ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA EN LA DEPENDENCIA DE FORMACIÓN PROFESIONAL INTEGRAL DEL SENA REGIONAL GUAINÍA, PARA EL DISEÑO DE UNA PROPUESTA DE ASEGURAMIENTO DE LA INFORMACIÓN BASADA EN LA METODOLOGÍA MAGERIT.

JEYSSER AURELIO PALACIOS PALACIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA "ECBTI"
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
GUAINÍA
AGOSTO DE 2020

ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA EN LA DEPENDENCIA DE FORMACIÓN PROFESIONAL INTEGRAL DEL SENA REGIONAL GUAINÍA. PARA EL DISEÑO DE UNA PROPUESTA DE ASEGURAMIENTO DE LA INFORMACIÓN BASADA EN LA METODOLOGÍA MAGERIT.

JEYSSER AURELIO PALACIOS PALACIOS

PROYECTO DE SEGURIDAD INFORMÁTICA II
Proyecto aplicado para optar al título de Especialista en Seguridad Informática

Msc. Katerine Marceles Villalba
Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA “ECBTI”
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
GUAINÍA
SEPTIEMBRE DE 2020

Nota de Aceptación:

_____

_____

_____

_____

_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Inírida, 24 de Septiembre de 2020

DEDICATORIA

De manera innegable dedico este título por el cual opto a DIOS, a mi familia y especialmente a mi esposa los cuales siempre están apoyándome y deseándome lo mejor.

AGRADECIMIENTO

De manera innegable agradezco a DIOS por las bendiciones, a mi familia por su apoyo, mi esposa por su entrega y a la UNAD que a través de un excelente equipo de profesionales facilito la oportunidad de formarme en esta prestigiosa institución.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

El Centro Ambiental y Ecoturístico del Nororiente Amazónico – Regional Guainía. Es uno de los 33 centros de formación con los que cuenta el SENA a nivel nacional. Este encargado dentro de su misión ejecutar programas de formación de nivel técnico, tecnólogo y complementario de modalidad presencial y virtual. Que permitan vincular al sector comercio del municipio de Inírida. Egresados con altas competencias, habilidades y destrezas alineadas a las necesidades productivas que las empresas requieren para ser más competitivas. Lo anterior que contribuya al desarrollo social, económico y el mejoramiento en la calidad de vida de los habitantes.

El centro de formación cuenta con una infraestructura tecnológica que apoya su funcionamiento para darle respuesta a la ejecución de la formación tales como: Equipos de cómputo, impresora (locales y de red) y dispositivos de interconexión de redes.

Con el desarrollo del presente proyecto aplicado se busca a través de la aplicación de una metodología de gestión de Riesgo como es MAGERIT. Se realice un inventario de los activos de información con los que cuenta la dependencia de Formación Profesional Integral del SENA Regional Guainía. Para posteriormente identificar los riesgos, vulnerabilidades y amenazas asociados a dichos activos de información. a partir de éste, se puedan definir los controles y salvaguardas necesarias enfocadas a proteger los activos de información y la infraestructura tecnológica de la dependencia.

TITULO DEL PROYECTO

Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del SENA Regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT.

1. FORMULACIÓN DEL PROBLEMA

1.1 PRESENTACIÓN

El Sena Regional Guanina es una institución que dentro de su misión esta impartir formación titulada, complementaria y virtual. Actualmente cuenta dentro de su organigrama con la dependencia de formación profesional integral, que es donde se realiza todo el proceso de registro, inscripción y matrícula de los aprendices a los programas que el SENA contempla dentro de su catálogo. Lo que ha propiciado un flujo o producción de información tanto impresa como digital, y que, al no contar con políticas definidas de seguridad de información, ha propiciado malas prácticas con relación a la manipulación, cadena de custodia o acceso a la información de manera oportuna, riesgos que de no ser controlados llegarían a afectar la integridad y disponibilidad de la información. Por otra parte, No se cuenta dentro de la dependencia con políticas de seguridad claras que permitan proteger la información de extravíos, accesos no autorizados tanto a equipos de cómputo, medios extraíbles y hasta archivos impresos que quedan en la bandeja de la impresora. Lo que afecta la propiedad de confidencialidad de la información producida.

Ante la importancia que tiene la seguridad de la información en el sector empresarial y educativo, el presente proyecto aplicado busca responder y suministrar los elementos de juicio con relación a los siguientes cuestionamientos ¿Cuáles son los factores que incidiría en la pérdida de información académica y administrativa dentro de la dependencia de formación profesional integral, SENA Regional Guainía? y ¿Cuáles son los salvaguardas que se pueden implementar para proteger los activos de información y la infraestructura tecnológica de la misma?.

La ausencia de mecanismos de seguridad destinados a conservar la integridad de la información dentro de la dependencia de formación, hace que se presenten brechas de seguridad a tal punto que afecta la toma de decisiones y la legitimidad de esta. Esto genera la necesidad de aplicar una metodología que permita definir los riesgos asociados a cada activo y a partir de allí, adoptar las acciones tendientes al tratamiento eficiente de dichas amenazas.

