilizar en lo

				de bases de datos. Tiene wifi y se conectan los equipos autorizados.	posible el servicio de acceso remoto de Windows.
A.13.1.2	Seguridad de los servicios de red		X		Políticas para aplicar en el área de Tecnologías de la Información, Estas políticas incluyen las condiciones generales para que estén destinados a mantener la red segura y estable.
					- Incidente de virus y de seguridad - detección de intrusiones, contención y eliminación. Preparar (políticas / procedimientos, listas de control) identificar (obtener pruebas) contenido (sacar de la red, modificar las contraseñas) erradicar (fijar, determinar la causa, mejorar las defensas, prueba para vulnerabilidades) recuperarse (validar el sistema, el monitor de re-infección) lecciones aprendidas (hacer recomendaciones para prevenir un incidente similar) * Política de copia de seguridad - Definir qué es una copia de seguridad "backup", que lo respalda, donde se almacena, ¿cuánto tiempo se almacena, cómo probar las copias de seguridad, ¿qué programa se utiliza para hacer copias de seguridad. * Políticas de actualización de clientes – Actualizar con frecuencia la información de los clientes y el uso de medios o herramientas. * Políticas de configuración del servidor, parche de actualización y modificación (seguridad) - Eliminar servicios innecesarios (servidor endurece). ¿Cuándo se determina hacer una actualización? ¿Qué se hace cuando alguien trabaja en el servidor?
A.13.1.3	Separación en la redes	X		Grupos de servicios de información, usuarios, sistemas de información. División de dominios lógicos – firewall, conmutación	El administrador debe verificar las conexiones internas, porque los empleados de una compañía pueden acceder, accidental o remotamente, a áreas de la red corporativa a las que no deberían tener acceso. Los emails pueden ser en sí mismos un foco de infección. Un correo electrónico es capaz de sustraer las credenciales de acceso de un empleado. Este robo puede ser utilizado para futuros ataques. En el caso de la seguridad del correo electrónico, identificar la fuente es clave Se debe reforzar el control de los accesos a las direcciones de alias así como recordar a los empleados las políticas de seguridad de la compañía.

				IP, red privada. Red wiki.	
A.13.2	**Transferencia de información**				
Objetivo:	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y procedimientos de transferencia e información	X		Se protege la información intercambiada, uso de comunicaciones inalámbricas, uso criptografía.	Implementar el etiquetado de soportes electrónicos, restringir acceso, registro de receptores autorizados. Proceso para manejar, procesar, almacenar, comunicar información de acuerdo a la clasificación.
A.13.2.2	Acuerdos sobre transferencia información		X		Elaboración de la política y acuerdos de confidencialidad, revisión de la ley.
A.13.2.3	Mensajería electrónica	X		Se envía la información certificada, encriptada, mediante PGP.	En el caso de la seguridad del correo electrónico, identificar la fuente es clave.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	X		Se tiene el mecanismo de encriptación, la información es solo accesible por aquellos a los cuales se ha autorizado a tener acceso.	Implementar acuerdos, notificaciones, trazabilidad.

DOMINIO A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Cumple	no cumple	que se tiene	Recomendaciones a implementar
A.14.1	**Requisitos de seguridad de los sistemas de información**				
Objetivo:	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		X		Incluir requisitos de seguridad. Proceso formal de adquisición y prueba. Requisitos en la etapa de diseño.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	X		Se tiene firewall en Servidores, autenticación, encriptación, control de conexión, procedimiento autorización.	
A.14.1.3	Protección de transa de los servicios aplicaciones	X		La empresa social del estado Fabio Jaramillo Londoño, se basa en el uso de servicios, los cuales son unidades de software que se ejecutan a través de la red.	

A.14.2.	Seguridad en los procesos de desarrollo y de soporte				
Objetivo	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	X		La Empresa, implementa la utilización del ciclo de vida al desarrollador de software, este se diseña, implementa y mantiene para protegerse contra el acceso no autorizado.	
A.14.2.2	Procedimiento de control de cambios en sistemas		X		Documentar procedimientos S.I. aprobación
A.14.2.3	Revisión Técnico de las aplicaciones después de cambios en la plataforma de operaciones		X		Procedimiento de integridad y control de aplicación, plan de revisión.
A.14.2.4	Restricciones en los cambios a los paquetes de software		X		Programa estándar de actualizaciones.
A.14.2.5	Principios de construcción de los sistemas seguros	X		La construcción se y desarrolla Implica contar con la confianza justificada en el software	

				exhibirá todas las propiedades de manera consistente y garantizará confiabilidad durante su operación a pesar de la presencia de fallas intencionales; en términos prácticos, software debe ser capaz de resistir la mayoría de los ataques, tolerar tanto como resulte posible aquellos ataques que no pueden resistir.	
A.14.2.6	Ambiente de desarrollo seguro	X		Se implementa bajo los parámetros de, Confiabilidad, Protección, Seguridad.	Hay que adicionar las prácticas relacionadas con la gestión del riesgo para garantizar la calidad del software seguro
A.14.2.7	Desarrollo contratado externamente		X		El proceso de desarrollo de software lo debe realizar un profesional con suficiente conocimientos. Realizar pruebas en la parte de desarrollo del software.
A.14.2.8	Pruebas de seguridad de sistemas		X		Autorizar la copia de prueba, borrar, rastro de auditoria.
A.14.2.9	Prueba de		X		Establecer criterios de aceptación de nuevos sistemas,

	aceptación de sistemas				actualizaciones, nuevas versiones, pruebas.
A.14.3	**Datos de prueba**				
Objetivo:	Asegurar la protección de los datos usados para pruebas				
A.14.3.1	Protección de datos de prueba		X		Autorizar la copia de prueba, borrar, rastro de auditoria.
DOMINIO A.15	**RELACIONES CON LOS PROVEEDORES**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.15 .1	**Seguridad de la información en las relaciones con los proveedores**				
Objetivo	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores				
A.15 .1.1	Política de seguridad de la información para las relaciones con proveedores	X		Se tiene implementado en línea a través de la red toda la información, con los proveedores y encriptada.	
A.15 .1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	X		Se utiliza siempre la autenticación de la información.	Aplicar las políticas y acuerdos de confidencialidad, revisión de la ley.
A.15 .1.3	Cadena de suministro de tecnología de información y comunicación		X		Muchos de ellos no son adquiridos con licencias, se utilizan software libre, esto hace más frágil la comunicación.

A.15 .2	Gestión de la prestación de servicios de proveedores				
Objetivo:	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A.15 .2.1	Seguimiento y revisión de los servicios de los proveedores		X		Se debe implementar seguimientos a los soportes de todos los proceso de los servicios prestados a los proveedores.
A.15 .2.2	Gestión de cambios en los servicios de los proveedores		X		La gestión de los sistemas y servicios, Identificar y registrar cambios, planificación, pruebas, evaluación de impacto, seguridad, aprobación de cambios. Comunicarlo. Controlar cambios en equipos, software y procedimiento. Actualización de software implica información adicional, costo, soporte, costos de mantenimiento.
DOMINIO A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**				
Objetivo	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A.16.1.1	Responsabilidades procedimientos		X		Se debe documentar, mantener, estar disponibles.
A.16.1.2	Reporte de eventos de seguridad de la información		X		Procedimiento de reporte de eventos al punto de contacto, disciplinario, coacción.
A.16.1.3	Reporte de debilidades de seguridad de la información		X		Exigir a los empleados, contratistas y usuarios.

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		X		Implementar seguimiento a los reportes sobre los eventos de seguridad de la información, Cantidad, monitorear, volúmenes, medir impacto, recurrentes, evaluación.
A.16.1.5	Respuesta a incidentes de seguridad de la información		X		Se debe establecer en el menor tiempo posible, tener copia de respaldo y contar con un servidor espejo.
A.16.1.6	Aprendizaje obtenido incidentes de seguridad información		X		Cantidad, monitorear, volúmenes, medir impacto-recurrentes-evaluación.
A.16.1.7	Recolección de evidencias		X		Recolectar, retener y presentar evidencias.
DOMINIO A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.17.1	Continuidad de seguridad de la información				
Objetivo	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	X		Cada plan-dueño, servicios de procesamiento de información y comunicación,	

				proveedores	
A.17.1.2	Implementación continuidad de la seguridad de la información	X		Responsabilidad, procedimiento para recuperar y restaurar las operaciones del negocio,	
A.17.1.3	Verificación, revisten y evaluación de la continuidad de la seguridad de la información		X		Eventos que ocasionan interrupciones en los procesos del negocio
A.17.2	**Redundancias**				
Objetivo	Asegurar la disponibilidad de instalaciones de procesamiento de información				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		X		Mantener el sistema operativo actualizado en todas las máquinas que se utilizan para la realización de los procedimientos de la información de la entidad.
DOMINIO A.18	**CUMPLIMIENTO**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.18.1	**Cumplimiento de requisitos legales y contractuales**				
Objetivo	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		X		Hacer resumen de normatividad y actualizarlo
A.18.1.2	Derechos de propiedad intelectual		X		Implementar procedimiento para cumplir DPI.
A.18.1.3	Protección de	X		Se tiene	

	registros			implementado la protección de estos registros-cambios	
A.18.1.4	Privacidad y protección de información de datos personales		X		Establecer las clausulas -controles a la recolección, procesamiento y transmisión de datos personales.
A.18.1.5	Reglamentación de controles criptográficos		X		Controles criptográficos deben cumplir la Ley.
A.18.2	**Revisiones de seguridad de la información**				
Objetivo	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A.18.2.1	Revisión independiente de la seguridad de la información		X		Implementar el plan de revisión de política con cambios, revisión independiente, partes interesadas, acciones preventivas-correcciones, revisiones previas, tendencias amenazas, incidentes, recomendaciones.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	X		Procedimiento, Formato para registrar el cumplimiento.	
A.18.2.3	Revisión del cumplimiento técnico		no cumple		Verificar para que cumplan con la norma.

Fuente Autor Proyecto

Autor: El desarrollo del diseño de un Modelo de un Sistema de Gestión de Seguridad de la Información para el área de sistemas para la Empresa Social del Estado Fabio Jaramillo Londoño con lineamientos de la norma ISO/IEC 27001:2013, fue llevado a cabo por la profesional Mercedes Sarria Cuéllar.

9 DISEÑO DEL PLAN DE IMPLEMENTACIÓN DEL SGSI

9.1 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Para el cumplimiento del dominio de políticas de la seguridad de la información, se hace necesario que la gerencia debe implementar, documentar las políticas de la seguridad de la información, publicarlas y socializarlas con todo el personal de la Empresa Social del Estado Fabio Jaramillo Londoño, debido a que no existen y teniendo en cuenta su objetivo de estas políticas de seguridad es definir qué están haciendo los usuarios con la información de la empresa, se deberá hacer un buen uso de los recursos de hardware y software y por su puesto enfatizar los costos, con esto se podrá garantizar la confidencialidad, integridad y disponibilidad de los sistemas de Información, debido a que:

- Es una necesidad primaria que se debe abordar y poner en conocimiento la responsabilidad de la Dirección.
- Implementar auditorías a los sistemas de información.
- Establecer y documentar las políticas de seguridad de la información en la Empresa.

Las políticas son la fase inicial para la implementación del sistema de seguridad y se debe tener muy en cuenta:

- Políticas de tecnología de la información: Definir las políticas del departamento de tecnologías de la información utilizada para regir la red, para obtener la máxima seguridad y estabilidad.

- Condiciones Generales: Las políticas de alto nivel para determinar quién es responsable de las políticas, junto con la planificación y las políticas de la continuidad de la empresa.

- Directivas de usuario: Definir lo que los usuarios pueden y deben hacer para usar su red y equipos informáticos de la organización. Definir los limitaciones a los usuarios mantener la red segura como; Como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que pueden utilizar y cómo pueden acceder a los datos. Algunas políticas incluyen:

- Directivas de contraseña: Esta política es para ayudar a mantener las cuentas de usuario seguras. Se define la frecuencia con los usuarios deben cambiar sus contraseñas, el tiempo que ha de ser, las reglas de complejidad (tipos de caracteres utilizados como letras minúsculas, mayúsculas, números y caracteres especiales), y otros artículos.

- Información de uso Propietario: Uso aceptable de cualquier información confidencial propiedad de la empresa. Define donde puede ser almacenada y donde se puede tomar, cómo y dónde se puede transmitir.

- Uso de Internet: Uso del correo de electrónico, Uso de programas con contraseñas y/o encriptar los datos enviados a través de Internet.

- VPN y el uso de sistema de usuario remoto (acceso remoto): debe ser revisado en busca de virus /troyanos / puertas traseras. Se debe tener firewall.

- El uso aceptable de hardware, tales como módems: No usar módems de Internet personal sin un firewall.

Estas políticas de seguridad de la información incluyen las condiciones generales para que estén destinados a mantener la red segura y estable de la empresa, por lo tanto de debería aprobar estas políticas de seguridad de la información en la empresa.

- Para mitigar los Incidente de virus y de seguridad en la detección de intrusiones, contención y eliminación.

- Preparar las políticas, los procedimientos y las listas de control, modificar las contraseñas, realizar pruebas de vulnerabilidades.

- Recuperarse en el menor tiempo posible el servicio en caso de un incidente, validar el sistema.

- Aplicar políticas para un copia seguro de la información.

- Realizar "backup", que respalde la información que se maneja en la empresa y se debe almacenar en un lugar seguro y distante del sitio del centro de cómputo,

- Implementar las políticas de actualización de clientes y a la vez esta actualizarla con frecuencia.

- Establecer políticas de configuración del servidor, parche de actualización y modificación. Eliminar servicios innecesarios.

- Tener en cuenta en las políticas de firewall, que puertos se deben permitir o bloquear y la forma de interactuar con ella o es propietario de ella, y solo deberá acceder quien tiene el permiso de acceso a la consola de control.

- Establecer políticas del uso de la información por medio de los correos electrónicos.

9.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para el dominio de la organización de la seguridad de la información, se hace necesario asignar al personal de acuerdo a sus funciones roles y responsabilidades con el resguardo de la información que manejan. Dar a conocer a los empleados sobre la Ética profesional.

- Debe existir contacto apropiado y buenas relaciones, con los superiores, demás organismos del estado y acatar órdenes, en cuanto al cuidado y tratamiento de la información.

- Consultar a especialistas de la seguridad para ejecutarla en toda las oficinas.

- Es deber de la dirección apoyar activamente en la evaluación periódicamente de la seguridad de la información de cualquier proyecto implementado o a desarrollar.

- Implementar seguridad de telefonía móvil, restricciones al ingreso a internet, encriptar la información. Controlar, bloquear, encriptar códigos móviles.

- Si la información de hace física, tener el envío con empresas con seguridad y reservado. Igualmente, se debe desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

Son responsabilidades de los funcionarios, servidores, contratistas y terceros la Empresa Social del Estado Fabio Jaramillo Londoño:

- Del buen uso de los elementos y de la información que reposan en ellos.

- Deben tomar conciencia de la aplicabilidad de las políticas de la información.

- Utilizar formatos establecidos para cada proceso, mediante la tabla de retención documental y dar cumplimiento a lo establecido en la Ley 594 de 2000; por medio del cual se establecen las reglas y principios generales que rigen la función archivística del Estado.

Son responsabilidades de los directivos de la Empresa Social del Estado Fabio Jaramillo Londoño:

- Realizar seguimientos en su entorno de control estratégico, apoyo al equipo MECI, dinámico que conoce sus funciones dentro de la aplicación, mantenimiento y fortalecimiento del modelo. Además, el comité coordinador de Control Interno se encuentra activo, desarrollando las reuniones correspondientes para tratar los temas relacionados, dejando evidencias de las mismas.

- Socializando la plataforma estratégica de la empresa en el cual se encuentra inmersa la Misión, Visión y objetivos institucionales alineados a la política administrativa de la entidad.

- Socializar el proceso de inducción y re inducción de la institución, código de ética y valores que contiene los principios y valores, adoptado mediante Resolución No.0754 del 18 de junio de 2009.

- Socializar y evaluar anualmente el plan de desarrollo, aprobado por la junta directiva. Contiene programas y proyectos enmarcados en las necesidades y expectativas de los usuarios, a quienes se orienta la prestación del servicio de salud.

- Implementar controles para los riesgos practicados en los distintos procesos; como guía para garantizar su aplicación y los posibles ajustes que se estimen convenientes para contribuir en la mejora de los mismos.

- Seguimiento de la actualización de la política de administración de riesgos y su plan de manejo, que incluye la metodología a utilizar para el desarrollo de las acciones; el mapa de riesgos por procesos y el mapa institucional de riesgos.

- La dirección determina los responsables del monitoreo y seguimiento a los mapas de riesgo y la periodicidad de seguimiento, de acuerdo a los niveles de riesgo residual.

- Llevar los proceso de autoevaluación institucional se desarrolla en los procesos prioritarios de la Empresa Social del Estado Fabio Jaramillo Londoño; con los cuales se elaboran los informes correspondientes según resoluciones 1043,1441 y 2003 de 2014. Se socializa con los funcionarios los temas tratados, levantando las actas pertinentes y se llevan a cabo los comités requeridos con las evidencias y registro de participantes.

- Socialización de manuales, guías, protocolos modificados por cambios en normatividad o ajustes en los procesos

- Apoyo al sistema de control interno para que se encuentre activo en la Empresa Social del Estado Fabio Jaramillo Londoño

Son responsabilidades del Área de sistemas:

- Realizar las actualizaciones en el Modulo de Inventarios, nomina, presupuesto y contabilidad del software de SIIGO.

- Mantener actualizada la página web brindando la información de interés al público en general para su consulta y demás fines pertinentes de la Empresa Social del Estado Fabio Jaramillo Londoño.

- Servir de enlace con las entidades externas contratadas para los servicios de los medios de comunicación como Internet y comunicación telefónica vía celular, obstaculiza el permanente flujo de información con las áreas internas y entidades externas relacionadas; afectando la comunicación interna y externa en el desarrollo de las actividades institucionales

- Realizar las actualizaciones de los Software de los sistemas de información, las licencias de Microsoft Office y antivirus para que permitan la protección de los softwares utilizados y la optimización de los procesos institucionales.

- Realizar controles en el ingreso de equipos de cómputo personales, elementos de USB, discos extraíbles.

9.3 SEGURIDAD DE LOS RECURSOS HUMANOS

Para el dominio de seguridad de los recursos humanos, se hace necesario desarrollar una política de seguridad para todos los usuarios de la empresa, que deben recibir entrenamiento apropiado en políticas, procedimientos organizacionales y socializar con claridad el manual de funciones para su con su labor y los cuidados a que tiene con los activos de la empresa, en cuanto a la información que va a manejar. Capacitar al personal sobre seguridad de la información sobre las amenazas, riesgos y vulnerabilidades.

- Establecer primero que todo las políticas de seguridad en la empresa, para ser difundida y concientizar a los empleados, de la importancia de la seguridad de la información. Dar a conocer los reglamentos de ética profesional. La empresa tiene que ofrecer unos planes de formación continua, promoviendo el desarrollo de una carrera profesional de sus empleados. Estos planes de formación han de incluir todos los temas básicos para el desarrollo de su trabajo (leyes aplicables, seguridad, prevención de riesgos laborales, metodologías, tecnologías y conocimientos funcionales).
- La falta de concientización de los usuarios, esto no es diferente de otras plataformas, sin embargo, un factor en algunos escenarios de riesgo. Por ejemplo, la divulgación no intencional de datos a menudo se basa en la falta de conciencia de los usuarios de las implicaciones que trae el consentimiento a la divulgación de datos.
- Se debe dar a conocer a los usuarios internos de la legislación sobre los delitos informáticos y sus las penalidades en caso de fraude, robo o fuga de información, daño o sabotaje informático.