La pérdida de información es un alto riesgo a las que están expuestas muchas empresas sino adoptan estrategias contundentes para prevenir, controlar y mitigar los ataque que se pueden llegar a producir por la explotación de las

vulnerabilidades que su sistema informático pueda tener. Por ello se debe garantizar a través de una metodología la incorporación de procedimientos y mecanismos eficaces que disminuyan las amenazas latentes.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿Cómo puede la metodología MAGERIT garantizar el aseguramiento de la información de la dependencia de Formación Profesional Integral del Sena regional Guainía?

2. JUSTIFICACIÓN

El desarrollo del presente proyecto aplicado es de suma importancia en la medida que proporcionará una documentación frente a medidas de seguridad enfocadas a la protección de la información almacenada y producida en la dependencia de formación profesional integral. Estará enfocado a través de la implementación de una metodología de análisis de riesgo, la identificación de las vulnerabilidades a los que están expuestos los activos de información de la oficina. Permitiendo así proporcionar los elementos de juicio necesarios que contribuyan a la implantación de mecanismos y procedimientos encaminados a salvaguardar la información conservando 3 principios básicos como lo es la confidencialidad, integridad y la disponibilidad de la misma.

Se espera que esta metodología se convierta dentro de la dependencia de Formación Profesional Integral del SENA Regional Guainía en un punto de referencia para la aplicación de procedimientos seguros que tiene como finalidad establecer las mejores condiciones de protección para la información y tratamiento de la misma.

La protección de la información y demás activos de la empresa es imprescindible. Toda vez, que es el insumo más invaluable, para la toma de decisiones y la prestación de un servicio con eficiencia. Por tal motivo debe ser conservada, producida y manipulada de forma segura.

Lo anteriormente expuesto para que se tomen todas las recomendaciones contemplados en el documento que se entregará. Con la convicción que sean implementados por parte de la empresa, capaciten a sus empleados frente a las políticas para el uso adecuado enfocado a la seguridad de la información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar la metodología MAGERIT para identificar los riesgos, vulnerabilidades y amenazas asociados a los activos de información de la dependencia de Formación Profesional Integral de SENA Regional Guainía.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar la identificación de los activos de información presentes en la Dependencia Formación Profesional Integral del SENA Regional Guainía.
- Definir los riesgos, vulnerabilidades y amenazas de los activos de información de la dependencia de formación.
- Diseñar un plan de tratamiento de riesgos y vulnerabilidades detectados a los activos de información.

4. ALCANCE Y DELIMITACIÓN

4.1 ALCANCE

Para el desarrollo del presente proyecto aplicado dentro de la dependencia de formación profesional Integral del SENA Regional Guainía. Se utilizará la metodología MAGERIT con el objetivo de identificar los activos de información asociados a la oficina. Para posteriormente relacionar los riesgos, vulnerabilidades y amenazas a los que pueden estar expuestos, y de esta forma poder describir los controles de seguridad a implementar destinados proteger la información.

4.2 DELIMITACIÓN

El presente proyecto aplicado llegará hasta la entrega de un documento en formato (Word o pdf) el cual contendrá la identificación de los activos de información asociados a la dependencia de Formación Profesional Integral del SENA Regional Guainía. Los riesgos y amenazas a los que pueden estar expuestos. Por otra parte, las recomendaciones para el aseguramiento de la información y la infraestructura tecnológica de la dependencia.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Como referencias que aportan elementos importantes para esta investigación se tienen:

Según los autores Jhon Alexander López y Andrés Fabián Zuluaga Tamayo. Los cuales presentaron la tesis de grado denominada “Desarrollo De Una Metodología Para El Control De Riesgos Para Auditoria De Base De Datos”. Para optar al título de Ingeniería De Sistemas y Computación de la Universidad Tecnológica de Pereira en el año 2013[1]. Permite dar soporte a los auditores de sistemas de información especializados en auditorias de bases de datos, logren identificar, analizar y controlar los riesgos que pueden afectar la información de las centrales de datos. Dicha investigación presenta relación con este estudio. Toda vez, que incorporan la metodología de análisis de riesgo MEGERIT y reconocen la importancia de valoración de amenazas a los que pueden estar inmersa las bases de datos dentro una empresa y como establecer medidas tendientes a salvaguardar la información contenidas en ella.

De acuerdo a la autora Yenny Maribel Alvarez Sosa. La cual presento el trabajo de grado denominado “Diseño De Una Metodología Para El Análisis De Riesgo En Los Sistemas De Gestión De Seguridad De Información (Marisgsi)”. Para optar al título de Magister Scientiarum en ciencias de la Computación, en la universidad Centroccidental “Lisandro Alvarado” de Barquisimeto Estado Lara en el año 2013[2]. El cual proporciona una perspectiva global sobre seguridad informática, específicamente en el aseguramiento de recursos de la empresa, tomando como base 3 pilares Confidencialidad, Integridad, Disponibilidad. Dicho trabajo se relaciona con este proyecto aplicado dado que proporciona pasos para la planeación y el establecimiento de medidas para el aseguramiento de la información dentro una empresa.

[1] LOPEZ, Jhon Alexander y ZULUAGA TAMAYO, Andrés Fabián. Desarrollo De Una Metodología Para El Control De Riesgos Para Auditoria De Base De Datos. Tesis de Grado Ingeniería De Sistemas y Computación. Pereira.: Universidad Tecnológica de Pereira. 2013. 5-51p.