- Debe existir, documentación, actas tanto para la entrega y/o recibo de bines de la empresa, se debe hacer la inducción al puesto de trabajo a cada empleado.

9.4 GESTIÓN DE ACTVIOS

Para el dominio de la gestión de activos, se hace necesario desarrollar una política para la seguridad de gestión de los activos, con medidas que mitiguen el riesgo y eviten que las amenazas afecten el buen funcionamiento de los mismos para así garantizar la calidad de los servicios de los sistemas de información en la empresa.

- Se debería ejecutar el levantamiento total de inventarios de los activos que cuenta la empresa, por parte del encargado área de sistemas, clasificándolos por niveles, manteniendo un inventario de activos definidos, relación de los riesgos con tipo de activos, mantener registros de personas con sus capacitaciones y realizar las hojas de vida de cada elemento de cómputo.

- Se debería realizar la individualización de los activos físicos y dejando soporte, al igual de las responsabilidades del cuidado de los mismos, por parte del contratado para el área de sistemas.

- Implementar reglas para el uso aceptable de los activos informáticos de la Empresa Social del Estado Fabio Jaramillo Londoño, implica la aceptación por parte de los usuarios, de las normas, políticas y estándares establecidos para garantizar la seguridad informática. Este trámite de sebe

estandarizar según las normas de calidad, para el cuidado, buen manejo y entrega definitiva de los activos.

- Estandarizar en el documento impreso, en la plantilla membretado de la Empresa de toda la información, ya sea secreto o reservado.

- Establecer normas y políticas del Ministerio del Interior sobre seguridad y uso de los sistemas de tratamiento de información, de las redes y del correo electrónico, secreto o reservado.

- Implementar política y gestión para el manejo de Activos Fijos.

- Diligenciar la información que se solicita en el formato del equipo usado antes de realizar el borrado, verificar en la hoja de vida que se solicita en este formato es el mismo de la placa que determine en el PC.

- Es responsabilidad del área de tecnología e informática disponer de medios seguros para que los funcionarios que posean notebooks accedan a la información.

- Implementar políticas de usuario.

9.5 CONTROL DE ACCESO

Desarrollar e implementar política de control de acceso de la seguridad informática y atendiendo la legislación aplicable: Para así asegurar que en la empresa, la información está protegida contra divulgación a usuarios no autorizados (confidencialidad), modificación inapropiada (integridad) y al no acceso cuando se

requiere (disponibilidad). Asimismo establecer, documentación y revisar reglas y derechos de cada usuario int/ext en servicios, sistemas y requisitos de seguridad de software.

- Los primeros elementos que se deben definir son las políticas relacionadas con el uso y manejo y de sus datos. Esto le ayudara a determinar las medidas y procedimientos de defensa.

- Procesos de autorización uso de redes y servicios.

- Crear políticas de directivas de usuario. Definir lo que los usuarios pueden y deben hacer para usar su red y equipos informáticos de la organización.

- Definir las limitaciones a los usuarios mantener la red segura como; Como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que pueden utilizar, y cómo pueden acceder a los datos.

- Se debería crear la directiva de usuarios, para por intermedio de ello se pueda realizar los permiso a los empleados de acurdo a sus funciones de trabajo y tener presente las novedades del personal, vacaciones, licencias, cambio de funciones o retiro, estos sean bloqueados mientras sean nuevamente reintegrados a sus labor, esto lo realiza el administrador.

- Se debería realizar procedimiento de registro/cancelación de usuarios para sistemas y servicios, autorización, verificación, dar a usuario declaración escrita de sus derechos.

- Establecer los permisos de acceso a las aplicaciones informáticas existentes en una organización. Garantizar la operación continua de los sistemas informáticos en cualquier organización.

- Implementar la clasificación de la documentación y por qué medio es más seguro la entrega.

- Estas reglas hay que documentarlas y firmadas por la dirección para que sean publicadas a todo el personal de la empresa.

- Se debería implementar y soportar todo proceso que se haga cuando un empleado se retire de la empresa o cualquier cambio.

- Implementar el uso del servicio de internet puede ser utilizado solamente con fines autorizados y legales, que se prohíba toda transmisión, difusión, distribución o almacenamiento de cualquier material digital o impreso en violación de cualquier ley o regulación aplicable, esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio, o que constituya una amenaza ilegal.

- Implementar políticas de control de acceso, prohibir a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios, aun con la autorización expresa del usuario propietario de la misma. De acuerdo a la política de control de acceso para usuarios y personal de soporte. Leer, escribir, eliminar y ejecutar

- Implantar el no compartir sus contraseñas ya que estas son personales e intransferibles, instalar en el sistema una política de bloqueo que cuando se

intente acceder varia veces a realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo informático.

- Implementar los privilegios de los usuarios que no se asignen más de dos perfiles o permisos de los diferentes sistemas o programas, y nunca dejarlo como administrador del equipo, para que no pueda ingresar o manipular todo el sistema.

- Restringir y asegurar el acceso a los códigos fuentes ya que cualquier personal, sin mucha experiencia puede llegar a dañarla información, para eso se deben hacer pruebas con el VPN y el uso de sistema de usuario remoto (acceso remoto): debe ser revisado en busca de virus /troyanos / puertas traseras. Se debe tener firewall, control y procedimiento de control de cambio.

- Implementar buenas prácticas y uso de contraseñas, las directivas de contraseña: Esta política de seguridad la debe conservar cada uno de los usuarios de equipos de cómputo de la empresa y las responsabilidades que adquiere para ofrecer seguridad a la información existente en la red de datos de la empresa, es para ayudar a mantener las cuentas de usuario son entre otras:

- El usuario y el password otorgado son personales e intransferibles, por tal razón no pueden ser compartidos, cedidos o entregados a terceros.

- La fuga de datos, pérdida o alteración de los mismos y en general toda la información a que sea manipulada a través del usuario, será únicamente responsabilidad del funcionario a quien se le asignó el mismo con las

consecuencias disciplinarias, administrativas y/o penales que fuera del caso.

- La utilización del usuario deberá hacerse desde computadores y equipos de la empresa asignados, salvo los casos excepcionales autorizados (VPN, comisiones en otras entidades, etc.)

- En el caso de las VPN, el funcionario debe asegurarse de cerrar la sesión una vez finalice la actividad a realizar y, conservar las medidas que considere necesarias para evitar que se ponga en riesgo la confidencialidad de su clave de acceso.

- Los usuarios deben cumplir con las siguientes recomendaciones:
- a. Cambiar el password mínimo cada 30 días
- b. Si cree que alguien diferente a usted conoce el password, cámbielo inmediatamente.
- c. Utilice siempre una combinación de diez (10) caracteres entre números, letras y símbolos; este tipo de combinación la ofrece mayor seguridad.

- El nombre del usuario y el password, no deben ser escritos en agendas, libros, post-it, por tal razón se recomienda memorizarlos para evitar que alguien encuentre esta información y acceda a la red con sus roles.

- Si por algún motivo el titular del usuario es trasladado, retirado, enviado a comisión o vacaciones, es su obligación y la de su superior inmediato coordinar la suspensión o cancelación del usuario, de lo contrario éste seguirá habilitado y cualquier manipulación de la información que se realice con el mencionado, continuará siendo responsabilidad del titular.

- No está permitida la utilización e instalación de modem inalámbricos de internet de cualquier operador tanto personales como los entregados por empresa, teniendo en cuenta que estos elementos vulneran enormemente la seguridad de la red de datos de la empresa al abrir una red pública paralela a la red de la empresa por donde cualquier HACKER y/o personas inescrupulosas puede ingresar.

- No se debe dejar información confidencial o delicada en oficios impresos, en lugares de fácil acceso o visibilidad de personas ajenas a esta información.

- Evitar realizar impresiones en hojas recicladas que contengan información reservada esta información si ya no es útil deberá ser destruida.

- Evitar la utilización de medios extraíbles y/o memorias USB para traslado de información sensible, ya que al extraviarse se pierde la información y puede ser utilizada por cualquier persona, en lo posible utilizar correos electrónicos para envío de esta información.

- Siempre que se vaya a ausentar de su puesto de trabajo bloquee su usuario evitando así que su equipo sea manipulado por personas ajenas.

La empresa se deberá comprometer a salvaguardar sus activos de información, protegiéndolos a través de una adecuada gestión del riesgo, el cumplimiento de los requisitos legales y una estrategia de seguridad basada en las mejores prácticas y controles, con el fin de proteger los activos de información de las amenazas que se ciernen sobre ellos.

- Normas de escritorios y pantallas limpias: Estas normas tienen como fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, para lo cual se establecen las siguientes pautas:

- Tratamiento de documentos e información: o almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral o guardar bajo llave la información clasificada en nivel 3 o superior (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso.

- Bloquear la sesión de los computadores cuando no se están usando. El protector de pantalla se activará en forma automática después de cinco (5) minutos de inactividad y con solicitud de contraseña.

- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

- Bloquear las fotocopiadoras fuera del horario normal de trabajo.

- Retirar inmediatamente la información sensible, una vez impresa.

- El escritorio de los equipos de cómputo no deberán tener accesos directos a archivos.

9.6 CRIPTOGRAFÍA

Para el dominio de criptografía, se hace necesario desarrollar una política para que se establezca recomendar a los usuarios internos y externos de la empresa,

el uso del cifrado conforme la norma actual para las claves públicas y privadas en el manejo de información enviada confidencial.

- Implementar políticas de encriptación en medios móviles, claves, recuperación, responsabilidades.
- Proteger las claves criptográficas por modificación, pérdida, destrucción. Registro y auditoria de claves.
- Implementar controles y asignar los derechos de acceso a los usuarios por medio de claves criptográficas en la telefonía móvil, restricciones al ingreso a internet, encriptar la información. Controlar, bloquear, encriptar códigos.

9.7 SEGURIDAD FISICA Y DEL ENTORNO

Para el dominio de seguridad física y del entorno, se hace necesario desarrollar, implementar una política para protección física adecuada con restricciones de control de acceso a los centros de cómputo e instalaciones, al igual a la información vital de los sistemas de Información de la organización.

- Implementar normas de seguridad y salud, no acceso de instalaciones claves, estrategia, señales, alarmas, detectores de humo, incendios u otros sistemas.
- Se debería definir las limitaciones a los usuarios mantener la red segura como; como evitar instalar programas en sus estaciones de trabajo, los tipos de programas que pueden utilizar, y como pueden acceder a los datos
- Se debería habilitar el área de almacén, separar envíos entrantes/salientes, escoger su ubicación.
- Establecer directrices de protección de no comer, beber, medir temperatura, humedad, pararrayo y reducir riesgo visual.

- Realizar revisión de servicios, tener UPS, planta, agua, luz, aire acondicionado, iluminación de emergencia y hacer pruebas.

- Establecer políticas de protección, interrupciones y daños; separar cables de comunicación, rotular, tener plano del cableado.

- Implementar políticas para retirar portátil, PC, celulares, cámaras y la autorización del uso fuera de la empresa.

- Establecer política y procedimiento borrar información y software.

- Implementar protección como protector de pantalla, logout, apagar, bloqueo con contraseña.

- Implementar que toda documentación no debe estar expuesta hay que tenerla guardada en gabinetes con llave, cerrar sesión, puntos de escritorio, correo, uso no autorizado de fotocopiadora, scanner, cámaras.

9.8 SEGURIDAD DE LAS OPERACIONES

Implementar y socializar para el dominio de seguridad de las operaciones, se hace necesario desarrollar una política para la seguridad de las instalaciones, las cuales las deberían conocer todos los usuarios como los procedimientos de copias, mantenimiento, manejo de información, informes especiales, manejo de medios, requisitos de programación, manejo de errores, lista de contacto de cada sistema, mantenimiento y software de recuperación, reinicio, eliminación segura y gestión de registros de auditoria y del sistema.

- Identificar y registrar cambios, planificación, pruebas, evaluación de impacto, seguridad, aprobación de cambios. Comunicarlo. Controlar cambios en equipos, software y procedimiento. Actualización de software implica información adicional, costo, soporte, costos de mantenimiento de sistemas y servicios, TR.

- Seguimiento y adaptaciones del uso de los recursos, actualizaciones, proyecciones, capacidad futura para cada actividad, requisitos, negocios nuevos, tendencias.

- Se debería establecer que se adquirirá y utilizará software únicamente de fuentes confiables y en caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

- Desarrollar los procedimientos de backup y respaldo, llevarlo a otro sitio de almacenamiento. Protección física, probar, encriptar.

- El administrador del sistema debe de llevar una bitácora de todos los registro de los eventos presentados en los sistemas, errores y fallas.

- Proteger estos registros, cambios.

- Registro de auditoria de operador, administrador del sistema.

- Tiempo coordinado universal (UTC), procedimiento para verificar y corregir.

- Se debe utilizar aplicaciones de seguridad, atributos para los datos del usuario, en los sistemas operativos, actualizaciones de los mismos.

- Implementar proceso = identificar vulnerabilidades de sistemas en uso, instalar parches.

- Se debería contratar para instalar programas estándar de actualizaciones.
- Establecer la protección del sistema operativo, documentar procedimiento.

9.9 SEGURIDAD DE LAS COMUNICACIONES

Implementar para el dominio de seguridad de las comunicaciones, se hace necesario desarrollar una política de firewall, para establecer qué puertos se deben bloquear o permitir y dar a conocer a todos los usuarios la forma de interactuar con ella o si es propietario de ella, quien tiene acceso a la consola de control a la VPN, router y conmutador de seguridad, la retención de correo electrónico, auto remitido política de correo electrónico, la capacidad de TI para auditar y realizar la evaluación de riesgos, los algoritmos de cifrado aceptables. Igualmente no utilizar en lo posible el servicio de acceso remoto de Windows.

- Establecer políticas para aplicar en el área de tecnologías de la Información, estas políticas incluyen las condiciones generales para que estén destinados a mantener la red segura y estable.

- Realizar políticas de actualización de clientes – Actualizar con frecuencia la información de los clientes y el uso de medios o herramientas.

- Implementar políticas de configuración del servidor, parche de actualización y modificación (seguridad). Eliminar servicios innecesarios (servidor endurece).

- Se debería desarrollar por parte del administrador la verificación de las conexiones internas, porque los empleados de una compañía pueden acceder, accidental o remotamente, a áreas de la red corporativa a las que no deberían tener acceso. Los emails pueden ser en sí mismos un foco de

infección, un correo electrónico es capaz de sustraer las credenciales de acceso de un empleado, este robo puede ser utilizado para futuros ataques, en el caso de la seguridad del correo electrónico identificar la fuente es clave, se debe reforzar el control de los accesos a las direcciones de alias así como recordar a los empleados las políticas de seguridad de la compañía.

- Implementar el etiquetado de soportes electrónicos, restringir acceso, registro de receptores autorizados, proceso para manejar, procesar, almacenar, comunicar información de acuerdo a la clasificación.

- Elaboración de la política y acuerdos de confidencialidad, revisión de la ley.
- Implementar acuerdos, notificaciones, trazabilidad.

9.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTMAS

La empresa debe desarrollar e implementar políticas para el dominio de adquisición, desarrollo y mantenimiento de sistemas, se hace necesario desarrollar una política en la realización de pruebas de datos estos deben ser seleccionados cuidadosamente, protegidos y controlados, considerar que la actualización de librerías de programa operativos, los sistemas deben tener solo código ejecutable y compiladores, el profesional que lo realiza debe ser capacitado y estableciendo las mejores alternativas para mitigar los riesgos en la información confidencial y la no confidencial.

- Se debería Incluir requisitos de seguridad, proceso formal de adquisición y prueba, requisitos en la etapa de diseño.
- Realizar la documentación de los procedimientos S.I. aprobación.

- Establecer procedimiento de integridad y control de aplicación, plan de revisión.

- Instalar programa estándar de actualizaciones.

- Implementar la realización de las prácticas relacionadas con la gestión del riesgo para garantizar la calidad del software seguro.

- Autorizar la copia de prueba, borrar, rastro de auditoria.

- Establecer criterios de aceptación de nuevos sistemas, actualizaciones, nuevas versiones, pruebas.

Partiendo de que la Empresa Social de Estado Fabio Jaramillo Londoño cuenta con el sistema operativo Windows Server 2008 R2 en el servidor, se definen los siguientes niveles de usuarios, los cuales deben ser creados dentro del Active Directory para el control de acceso:

- Crear los grupos dentro del Active Directory.
- Crear las políticas de seguridad dentro de la GPO (Group Policy Object – Objeto de Directivas de grupo) para controlar el acceso a los sistemas operativos.
- Crear los usuarios y equipos en el árbol de Active Directory.
- Vincular los usuarios a los grupos.
- Vincular los grupos a sus respectivas GPO.
- Los equipos deben quedar bloqueados para su acceso local con un usuario administrativo y una contraseña robusta.

Se recomienda a la empresa que se debería realizar los siguientes requerimientos para el mantenimiento y soporte de los equipos informáticos. (Ver Tabla 7)

9.11 RELACIONES CON LOS PROVEEDORES

Para el dominio de relación con los proveedores, que se hace necesario desarrollar políticas de autenticación adicionalmente el certificado digital, para algunos usuarios críticos, acuerdos de confidencialidad, revisión de la ley, con los proveedores, contratistas y demás usuarios.

- Se debe implementar seguimientos a los soportes de todos los proceso de los servicios prestados a los proveedores.

- La gestión de los sistemas y servicios, identificar y registrar cambios, planificación, pruebas, evaluación de impacto, seguridad, aprobación de cambios, se debe comunicar.

- Controlar cambios en equipos, software y procedimiento. Actualización de software implica información adicional, costo, soporte, costos de mantenimiento, muchos de ellos no son adquiridos con licencias, se utilizan software libre, esto hace más frágil la comunicación.

9.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para el dominio de gestión de incidentes de seguridad de la información, se hace necesario desarrollar, implementar políticas de seguimiento a los reportes de incidentes sobre los eventos de seguridad de la información, con el fin de asegurar una gestión efectiva de incidentes, de monitoreo y evaluación bien sea de manera reactiva o proactiva en la seguridad de la información.

- Debería de existir un control de responsabilidades y que se establezcan procedimientos para asegurar una rápida recuperación.

- La implementación de un mecanismo que permita que los tipos de costos de los incidentes en la seguridad de la información sean cuantificados y monitoreados.

- Se debe documentar, mantener, estar disponibles.

- Realizar procedimiento de reporte de eventos al punto de contacto, disciplinario, coacción, exigir a los empleados, contratistas y usuarios.

- Se debe restablecer el servicio en el menor tiempo posible, tener copia de respaldo y contar con un servidor espejo.

9.13 ASPECTOS DE SGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO

Para el dominio de aspectos de seguridad de la información de la gestión de continuidad de negocio de acuerdo a la prioridad del evento, es necesario implementar un plan de recuperación del servicio para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas tras la interrupción y garantizando la seguridad del personal, la protección de los servicios y tener procesos de continuidad del negocio. El plan de continuidad del negocio estará alineado con la Norma ISO 27001: 2013.