[2] ALVAREZ SOSA, Yenny Maribel. Diseño De Una Metodología Para El Análisis De Riesgo En Los Sistemas De Gestión De Seguridad De Información (Marisgsi) En Las Universidades De Barquisimeto Estado Lara. Trabajo de Grado Magister Scientiarum En Ciencias De La Computación. Barquisimeto: Universidad Centroccidental “Lisandro Alvarado”. 2013. 2-34p.

Según la autora Karina del Rocio Vásquez Gaona. La cual presento la tesis de grado denominada “Aplicación De La Metodología MAGERIT Para El Análisis Y Gestión De Riesgos De La Seguridad De La Información Aplicado A La Empresa Pesquera E Industrial Bravito S.A En La Ciudad De Machala”. Para optar al título de Ingeniera de sistemas en la universidad Politécnica Salesina. Sede cuenca en el año 2013[3]. Define apartes importantes en la identificación y valoración de los riesgos a los que puede estar sujeta la información. Si no se toman medidas tendientes a protegerlos de ataque que afecte su integridad. Dicha investigación se relaciona con este trabajo, que se coindice en el establecimiento de una metodología que proporcione los elementos de juicio necesario encaminados a la protección de la información mitigando las amenazas a las que pueden estar expuestas.

De acuerdo a la autora Maria Carolina Duarte Martinez. La cual presento la tesis de grado denominada “Diseño De Politicas De Seguridad De La Información Para La Unidad De Tecnología De La Cámara De Comercio De Cúcuta”. Para optar al título de Especialista en Seguridad Informática con la Universidad Nacional Abierta y a Distancia UNAD en el año 2019[4]. El cual define a partir de la gestión de riesgos, las salvaguardas necesarias para maximizar las condiciones de seguridad. Tendientes a proteger la información de amenazas que afecten la integridad, disponibilidad y confidencialidad. Dicho trabajo se relaciona con este proyecto ya que en ambos se pretende suministrar los controles que permitan asegurar los activos de información y la infraestructura tecnológica de una empresa.

5.2 MARCO TEÓRICO

Dentro del proceso investigativo para el establecimiento de la metodología para el desarrollo proyecto aplicado. Se hace necesario tener claridad en los siguientes aspectos teóricos:

[3] VÁSQUEZ GAONA, karina del Rocio. APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANALISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A EN LA CIUDAD DE MACHALA. Tesis de grado para la obtención del título Ingeniera de sistemas. Cuenca: Universidad Politécnica Salesina. Sede cuenca. Facultad de Ingeniería. 2013. 53-79p.

[4] DUARTE MARTINEZ, Maria Carolina. DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA. Trabajo de grado presentado como requisito para optar al título de: Especialista en Seguridad Informática. Cúcuta: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2019. 29-56p.

5.2.1 Seguridad Informática. La seguridad Informática abarca procedimientos meticulosos destinados a proteger contra intrusos externos e internos los activos de infraestructura tecnología (Hardware, Software, redes de datos y sistemas de información) con la que cuentas las empresas y son utilizados diariamente para almacenar y procesar la información[5].

Establecer controles tendientes a proteger la infraestructura tecnológica de una empresa. Es de suma importancia en la medida que contendrá las amenazas que puedan poner en riesgo la integridad de estos.

La estrategia que una empresa adopta para proteger sus activos debe estar soportada en estándares internacionales, la cual debe involucrar todos niveles que dentro se estructura jerárquica de la misma. Siempre teniendo la premisa que la seguridad genera confianza sobre los resultados obtenidos.

5.2.2 Seguridad de la Información. La seguridad de la información[6] pretender proporcionar elementos de juicio que permita enfocarse en la importancia del manejo adecuado de la información enmarcado dentro de 3 pilares fundamentales como son: la confidencialidad, la integridad y la disponibilidad, esto generara confianza en las personas que acceden a través de diferentes dispositivos a dicha información almacenada.

5.2.3 Sistema de Gestión de Seguridad de la Información (SGSI). Soportado por la ISO 270017 permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implementar controles y medidas de seguridad adaptados a las necesidades de cada organización. Garantizando la confidencialidad, Integridad y Disponibilidad de la Información.

La importancia de adoptar un SGSI sin importar el tamaño de la organización permitirá establecer politicas de seguridad enfocadas a proporcionar los controles y salvaguardas necesarios para proteger los activos de información y la infraestructura tecnológica con la que cuenta la empresa.