- Se debe tener identificado todos los activos implicados en los procesos críticos de la empresa.

- Realizar la identificación de los eventos que puedan causar interrupciones a los procesos operativos junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias.

- Establecer responsabilidad, procedimiento para recuperar y restaurar las operaciones del negocio.

- Reconocer los eventos que ocasionan interrupciones en los procesos del negocio.

Plan de continuidad de negocios - Incluye los siguientes planes:

- Gestión de Crisis - ¿Qué hacer durante la crisis (cualquiera) que pueda poner en peligro la organización?
- Recuperación de Desastres – Sub funciones:
- Recuperación del servidor
- La recuperación de datos
- Recuperación de usuario final
- Plan de respuesta de emergencia
- Recuperación del espacio o lugar

9.14 CUMPLIMIENTO

Para el dominio de cumplimiento, se hace necesario desarrollar una política para el cumplimiento de las políticas y normas y estándares de seguridad implantadas en la empresa en los procesos de tecnología de la información, ya que es de carácter obligatorio tener presente la legislación que aplica en los procesos que intervienen en el manejo de la información.

- Se debería implantar seguridad en los sistemas de información, con la finalidad de asegurar el cumplimiento.

- Realizar resumen de normatividad y actualizarlo.
- Establecer las clausulas -controles a la recolección, procesamiento y transmisión de datos personales.
- Implementar controles criptográficos deben cumplir la Ley.
- Implementar el plan de revisión de política con cambios, revisión independiente, partes interesadas, acciones preventivas-correcciones, revisiones previas, tendencias amenazas, incidentes, recomendaciones.
- Verificar para que cumplan con la norma.
- Se realiza un modelo del plan maestro para la implementación de un sistema de gestión de seguridad de la información (SGSI) (Ver Anexo 17)

Autor: El desarrollo del Diseño del Plan Implementación de un Sistema de Gestión de Seguridad de la Información para el área de sistemas para la Empresa Social del Estado Fabio Jaramillo Londoño con lineamientos de la norma ISO/IEC 27001:2013, fue llevado a cabo por la profesional Mercedes Sarria Cuéllar.

10 PLAN DE CONTINGENCIA INFORMATICO PARA LA EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO EN EL ÁREA DE SISTEMAS

Para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO es necesario acudir a los recursos de Tecnología de la información como un medio para proporcionar los servicios que la empresa brinda a los usuarios y de vital importancia que dicha información sea lo más exacta posible, lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia Informático en el Área de Sistemas.

Es importante resaltar que para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones. Este Plan de Contingencias, es necesario que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños producidos por hechos naturales o producidos por los hombres, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

En este documento se resalta la necesidad de contar con estrategias que admitan ejecutar, Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y Recuperación para enfrentar algún desastre.

Se entiende por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior, habiendo reemplazado o recuperado el máximo posible de los recursos e información".

INTRODUCCION

Para plasmar el Plan de contingencia informático de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, se tiene que la información de toda la organización, constituye el núcleo de la misma, es su activo más valioso, entenderemos como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio bajo su responsabilidad. Entenderemos también como procedimiento relevante a la infraestructura informática a todas aquellas tareas que su personal realiza frecuentemente cuando interactúa con la plataforma informática (entrada de datos, generación de reportes, consulta, etc.). El plan está orientado a establecer, junto con trabajos de seguridad, un sistema de seguridad física y lógica en previsión de desastres.[11]

Es importante resaltar que para la Empresa Social del Estado FABIO JARAMILLO LONDOÑO logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá mantener una productividad eficiente en todas las áreas operativas; así mismo es necesario, por tanto, prever cómo y qué recursos necesitamos ante

[11] MARINAO, Manuel" Plan de Contingencia de Información de Empresa_X" {En línea}. Recuperado el 12 de junio de 2015. Disponible en: http://www.monografias.com/trabajos90/seguridad-informatica-empresa/seguridad-informatica-empresa.shtml

una situación de contingencia con el objeto de que su impacto en las actividades sea lo menor posible .

OBJETIVOS

Detallar los procesos de la proyección y elaboración de los cuidados para resguardar la información de los diferentes daños y perjuicios producidos por corte de servicio, hechos naturales o por los hombres.

Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.

Implementar acciones que permitan evaluar los resultados y retroalimentación del plan de contingencia informático.

Principales procesos de Identificados

Software

- Servicios de Salud
- Citas Médicas
- Atención al Usuario
- Presupuesto y Tesoreria
- Contabilidad
- Programa Generación Archivos Planos
- Programa Captura de Historias Clínicas
- Facturación
- Estadística

Principales servicios que deberán ser restablecidos Y/O recuperados

Windows

- Explorador de Internet 8.0
- Antivirus Nod .32
- Clientes de Grupo (Correo Electrónico)
- Herramientas de Microsoft Office 2013

Software Base

- Bases de Datos MYSQL
- Bases de Datos SIIGO
- Bases de Datos POSTGRES
- Bases de Datos SQLSERVER
- Ejecutables de las aplicaciones

Respaldo de la Información

- Backup de la Base de Datos de MYSQL
- Backup de la Bases de Datos SIIGO
- Backup de la Bases de Datos POSTGRES
- Backup de la Bases de Datos SQLSERVER
- Backup de la Plataforma de Aplicaciones (Sistemas)
- Backup de la WEBSITE (esefjl.gov.co)
- Backup del Servidor controlador de Dominio Windows Server 2012.
- Backup del Servidor de Backup de Archivos Windows Server 2008.

ANÁLISIS DE EVALUACIÓN DE RIESGO Y ESTRATGÍAS

Metodología

El Análisis del Impacto tiene como objetivo determinar los procesos críticos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO y las aplicaciones que

lo soportan con el fin de proporcionar las bases para el Plan de Recuperación de Tecnología de la Información.

Actividades que se llevarán a cabo:

- Entrevistas a diferentes empleados responsables de las áreas que conforman la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

- Identificación de los Procesos en línea
- Subprocesos
- Aplicaciones que soporta la Empresa Social del Estado FABIO JARAMILLO LONDOÑO
- Máximo tiempo de interrupción en que el subproceso puede estar interrumpido en horas.
- Validación de la criticidad por proceso.

Para la clasificación de los activos de Tecnología Informática y Comunicaciones se han considerado tres criterios.[12]

- Criticidad.
- Frecuencia de uso
- Tecnología.

[12] INSTITUTO VERACRUZANO DE ACCESO A LA INFORMACIÓN IVAI. {Mayo 4 de 2012}. "Plan de Contingencia Informático" {En línea}. Recuperado el 12-06- 2015. Disponible: http://ivai.org.mx/DatosPersonales/Archivos/Interes/Extracto_Plan_De_Contingencia_IVAI.pdf

Se tiene el criterio de criticidad como el más importante, y los criterios de frecuencia de uso y tecnología que confirman la clasificación de Activos de Tecnología Informática y Comunicaciones[12].

Criticidad: el activo se define como crítico si su falta o falla es motivo de interrupción para el proceso.

Frecuencia de uso: el grado de utilización que se le da al activo.

Tecnología: el nivel de innovación tecnológica que tiene el activo, relacionado también a su valor de mercado y grado de obsolescencia.

Plan de contingencia: Es una herramienta de gestión para una buena administración de las Tecnologias de la Información y de las comunicaciones en el dominio del soporte y desempeño.

Los sistemas de Tecnología Informática son vulnerables a diversas interrupciones.

- Leves: Caídas de energía de corta duración, fallas en disco duro, etc.
- Severa: Destrucción de equipos, incendios, etc.

Existen varios tipos de riegos:

- Riesgos Naturales: tales como mal tiempo, terremotos, etc.
- Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
- Riesgos Sociales: como actos terroristas y desordenes.

Asegura que se dé una interrupción mínima a los procesos de negocios en caso de una interrupción significativa de los servicios que normalmente soportan esos procesos. Todos los aplicativos críticos y sistemas de soporte general deben tener un plan de contingencias.

Bienes susceptibles de un daño[13]

- Personal
- Hardware
- Software y utilitarios
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

Posibles daños

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, como cambios de claves de acceso, datos maestros claves,

[13] MARINAO, Manuel" Plan de Contingencia de Información de Empresa_X" {En línea}. Recuperado el 12 de junio de 2015. Disponible en: http://www.monografias.com/trabajos90/seguridad-informatica-empresa/seguridad-informatica-empresa.shtml

eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

- Divulgación de información a instancias fuera de la Empresa y que afecte a su patrimonio estratégico, sea mediante Robo o Infidencia

Prioridades

La estimación de los daños en los activos y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que se pierden en el acontecimiento.
Por lo tanto, los activos de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistemas computacionales

Desastres Naturales (Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas, equipos computacionales, Inundaciones causados por falla en los suministros de agua, Fallas en los equipos de soporte causadas por la agresividad del ambiente, la rede de energía eléctrica, acondicionamiento atmosférico necesario

- Fallas de Personal Clave (Enfermedad, Accidente, Renuncias, Abandono de sus puestos de trabajo. Otros imponderables)
- Fallas de Hardware (Falla en los Servidores de Aplicaciones y Datos, Fallas en el hardware de Red Swiches, Fallas en el Cableado de Red Router y FireWall).

Clases de Riesgos

- Terremoto
- Incendio
- Fallas en la red de voz y datos
- Fallas en el hardware y software
- Hacking, sabotaje o daño accidental
- Vandalismo y/o manifestaciones

MINIMIZACIÓN DE LOS RIESGOS

Para la minimización de los riesgos antes descritos y teniendo en cuenta los procesos de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, se pueden ver perturbadas también por fenomenos naturales, en el Departamento del Caquetá se encuentra en mayor proporción en el piso térmico cálido húmedo (91.3%) y se encuentra cerca de la cordillera oriental, esto hace que se presenten movimeintos fuertes y con mas frecuencia, al igual presenta lluvias repentinas y fuertes que producen rayos haciendo que se generen cortes de luz, asimismo tenemos que el Departamento es catalogado como zona roja debido a que hay presencia de varios grupos delictivos.