---

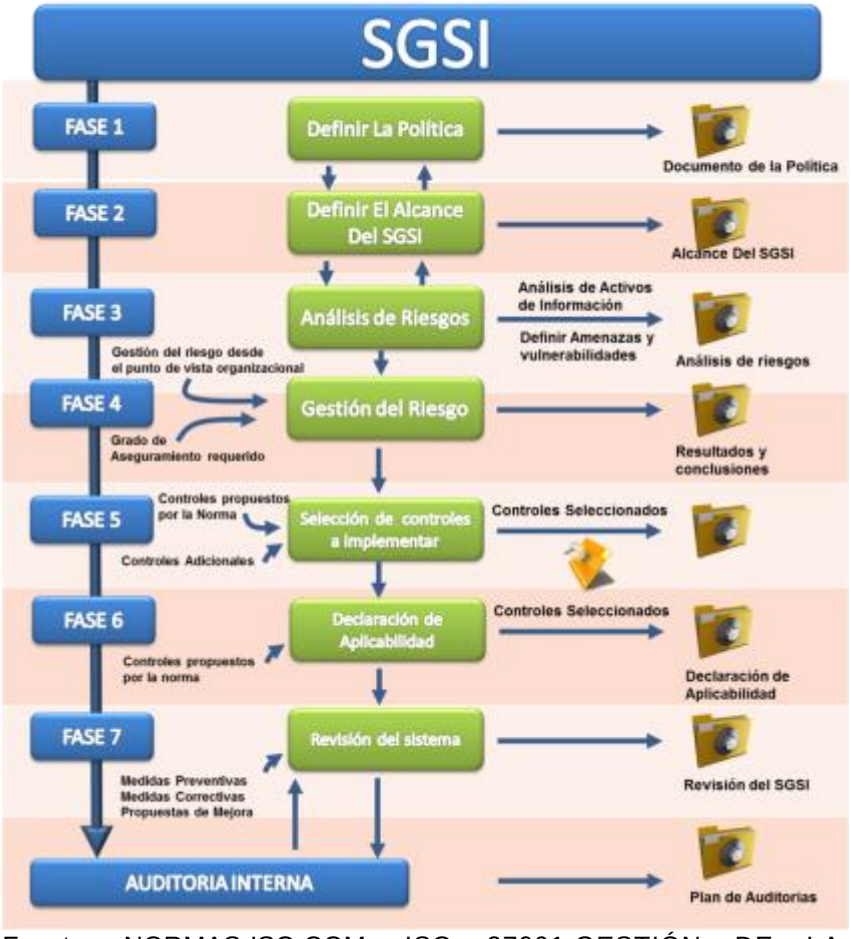
[5] NECTEC.COM. ¿Qué es seguridad informática? (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.netec.com/que-es-seguridad-informatica

[6] NORMAS-ISO.COM. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.normas-iso.com/

7 NORMAS-ISO.COM. ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.normas-iso.com/iso-27001/

Una vez definido el SGSI se debe contar con un proceso de auditoria constante, basado en el ciclo PHVA, el cual permitirá de manera oportuna establecer acciones de mejora a que haya lugar. Teniendo como premisa la protección de la información.

Figura 1. Fases para implementar un SGSI



Fuente: NORMAS-ISO.COM. ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.normas-iso.com/iso-27001/

La Figura 1. Muestra los pasos a seguir al momento de implementar un SGSI tal cual lo define la norma ISO 27001 dentro de una empresa.

5.2.4 Metodología de gestión de riesgo. El análisis y gestión de riesgo es de vital importancia[8] dentro de la implementación de un SGSI en la toda organización que valore y sepa, que la información es un recurso invaluable para la toma de decisiones y transacciones. Ya que proporciona a través de la utilización de una metodología permite el tratamiento e identificación de los riesgos, amenazas y vulnerabilidades a los que puede llegar a estar expuesta los activos información en la empresa. Por otra parte, una adecuada y oportuna gestión del riesgo provee las herramientas necesarias para minimizar o en su defecto eliminar los peligros que rodean no solo la información, sino también demás activos hardware y software con los que cuenta la organización.

La pérdida de información es un alto riesgo a las que están expuestas muchas empresas sino adoptan estrategias contundentes para prevenir, controlar y mitigar los ataque que se pueden llegar a producir por la explotación de las vulnerabilidades que su sistema informático pueda tener. Por ello se debe garantizar a través de una metodología de análisis y gestión del riesgo la incorporación de procedimientos y mecanismos eficaces que disminuyan las amenazas latentes[9].

Una adecuada gestión del riesgo involucra un inventario de activos[10] en su fase inicial, lo que luego nos conduce a una identificación y valoración de las amenazas a los que puede estar expuesta la información. Lo que permitirá proporcionar los elementos de juicio necesarios que contribuyan a la implantación de mecanismos y procedimientos encaminados a salvaguardar la información conservando 3 pilares fundamentales[11] como lo es la confidencialidad, integridad y la disponibilidad de esta.

Para el desarrollo de este proyecto se utiliza una Metodología de Análisis y Gestión de Riesgo como ejemplo: MAGERIT

[8] TORRES, Cesar. Universidad Piloto de Colombia. La Importancia de Realizar un Análisis de Riesgo en las empresas. (En línea) (citado el 15 de abril de 2020). Disponible en: http://polux.unipiloto.edu.co:8080/00003266.pdf

[9] Publicaciones e Investigación. UNAD (2015). Revista Especializada en Ingeniería**.** Metodologías Para el Análisis de Riesgos en los SGSI. (En línea) (citado el 15 de abril de 2020). Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

[10] ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos. (En línea) (citado el 15 de abril de 2020). Recuperado de: https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

[11] MINTIC.GOV. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

5.2.5 Análisis de activo**.** Siendo estos un recurso vital para toda organización es aquí donde se debe identificar y valorar con el ánimo de medir su grado de importancia dentro de la empresa. El análisis de activo[12] proporcionará una información actualizada sobre qué es lo que se debe proteger.

5.3 MARCO CONCEPTUAL

Dentro del proceso investigativo se abordan diferentes conceptos, los cuales son importantes tener claridad:

5.3.1 Seguridad**.** Definida por la Real Academia Española (RAE)[13] como "cualidad de seguro" y seguro como "libre y exento de todo peligro, daño o riesgo"; por lo que se puede decir entonces que seguridad, es la ausencia de riesgo o la confianza en algo o alguien.

5.3.2 Amenazas. Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Así, una amenaza es todo aquello que intenta o pretende destruir. La amenaza se presenta cuando haya una vulnerabilidad[14].

5.3.3 Vulnerabilidades. La vulnerabilidad de un sistema informático son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático[15].

---

[12] Publicaciones e Investigación. UNAD (2015). Revista Especializada en Ingeniería**.** Metodologías Para el Análisis de Riesgos en los SGSI. (En línea) (citado el 15 de abril de 2020). Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

[13] RAE.ES. Real Academia De La Lengua. Diccionario de la lengua española. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://dle.rae.es/seguridad?m=form

[14] SEGURIDADINFORMACTICA.UNLU.EDU.CO. Universidad Nacional de Luján. Departamento de seguridad Informática. Amenazas a la seguridad de la Información. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[15] SEGURIDADINFORMACTICA.UNLU.EDU.CO. Universidad Nacional de Luján. Departamento de seguridad Informática. Amenazas a la seguridad de la Información. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/15

5.3.4 Ataques. Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema. En el flujo normal de la información no debe existir ningún tipo de obstáculos para que la información llegue al destinatario[16].

5.3.5 Confidencialidad. Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

5.3.6 Autenticación. Es el servicio que trata de asegurar que una comunicación sea auténtica[17,] es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.

5.3.7 Integridad. Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado[18].

El sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga, la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.

5.3.8 Control de acceso. Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso de manera física o lógica al sistema de información[19].

16 ECURED.COM. Ataque Informático. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

17 IBM.COM. Identificación y Autenticación. (En línea) (Citado el 16 de abril de 2020). Disponible en:https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm

18 IBM.COM. Integridad de datos. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009780_.htm

19 TECNOSeguro.com. ¿Qué es un Sistema de Control de Acceso? (En línea) (Citado el 15 de abril de 2020). Disponible en:https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

5.3.9 Base de datos. Es una colección de archivos interrelacionados que son creados con un Sistema Manejador de Bases de Datos (DBMS)[20]. El contenido de una base de datos engloba la información concerniente de una organización.

5.3.10 Activo de información. Cualquier elemento hardware, software, y/o información sin importar su medio de almacenamiento. Que tiene un valor para la empresa y por concerniente deben ser protegidos contra factores que puedan afectar su integridad.[21]

5.3.11 Disponibilidad. La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido[22].

5.4 MARCO LEGAL

Con relación a la normatividad involucrada dentro este proyecto tenemos.

5.4.1 ISO 27000. Gestión de la seguridad de la información (Fundamentos y vocabulario). Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI)[23], una descripción del ciclo PDCA, al igual que las definiciones de los términos que se emplean en toda la serie 27000.

5.4.2 ISO/IEC 27001. Especificaciones Para un SGSI. Norma publicada el 15 de Octubre de 2005, donde se enmarcan los requisitos y/o especificaciones del

[20] TICPORTAL.ES. Base de datos. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.ticportal.es/glosario-tic/base-datos-database

[21] NORMAS-ISO.COM. ISO 27001 seguridad de la información .ISO 27001 gestión de la seguridad de la información. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://www.normas-iso.com/iso-27001/

[22] INFOSEGUR.COM. Seguridad Informática. Objetivos de la seguridad informática. (En línea) (Citado el 15 de abril de 2020). Disponible en: https://infosegur.wordpress.com/tag/confidencialidad/

[23] ISO27000.ES. Temas relacionados con los SGSI y la seguridad de la información. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.iso27000.es/

sistema de Gestión de la seguridad de la información[24]. Fue originaria de la BS 7799-2:2002, siendo identificada actualmente como norma ISO 27001:2013, se enuncian los objetivos de control y controles, a ser seleccionadas por las empresas que desean implantar el SGS.

5.4.3 ISO/IEC 27005. Gestión de Riesgos de Seguridad de la Información. Esta norma contiene recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001[25] y está diseñada como soporte para aplicar satisfactoriamente un SGSI basado en un enfoque de gestión de riesgos.

5.4.4 ISO/IEC 27002. Descripción de Controles en Seguridad de la Información. Norma publicada el 1 de julio de 2007. Contiene las recomendaciones para aplicar de manera correcta los controles de seguridad para proteger los activos de información dentro de la empresa. Está compuesta por 39 objetivos, 11 dominios y 113 controles[26].

5.4.5 Ley 1273 del 2009. Se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos[27]. Publicada el 5 de enero de 2009 esta ley modifica el código penal LEY 599 del 2000. La cual crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Lo anterior permite tipificar como delitos informáticos acciones que atenten contra la integridad de la información y se haga un uso inadecuado de las herramientas TIC.