Terremoto

Criticidad: Muy Severa
Frecuencia de uso: Leve
Tecnología: severa

Con perdidas o daños de las instalaciones: estos casos afectarán gravemente a la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, en cuanto a su

infraestructura ya que no esta construida en estructuras anticismicas y esto hace que sea vulnerable, al igual los Rack se encuentran instalados uno en cada pisos y sin nunguna protección, lo cual haría que su interrupción del servicio sea por unas horas o días.

Escenario Actual	**Correctivo**
El área de informática no cuenta con un área segura frente a los desastres naturales donde almacena los backup de toda la Empresa junto con los servidores.	Realizar backups del servidor de forma mensual, almacenada en DVD y ubicarlos cerca a la salida principal de la Empresa y tener otra copia en un lugar aislado del sitio.
El área de informática no cuenta con elementos de seguridad industrial.	Debería capacitar a todo el personal en y tener activada la brigada de emergencias, dotarlos de los elementos de protección mínimos como (cascos, guantes, gafas, tapa bocas, etc.) y contar con extintor, en caso de evacuación contar señalizaciones de salida y un sitio seguro de encuentro.

Hasta la fecha no se han presentado esta clase de riesgo en la empresa pero en caso de presentarse sería catastrófico ya que no se tiene contratada una entidad para el resguardo la copia de respaldo, esto haría más compleja su recuperación.

Incendio

Criticidad: Muy Severa
Frecuencia de uso: Leve

Tecnología: severa

Escenario Actual	Correctivo
El área de informática no se encuentra protegida de acceso a usuarios, puesto que todas las personas pueden acceder a ella.	La empresa debería establecer un sitio aislado de las demás oficinas para el centro de cómputo, y que cuente al menos con extinguidores para mitigar el incendio, activar el plan de emergencias, llamar a las autoridades como Bomberos para el cubrimiento y control de la situación, así mismo restringir el acceso a estos espacios, ya que podrán sacar copias de la información no autorizadas y/o robo o pérdida de la Información.
Las instalaciones no cuentan sino con una medida de seguridad de acceso a la oficina donde se encuentran los equipos, se destaca que todas las personas que pertenecen al departamento de sistemas tienen las llaves de acceso, es decir es semi restringido.	Establecer otra salida de evacuación y que las llaves solo sean manejadas por las personas encargadas de los sistemas, ya que si no se hace se podrían presentar, Incendios premeditados, estos produciendo cortos circuitos y hasta quemaduras de trabajadores o Electrocutación.
Red de Emergencia	En el inventario de bodega de equipos de comunicación solo debe de existir la red de emergencia, la

	cual no puede superar el 5% de la totalidad de equipos portátiles

Al llegarse a presentar un incendio dependiendo de su dimensión, puede afectar los servidores, estaciones de trabajo, dispositivos de comunicaciones y su criticidad es muy alta y esto requerirá la adquisición de nuevos equpos, configurar nuevamente los servidores y los demás sistemas de respaldo a los ordenadores afectados de la sede de la Administrativa de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

Fallas en la red de voz y datos

Criticidad: Severa
Frecuencia de uso: Leve
Tecnología: severa

Escenario Actual	**Correctivo**
En cableado dentro del centro de computo se encuentra disponible.	Deben tener cableado estructurado para lo cual deberá cada computador estar conectado a la red mediante una conexión física (canaleta plástica, metálica o en muro) que comprende: A. Punto de conexión DATOS: Gabinete o Rack, Patch panel,

	Cable UTP, Jack de conexión, placa o face plate y un Patch cord de conexión. B. Punto de conexión ENERGIA: el computador deberá tener una toma de conexión eléctrica regulada por UPS en color naranja.
Las instalaciones eléctricas no tienen polo a tierra.	Se tiene UPS instalada para los equipos de escritorio, al igual se debe realizar las instalaciones de polo a tierra con las especificaciones técnicas indicadas, para que no se presenten voltaje muy alto que entre directamente al hardware y dañarlos.
Mantenimiento de los sistemas de puestas a tierra.	Las unidades deben realizar mínimo un mantenimiento anual, unificando el sistema de tierras y protección de equipos, asegurando que el valor óhmico este por debajo de los 3 tres ohmios.
Todos los puertos del servidor de dominio estan disponibles desde la red interna, donde cualquier computadora puede conectarse a la red y no se tiene rentringido la	En la instalación del Windows Server 2008 - 2012, se debe bloquear los puertos innecesarios, para que no se presenten denegación de servicio, códigos maliciosos.

utilización memorias USB, laptos personales.	
El Internet se va con frecuencia, debido a factores climáticos interfieren en el buen funcionamiento.	Tener instalado un banco de baterías o UPS que soporten nuestro rack, ya que es el comunicador con el servidor principal.
Controlar usuarios de la red	Todos los usuarios que tengan acceso a la red de datos de la Empresa deben firmar un acta de confidencialidad y compromiso por el usuario de acceso a la red.

Las fallas en la red de voz y datos, son de criticidad sebera por el motivo que al presentarse un daño deja por fuera del servicio a todo la empresa, pero al igual se pueden restablecer de inmediato ya que su infraestructura es pequeña y se podría utilizar router y swiches alternos.

Fallas en el hardware y software

Criticidad: Muy Severa
Frecuencia de uso: Severa
Tecnología: Leve

Escenario Actual	**Correctivo**
Los pc presentan problemas de encendido, los usuarios en su afán no	Se debería capacitar a todo el al personal de la empresa en el uso,

apagan correctamente los computadores sino que los desconectan directamente, lo que hace que el sistema operativo comience a fallar.	manejo y cuidado de los activos de información, porque al no llegar hacerlo podría ocasionar una pérdida de información y hasta el daño del hardware.
Relación uso de los equipos de cómputo.	Instruir al personal del uso de equipo Telemático/Electrónico existente, Georreferenciación, a las oficinas desconcentradas o proveedores, para así mejorar las condiciones del servicio de la Empresa y verificar que el personal de un buen uso de las herramientas.
Seguridad física y del entorno	Las unidades asegurarán el entorno físico de los equipos en donde se procese y almacene información Empresarial, según la clasificación y control de acceso definidos para las Áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se admite el paso de personal autorizado a los sistemas de información y a las instalaciones de la Empresa Social del Estado Fabio Jaramillo Londoño.
Mantenimiento a los equipos informáticos.	Planear la programación de mantenimientos preventivos en

coordinación con la empresa.

Realizar un mantenimiento preventivo a la totalidad de los equipos detallados en las listas de inventarios durante la ejecución del contrato.

Mensualmente el contratista entregará un informe de avance de mantenimiento en el cual se estipule lo siguiente:

- Problemas reportados.
- Causas y soluciones en los mantenimientos correctivos por equipo.
- Fecha de llamada.
- Tiempo de respuesta a la llamada.
- Tiempo de solución del problema.
- Partes dañadas y cambiadas.

Las modificaciones sufridas en los servidores software y su hardware muchas veces son corregidas de inmediato sin necesitar restauraciones de copias de respaldo, pero cuando existe un daño en estos se considera crítico debido a que hay que instalar programas y la recuperación de las copias de respaldo si no están actualizadas, se pierde la última información digitada en las bases de datos y esto gastaría días en la puesta nuevamente en marcha.

Hacking, sabotaje o daño accidental

Criticidad: Severa
Frecuencia de uso: Severa
Tecnología: Severa

Escenario Actual	Correctivo
Antivirus empresarial	Todos los equipos de cómputo de la Empresa, deben tener el antivirus Empresarial instalado y actualizado.
Equipos de cómputo validados en el servidor de dominio.	Este proceso lo realiza solamente el encargo de sistemas, verifica que los equipos de cómputo conectados a la red de la empresa, Oficinas, deben ser miembros del dominio, con direccionamiento automático y reservas por DHCP.
Uso cuentas correo electrónico Institucional.	Creación de las cuentas de correo electrónico empresariales y mediante convenios deben estar activas.
Mala manipulación de los sistemas	Es responsabilidad de los usuarios que la información que manejan sean los asignados a su cargo y perfil.

En caso de que la información sea alterada se deberá capturar los datos faltantes en las bases de datos de los sistemas, o si es eliminada y se haga imposible el

inicio inmediato de las operaciones, se deberá obtener los respaldos de datos, programas, manuales y claves, del lugar donde se encuentren resguardados, restaurar la información de las bases de datos y programas.

Vandalismo y/o manifestaciones

Criticidad: Severa
Frecuencia de uso: Leve
Tecnología: Leve

Escenario Actual	Correctivo
Instalaciones alternas	El personal Subgerencia de Informática debe prever un sitio alterno para continuar con las operaciones críticas, establecer un tiempo de espera de solución de la huelga, si continua, se deberá definir al personal que apoyará en la restauración, el retito de los quipos, elementos que sean necesarios hacía el lugar distante de los hechos, los cuales se hacen por medio de una lista, con nombre o placa del elemento retirado, responsable y ubicación física de la dependencia que se encuentra.

Realizar el inventario de los equipos dañados, perdida de documentos importantes, mobiliarios.	Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la recuperación de las operaciones.
Resguardo de Copias de Respaldo	Determinar lugares especiales, fuera del centro de cómputo, para el resguardo de copias de respaldo, documentación importante de los procesos.
El personal clave del Plan de contingencia informático.	Debe de dar la señal del paro total y sacar las copias de respaldo de la información fuera de las instalaciones en un tiempo límite antes de ser declarada la huelga.
Dispositivos de almacenamiento, si se mantienen en la misma sede de la Administrativa de la Empresa Social de Estado FABIO JARAMILLO LONDOÑO.	Se debe resguardar estos dispositivos en lugar distinto para en caso de tener que restablecer los sistemas a los procesos más críticos.