[24] ISO27000.ES. Serie "27000". Requisitos de la norma ISO/IEC 27001. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.iso27000.es/iso27000.html

[25] ISO27000.ES. Serie "27000". Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.iso27000.es/iso27000.html

[26] ISO27000.ES. Serie "27000". Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. (En línea) (Citado el 15 de abril de 2020). Disponible en: http://www.iso27000.es/iso27000.html

[27] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

5.4.6 Ley 1581 del 2012. Por la cual se dictan disposiciones generales para la protección de datos personales[28] Sancionada el 17 de octubre de 2012 esta ley ratifica los derechos que tiene todas las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. Igualmente darle un tratamiento adecuado a dicha información, bajo protocolos de seguridad y confidencialidad.

5.4.7 Decreto 1377 del 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Emitido el 23 de junio de 2013 este decreto provee los lineamientos para poder implementar la LEY 1581 de 2012. Con relación a la política de tratamiento de datos personales, de los encargados y responsables que se involucran en la cadena de la protección de los datos personales[29].

5.5 MARCO CONTEXTUAL

La dependencia objeto para el desarrollo del presente proyecto aplicado es la oficina de Formación Profesional Integral del SENA Regional Guainía. La cual tiene la tarea de ejecutar las acciones pertinentes para el cumplimiento de la misión de la entidad, como lo es el proceso de inscripción, matricula, registro, creación de fichas o programas de formación ya sean presenciales o virtuales, titulados o complementarios.

La coordinación de Formación Profesional Integral cuenta con 14 funcionarios, cada uno con un equipo de cómputo de escritorio asignado, 11 con sistema operativo Windows y 3 con sistemas MAC, se cuenta con 2 impresoras, 1 de red y la otra conectada a un equipo iMAC.

Tabla 1. Tabla relación de activos de información dependencia de formación.

TIPO DE ACTIVO	DESCRIPCIÓN
Activo de	Archivo físico con documentos producidos en la oficina

[28] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.

[29] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (23, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá D.C. El Ministerio. 2013. 11 p.

Información	
PC	11 computadores lenovo, con sistema operativo Windows 10, 4 GB de memoria RAM, 500 BG de HDD.
PC	3 computadores iMAC
Impresora	Impresora Samsung

Tabla 1. (Continuación)

TIPO DE ACTIVO	DESCRIPCIÓN
Personal	Encargado de Ingreso, líder de contrato de aprendizaje, encargado de certificación, administración educativa, coordinador académico, líder SIGA, responsable ambiental, encargado de radicación, coordinador de formación, apoyo a la coordinación de formación, líder de articulación con la educación media, profesional de aseguramiento de la calidad, responsable de PQRS, profesional de diseño curricular.

Fuente: Elaboración propia

La tabla 1 relaciona los activos de información que hace parte de la dependencia de Formación Profesional Integral del Sena Regional Guainía.

Con este proyecto se pretende realizar un análisis en la gestión de riesgo apoyado en la metodología MAGERIT. Con la intención de identificar de manera temprana las amenazas a las que pueden estar sujeto los activos de información y con ello establecer las medidas de protección que sean del caso.

6. DISEÑO METODOLÓGICO

6.1 METODOLOGÍA DE APLICACIÓN

En función al problema planteado y los objetivos que se desean alcanzar en este proyecto aplicado, se abordó una metodología práctica que permitió a partir del hacer, hallar los resultados esperados para el aseguramiento de los activos de información asociados a la dependencia de Formación Profesional Integral del SENA Regional Guainía.

6.2 POBLACIÓN Y MUESTRA

Se consideran todos los funcionarios que laboran en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Como población objeto para la obtención de la información, se contemplan las 14 personas para una muestra del 100% de la población. Distribuidos 1 funcionario por cada cargo de la siguiente forma.

Encargado de Ingreso, líder de contrato de aprendizaje, encargado de certificación, administración educativa, coordinador académico, líder SIGA, responsable ambiental, encargado de radicación, coordinador de formación, apoyo a la coordinación de formación, líder de articulación con la educación media, profesional de aseguramiento de la calidad, responsable de PQRS, profesional de diseño curricular.

6.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la obtención de la información como insumo para el desarrollo del proyecto, se aplicó la técnica de la observación. Que sumada a la experticia profesional, permitiera realizar el inventario de activos, insumo que conlleve a la identificación de las vulnerabilidades presentes sobre cada activo de información. Igualmente, se realizó a través de la entrevista. La valoración de los activos de información conforme lo requiera la metodología MAGERIT.

6.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo de este proyecto se utilizó la metodología MAGERIT como estrategia procedimental para la identificación y gestión de los riesgos, vulnerabilidades y amenazas asociados a los activos de información presentes en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Con el objetivo de finalizar exitosamente dicho proyecto y establecer medidas tendientes a proteger los activos de información. Se desarrollaron una serie de actividades que se encuentran alineadas a las siguientes fases:

- ✓ Fase 1: Identificación de los activos de información presentes en la Dependencia Formación Profesional Integral del SENA Regional Guainía.

Actividad 1. Identificación y clasificación de activos de información: Se realizará una identificación de activos de información dentro de la dependencia. Luego de identificar los activos se procederá a realizar una organización de cada uno de ellos a partir de la clasificación de activos que determinar MAGERIT.