Si se presentara alteración de orden público por vandalismo y/o manifestaciones que afecte el funcionamiento parcial de las actividades o el paro total de las operaciones dentro de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, afectaría principalmente a los servicios que se prestan a los usuarios en general.

Como el soporte de los sistemas lo tenemos contratado con externos, para el plan de contingencia deberemos asegurar que se tenga un contrato que incluya:

- Tiempos mínimos de respuesta para soporte en sitio y soporte remoto.

- Planes periódicos de mantenimiento preventivo y correctivo.

- Un procedimiento que nos asegure los esquemas de backups de las estaciones del área administrativa y del servidor, estaciones POS, estaciones brutas, y swich de acuerdo a las políticas de respaldo que se hayan fijado en el contrato, también debe incluir los procesos de recuperación para cada uno de los equipos que se estén respaldando, fichas de control que nos permite validar lo anterior, que nos servirán de históricos y procesos de seguimiento.

- Unos términos con tiempo mínimos, para que en caso de daño de las maquinas POS, estaciones brutas, router y swich sean arreglados o reemplazados por unos de igual o mejores características, los cuales deberán configurarse y ponerse en funcionamiento de acuerdo a los tiempos estipulados.

Plan de Recuperación[14]

Objetivos del Plan de Recuperación

[14] MARINAO, Manuel" Plan de Contingencia de Información de Empresa_X" {En línea}. Recuperado el 12 de junio de 2015. Disponible en: http://www.monografias.com/trabajos90/seguridad-informatica-empresa/seguridad-informatica-empresa.shtml

- Determinar de las políticas y procedimientos para respaldar las aplicaciones y datos.
- Planificar la reactivación dentro de las 12 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
- Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
- Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operaciones normal del centro de procesamiento de la información, basándose en los planes de emergencia y de respaldo a los niveles del centro de cómputo y de los demás niveles.

Las responsabilidades sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

Activación del Plan

Decisión

Queda a juicio del Gerente de la Empresa, determinar la activación del Plan de Desastres, y además iniciar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste

Duración estimada

Los supriores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procedimiento en un lugar alternativo.

Responsabilidades

- Orden de Ejecución del Plan : Gerencia de Administrativa
- Supervisión General de Plan: Empresa en convenio para Recuperación.
- Supervisión del Plan de Recuperación: Supervisor(es) de Área(s).
- Abastecimiento (hardware, software): Asistente de Administración.
- Tareas de Recuperación: Personal de tareas afines.

Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un periodo mayor a 24 horas durante los fines de mes (durante los cierres contables)

11 CONCLUSIONES

La información de toda organización, constituye el corazón de la misma, es su activo más valioso. Por tal razón, ante el avance imparable de las nuevas tecnologías, nace la necesidad de asegurar la información.

Después de mucho indagar y en base a la normatividad vigente se sugiere al área administrativa tomar la decisión de profundizar en el mejor sistema, o el que mejor se adapta a las necesidades de Empresa Social del Estado FABIO JARAMILLO LONDOÑO.

Herramienta como las encuestas, permite visualizar que tanto el personal interno de la empresa conoce de políticas de seguridad para la protección de los activos de la información, las cuales ayudan a identificar el nivel de riesgo que está expuesta la empresa y a su vez que la gerencia vea la importancia de implementar metodologías que ayuden a mitigar las amenazas, riesgos y vulnerabilidades a las que están expuestos a diario.

La matriz de riesgo ayuda determinar las acciones correctivas y preventivas para cada riesgo reconocido durante la fase del análisis de la empresa, esto nos sirve para tener un enfoque sobre el comportamiento de las vulnerabilidades y amenazas a través de la caracterización en procura de minimizar pérdidas o daños. En este escenario se analizan las diferentes opciones, se hace un análisis de riesgos por la metodología de Margerit y se determinan los principales riesgos que pueden afectar a la Empresa Social del Estado FABIO JARAMILLO LONDOÑO son: la filtración, el hurto o robo, la modificación o saboteo y la eliminación de la información.

El diseño de un modelo general de seguridad de la información (SGSI), da a conocer la importancia a la empresa , de la implementación de un Sistema Gestión de la Seguridad de la Información (SGSI) proporciona herramientas para

cada uno de los activos informáticos, los recursos humanos y todas sus áreas de la empresa que requieran de la utilización de las tecnologías de la información y dentro de éste, por lo tanto estudiamos la Norma ISO 27001:2013, la idea de generar unos procesos y procedimientos, considerando establecer unos parámetros para estructurar y garantizar que los riesgos de la seguridad de la información sean minimizados.

El plan de contingencia informático para la empresa, es primordial que cuente con recursos de Tecnología de la información actualizados, para poder proporcionar unos servicio óptimos que necesita para garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones. Este Plan de Contingencias, es necesario que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

RECOMENDACIONES

Se hace necesaria la capacitación del personal técnico de la red de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, que le brinde las herramientas y conocimientos a nivel técnico para ofrecer a la administración la mejor solución para la adquisición de equipos.

Capacitar al resto de personal en las políticas de seguridad y mínimos niveles de resguardo de la información permitiendo minimizar los márgenes de riesgo.

La implementación de un Plan de Contingencia Informático en el Área de Sistemas en la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, se hace necesario en caso de que se llegue a presentar un daño o siniestro, y pueda lograr los objetivos de tiempo de disponibilidad, tanto en sus recursos informáticos como en las comunicaciones.

BIBLIOGRAFIA

BORGHELLO, Cristian [2000 – 2009]. “Plan de Contingencia”. [En línea]: [16 mayo de 2015]: Disponible: http://www.segu-info.com.ar/politicas/contingencia.htm

CONSTAIN, Gustavo Eduardo, RAMÍREZ, Gabriel Mauricio, “Módulo Modelos y Estándares de Seguridad Informática”, [2013].

Gerencia De Calidad. Gerencia de Procesos. “Método de Control de Procesos” [En línea]. Junio 27 de 2013. Recuperado el 24-05- 2015. Disponible: http://www.unalmed.edu.co/josemaya/Ing_prod/Control%20de%20Proceso-%20Metodo.pdf

Instituto Veracruzano de Acceso a la Información IVAI. [Mayo 4 de 2012]. “Plan de Contingencia Informático” [En línea]. Recuperado el 12-06- 2015. Disponible: http://ivai.org.mx/DatosPersonales/Archivos/Interes/Extracto_Plan_De_Contingencia_IVAI.pdf

MARINAO, Manuel” Plan de Contingencia de Información de Empresa_X”. [En línea]. Recuperado el 12 de junio de 2015. Disponible en: http://www.monografias.com/trabajos90/seguridad-informatica-empresa/seguridad-informatica-empresa.shtml

Portal Administración Electrónica. [Madrid, octubre de 2012].” Magerit v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información” [En línea]. Recuperado el 05 de junio de 2015. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_cat%C3%A1logo%20de%20elementos_es_NIPO_630-12-171-8.pdf

REPUBLICA, G. N. [5 de Enero de 2009]. Ley 1273 del 2009. Obtenido de MinTic: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

RÍOS, J. Seguridad Informática, [10 de Mayo de 2014]. Disponible: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml#introducca#ixzz2fCGghfuG.

SABOGAL ROZO, Esther. [Enero 2013]. “Proyecto de *Seguridad Informática I"*. La Plata. UNAD.

SABOGAL ROZO, Esther Angélica, [Enero 2013]. “Módulo Proyecto de Seguridad Informática I”, [2013].

SABOGAL ROZO, Esther Angélica, Módulo Proyecto de Seguridad Informática II, [2013].

Secretaría General de la Alcaldía Mayor de Bogotá D.C. [2013]. http://www.alcaldiabogota.gov.co. [En línea]: [Junio 27 de 2013]. Recuperado el 11 de mayo de 2015. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Secretaría General de la Alcaldía Mayor de Bogotá D.C. [2013] ” Ley 1273 del 2009” [En línea]: [Enero 5 de 2009]. Recuperado el 11 de mayo de 2015. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

SOLARTE, Francisco. [2013]. Modulo Aspectos Éticos y Legales. Universidad Nacional Abierta y a Distancia UNAD

SUÁREZ CIERRA, Lorena. [2013]. Modulo Sistema de Gestión de la Seguridad Informática. Bogotá: Universidad Nacional Abierta y a Distancia UNAD

Universidad Distrital Francisco José de Caldas. “Seguridad de la Información SGSI” [En línea]. Recuperado el 24-05-2015. Disponible: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

ANEXOS

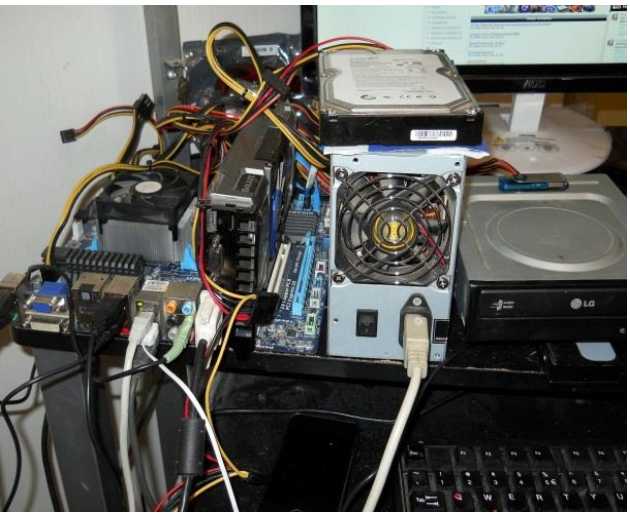
Anexo 14. Encuesta realizada al personal de la empresa sobre la Seguridad de la Información.