- ✓ Fase 2: Establecimiento de los riesgos, vulnerabilidades y amenazas en los activos de información de la dependencia de formación.

Actividad 1. Identificación de vulnerabilidades, amenazas y riesgos: Se realizará una identificación (Vulnerabilidades, amenazas y riesgos) y valoración de cada uno de los activos de acuerdo a la metodología MAGERIT.

- ✓ Fase 3: Diseño de un plan de tratamiento de riesgos y vulnerabilidades detectados a los activos de información.

Actividad 1. Plan de tratamiento de riesgo: A partir de las vulnerabilidades detectadas para cada activo de información. Se establecen las salvaguardas y controles necesarios que permita disminuir y controlar el riesgo.

7. APLICACIÓN DE LA METODOLOGÍA

Durante el desarrollo de este capítulo abordaremos en orden secuencial la aplicación de la metodología MAGERIT conforme los objetivos propuestos. Para poder así establecer a partir de la norma los controles tendientes a proteger los activos de información de la dependencia de Formación Profesional Integral del SENA Regional Guainía.

7.1 METODOLOGÍA DE GESTIÓN DE RIESGO

Para el análisis y gestión del riesgo de los activos de información y la infraestructura tecnológica perteneciente a la dependencia de Formación Profesional Integral del SENA Regional Guainía. Se tiene contemplado utilizar la metodología MAGERIT. La cual presenta las siguientes ventajas.

- ✓ Alcance completo en el análisis y gestión de riesgo.
- ✓ Documentación suficiente con relación a recursos de información, amenazas y tipos de activos.
- ✓ Utiliza un completo análisis de riesgo cuantitativo y cualitativo.
- ✓ Es libre y no requiere autorización para su uso.
- ✓ Divide los activos y así poder realizar una valoración de riesgo oportuna sobre cada uno.
- ✓ Posee una herramienta de software llamada PILAR, para el análisis de riesgo.
- ✓ Tiene una base documental compuesta de 3 módulos para ser consultada.
- ✓ Involucra tres objetivos a tener en cuenta durante para su implementación

El objetivo es realizar un inventario de activos, un análisis de riesgo para determinar las amenazas o vulnerabilidades a las que están expuestos los activos de información con los que cuenta la dependencia y así poder determinar las salvaguardas que propicien las medidas de seguridad a dichos activos.

Para lo cual se trabajará con el libro 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8 de MAGERIT donde describe la característica de los activos (identificación, dependencia y valoración).

Figura 2. Pasos aplicación metodología MAGERIT

Fuente: Elaboración Propia

En la figura 2 podemos observar los pasos que se debe seguir dependiendo el objetivo propuesta la aplicación dentro de una empresa la metodología MAGERIT.

7.2 ALCANCE DEL ANÁLISIS

El alcance para la aplicación de la metodología MAGERIT dentro del proyecto que involucra la oficina de formación. Partirá con la identificación de los riesgos a los que están expuestos los activos de información y la infraestructura tecnológica de la dependencia de formación. Para luego definir un plan de tratamiento de riesgo, que permita la adopción de medidas de seguridad. Tendientes a minimizar o en su defecto controlar las vulnerabilidades y amenazas que pueden llegar a afectar dichos activos. Favoreciendo así la continuidad de la operación y garantizar la aplicación de controles que aseguren la información, los dispositivos, los servicios y el software que utilizan.

7.3 FASE 1

7.3.1 Identificación y clasificación de activos. Dando cumplimiento a la metodología MAGERIT como primer paso. Dentro del proceso de gestión del riesgo. Es la **IDENTIFICACIÓN DE LOS ACTIVOS** de información a los cuales posteriormente se le realizará la valoración. Para poder así determinar los riesgos y amenazas asociadas.

Tabla 2. Clasificación de Activos según MAGERIT

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	1. [BD_SISAGRI] Base Datos SISAGRI.
	2. [BD_PREC] Base Datos Precios.
	3. [BD_TRADOC] Base Datos Trámite Documentario.
	4. [BD_PDT_PLANI] Base de datos del PDT Planilla Electrónica.
	5. [COD_FU] Código Fuente del Portal Web
SERVICIOS	6. [SERV_INFOR] Servicio de información a agricultores, instituciones públicas, ONGs y público en general.
	7. [SERV_EMI_REP] Emisión de reportes al INEI, BCRP y al Ministerio de Agricultura.
	8. [SERV_PLANIL] Formular y elaborar la planilla única de sueldos de personal activo y cesante.
	9. [SERV_CONT_INST] Registrar las operaciones contables y patrimoniales de la institución.
	10. [SERV_PRESU] Formular los Estados Financieros y Presupuestarios de periodicidad mensual, trimestral y anual.
	11. [SERV_ADQUISI] Adquirir, Almacenar y distribuir los bienes a la institución.
	12. [SERV_TRA_DOC] Servicio de tramitación documentaria.
	13. [POR_WEB] Portal Web.
	14. [SI_SISAP] Sistema de Información de Abastecimiento y Precios (SISAP).
	15. [SI_SISPECE] Sistema Pecuario Extensivo (SISPECE).
	16. [SI_SISAGRI] Sistema Agrícola (SISAGRI)
	17. [SI _PRECIOS] Sistema Informático de Precios
APLICACIONES	18. [SI_TRADOC] Sistema informático de Tramite Documentario