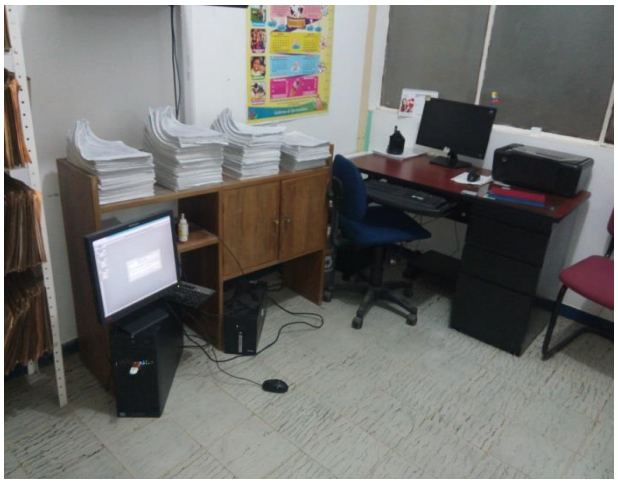
ENCUESTA REALIZADA AL PERSONAL DE LA EMPRESA SOBRE LA SEGURIDAD DE LA INFORMACIÓN.			**VESION:**	01
			Fecha de Aplicación	15/07/2014
			Elaborado por:	Ing. Mercedes Sarria Cuellar
		SI	**NO**	**N/A**
1	El documento Política de Seguridad: ¿contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia?		X	
2	En la resolución de nombramiento del Encargado de Seguridad de la Información: ¿se encuentra explicitada la función: "Coordinar la respuesta a incidentes que afecten a los activos de información institucionales"?		X	
3	En la actualidad: ¿el Servicio aborda todos los requerimientos de seguridad antes de entregar acceso a los activos de información a sus clientes/usuarios/beneficiarios?	X		
4	En el servicio, ¿se identifican los activos de información y se elabora un inventario de ellos?		X	
5	¿Se actualiza dicho inventario?		X	
6	En el servicio, ¿se ha designado responsabilidad administrativa por los activos de información?	X		
7	En el servicio, ¿existen normas para el Copiado de los activos de información clasificados?		X	

8	En el servicio, ¿existen normas para el Almacenamiento de los activos de información?		X	
9	En el servicio, ¿existen normas para Transmisión por correo electrónico de los activos de información clasificados?	X		
10	En el servicio, ¿existen normas para la destrucción de los activos de información clasificados?		X	
11	En el servicio, ¿existen procedimientos de etiquetado y manejo de los activos de información que consideren dicha clasificación?	X		
12	El Coordinador de Sistemas: ¿ha impartido instrucciones sobre la generación, transmisión, recepción, procesamiento y almacenamiento de activos de información?		X	
13	El documento Política de Seguridad: ¿contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia?		X	
	OBSERVACIONES:			

Fuente Autor Proyecto

Anexo 15. Registró Fotográfico de visita





Anexo 16. Políticas de Seguridad de Uso Aceptable de los Recursos Informáticos

ESE FABIO JARAMILLO LONDOÑO

POLITICAS DE SEGURIDAD DE USO ACEPTABLE DE LOS RECURSOS INFORMÁTICOS

Revisó	Gerencia General	
Aprobó	Coordinador de sistemas	
Fecha Aplicación	11/052015	

INFORMACIÓN DEL DOCUMENTO

Versión	**Fecha** [11/05/015]	**Elaborado por:**	**Razón de la actualización**
0	11/05/015	Ing. Mercedes Sarria Cuellar	Creación del documento
1	11/05/015	Ing. Mercedes Sarria Cuellar	Ajustes de los directivos del Áreas de Sistemas

CONTENIDO

OBJETIVO

ALCANCE

POLITICA

RESPONSABILIDADES

OBJETIVO

Definir los aspectos de seguridad de la información asociados con el cumplimiento del uso aceptable de los recursos informáticos que deben ser considerados por la Empresa Social del Estado FABIO JARAMILLO LONDOÑO para evitar infringir la vulnerabilidad de la existente de un activo o un grupo de activos, generándole pérdidas o daños.

ALCANCE

Las políticas consignadas en este documento deben ser cumplidas por todos los Empleados de la Empresa Social del Estado FABIO JARAMILLO LONDOÑO, y terceras partes que tengan acceso a la información y los recursos tecnológicos de la empresa y/o hagan uso de sus recursos tecnológicos.

POLITICA DE USO ACEPTABLE EN LOS RECURSOS INFORMÁTICOS

POLITICAS DE SEGURIDAD DE USO ACEPTABLE EN LOS SISTEMAS DE INFORMACIÓN

1. El intento o violación de los controles de seguridad establecidos para la protección de los activos informáticos.
2. Realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo informático.
3. El uso sin autorización de los activos informáticos.
4. El uso NO autorizado o impropio de la conexión al sistema.
5. Intentar evadir o violar la seguridad o autenticación de usuarios de cualquier host, red o cuenta.
6. El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.
7. Está prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios.
8. El almacenamiento, instalación, configuración, o uso de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.

9. El hurto, robo, sustracción o uso no autorizado de datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos de la ESE FABIO JARAMILLO LONDOÑO.
10. Está prohibido retirar de las instalaciones de la ESE FABIO JARAMILLO LONDOÑO o áreas bajo su administración o control, cualquier activo informático sin autorización previa.
11. El acceso, modificaciones o alteraciones no autorizadas de componentes, datos o información de los activos informáticos de la ESE.
12. El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización del administrador del sistemas.
13. El servicio de internet puede ser utilizado solamente con fines autorizados y legales. se prohíbe toda transmisión, difusión, distribución o almacenamiento de cualquier material digital o impreso en violación de cualquier ley o regulación aplicable. estos incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio, o que constituya una amenaza ilegal.
14. En el uso del correo electrónico, está prohibido el SPAM, TROLL, MAILBOMBING, etcétera, reenvió o retransmisión de mensajes de carácter no oficial, o la suscripción a otro usuario a una lista de correo sin su permiso.
15. Realizar por internet, o a través de los activos informáticos, cualquier actividad que pudiera potencialmente traer desprestigio a la ESE.
16. Está prohibido el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o video que no estén relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.
17. El usuario está de acuerdo en aceptar responsabilidad por todas las actividades realizadas con los activos informáticos bajo su responsabilidad y custodia o desde las cuentas asignadas para su acceso a los servicios informáticos de la ESE.
18. Las cuentas de la ESE operan con recursos compartidos. está prohibido el uso abusivo de estos recursos por parte de un usuario en una forma tal que afecte negativamente el rendimiento de la misma.
19. Cualquier violación o sospecha de violación de las medidas o controles de seguridad de los sistemas de información o de las políticas de seguridad

informática para la ESE FABIO JARAMILLO LONDOÑO, debe ser reportada por escrito inmediatamente por quien conozca de ella, al ADMINISTRADOR DEL SISTEMA O COORDINADOR DE SEGURIDAD INFORMATICA de su respectiva IPS, para los fines pertinentes la ESE cooperan con investigaciones de violaciones a la seguridad de redes y sistemas, incluyendo la cooperación con las autoridades legales en la investigación de cualquier incidente informático, que de origen a procesos administrativos, disciplinarios, penales o civiles.

Anexo 17. Modelo plan maestro para la implementación de un sistema de gestión de seguridad de la información (SGSI)

VER.	FECHA	AUTOR	MODIFICACIONES
1.0	2015-05-18	Ing. Mercedes Sarria Cuellar	Versión Inicial
ÁREA DE INFLUENCIA	EMPRESA SOCIAL DEL ESTADO FABIO JARAMILLO LONDOÑO		
	Centro de Sistemas y Comunicaciones		
Revisó	Gerencia General		
Aprobó	Coordinador de sistemas		

Tabla de Contenido

1. Introducción

2. Acerca de la Seguridad de la Información

3. Organización para la Seguridad de la Información

4. Política de Seguridad de la Información

4.1 Generalidades

4.2 Alcance

4.3 Objetivos

4.4 Responsabilidad

5. Identificación, clasificación y valoración de activos de información

6. Seguridad de la información en el Recurso Humano

6.1Responsabilidades del personal de la Empresa

6.2 Responsabilidades de Usuarios

6.3 Usuarios invitados y servicios de acceso público

7. Seguridad Física y del entorno

7.1 Acceso

7.2 Seguridad en los equipos

8. Administración de las comunicaciones y operaciones

8.1 Reporte e investigación de incidentes de seguridad

8.2 Protección contra software malicioso y hacking

8.3 Copias de Seguridad

8.4 Administración de Configuraciones de Red

8.5 Intercambio de Información con Organizaciones Externas

8.6 Internet y Correo Electrónico

8.7 Instalación de Software

9. Control de Acceso

9.1 Categorías de Acceso

9.2 Control de Claves y Nombres de Usuario

9.3 Computación Móvil

9.4 Auditoria y Seguimiento

9.5 Acceso Remoto

10. Adquisición, Desarrollo y Mantenimiento de Sistemas Software

11. Administración de Continuidad del Negocio

12. Política de Seguridad de la Información

13. Cumplimiento

13. Referencias.

14. Términos y Definiciones

14.1 Información

14.2 Activo de Información

14.3 Sistema de Información

14.4 Propietario de Activos de

14.5 Tecnología de la Información
14.6 Evaluación de Riesgos
14.7 Administración de Riesgos
14.8 Comité de Seguridad de la Información
14.9 Responsable de Seguridad Informática
14.10 Grupo responsable de Seguridad Informática
14.11Incidente de Seguridad Informática
14.12 Cadena de custodia

Fuente Autor Proyecto