Tabla 2. (Continuación)

TIPO	NOMBRE DEL ACTIVO
APLICACIONES	19. [SI_SIAF] Sistema Integrado de Administración Financiera (SIAF).
	20. [SI _PDT] PDT Planilla Electrónica
	21. [SI _SEACE] Sistema Electrónico de Adquisiciones y Contrataciones del Estado (SEACE).
	22. [SO] Sistema Operativo.
	23. [HER_OFI] Herramientas de ofimática.
	24. [ANT_VIR] Anti virus.
EQUIPAMIENTO INFORMÁTICO	25. [SRV_FIRE] Servidor de Firewall.
	26. [PC] Computadora.
REDES DE COMUNICACIONES	27. [ADSL] Conexión a internet.
EQUIPAMIENTO AUXILIAR	28. [CAB_RED] Cableado de Red.
INSTALACIONES	29. [LOCAL] Local de la DRAC.
	30. [GABI] Gabinete de Red
PERSONAL	31. [ESP_EST_III] Especialista en Estadística e Informática III.
	32. [ESP_ADM_IV] Especialista Administrativo IV.
	33. [TEC_FIN_III] Técnico en Finanzas III.
	34. [TEC_ADM_I] Técnico Administrativo I.
	35. [TEC_ADM_III] Técnico Administrativo III.
	36. [ESP_ADM_II] Especialista Administrativo II.

Fuente. 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8

En la tabla 2 se puede observar cómo se clasifican los activos dentro una empresa teniendo en cuanta lo dispuesto por la metodología MAGERIT.

Se procede a identificar que en la dependencia de formación se encuentran los siguientes activos de información e infraestructura tecnológica los cuales soportan la operación para el desarrollo de las actividades que realizan en cumplimiento de la misión institucional.

Tabla 3. Tabla de identificación de los activos de Formación.

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	[BD_TRADOC] Se cuenta con un archivo físico en donde se guardan las solicitudes tramitadas, los informes de ejecución de los instructores, documentos de certificación de los aprendices, de las matrículas y documentos producidos en la dependencia.
SERVICIOS	[SERV_ADQUISI] Se almacenan y distribuyen los materiales de formación a los instructores de cada programa en ejecución.
	[SERV_INFOR] Se informa a la población en general sobre programas de formación y si le da respuesta a QPRS se son radicadas que involucren a los aprendices, instructores, matriculas, e inscripciones a programas técnicos, tecnólogos y complementarios.
APLICACIONES	[POR_WEB] Se cuenta con un aplicativo llamado Sofia Plus www.senasofiaplus.edu.co
	[SO] Los equipos de cómputo cuentan con Sistema Operativo
	[ANT_VIR] Los computadores cuentan con programa antivirus.
EQUIPAMIENTO INFORMÁTICO	[PC] La dependencia de formación cuenta con 14 computadores de escritorio.
REDES DE COMUNICACIONES	[ADSL] La dependencia cuenta con una conexión a internet.
EQUIPAMIENTO AUXILIAR	[CAB_RED] La oficina cuenta con una distribución de cableado a cada uno de los equipos.
INSTALACIONES	[GABI] Dentro de la dependencia se encuentra un gabinete para recepcionar y distribuir el cableado a cada equipo.
PERSONAL	[ESP_ADM_IV] Hacen parte de la dependencia de formación 14 funcionarios que realizan procesos administrativos. Según su cargo.

Fuente. Elaboración Propia

Como se puede observar en la tabla 3 se realizó la identificación de los principales activos que hacen parte de la dependencia de Formación Profesional Integral.

7.3.2 Descripción de los activos. A continuación, se describen los diferentes tipos acticos de información identificados dentro de la dependencia de formación. Aplicando la metodología MAGERIT, y a la vez el responsable asignado al mismo.

Tabla 4. Tabla descripción de los Activos de Información

ACTIVO	DESCRIPCIÓN	RESPONSABLE
[HW] Computador de escritorio	Computador Lenovo, Procesador Intel i7, con sistema operativo Windows 10 pro, 4 GB de memoria RAM, 500 BG de HDD, pantalla de 14".	Funcionario encargado de Ingreso
		Líder de contrato de aprendizaje
		Líder SIGA "Sistema Integrado de Gestión y Autocontrol"
		Líder componente ambiental
		Encargado de Certificación.
		Encargado de Certificación.
		Encargado de Radicación
		Encargado de PQRS
		Encargado de diseño curricular
		Líder de articulación con la educación media
		Apoyo a la coordinación de formación profesional.
	Computador iMAC, Intel Core i5 dual core de 2.3 GHz, pantalla de 21.5", memoria de 8 GB DDR4, 1024 GB de HHD.	Coordinador de Formación Profesional Integral.
		Profesional de aseguramiento de la calidad.
		Coordinador académico
[HW] Impresora de Red	Samsung Multi Xpress M5370LX	Soporte en Sitio
[D] Archivo	Archivo donde se almacena en físico información producida en la dependencia.	Coordinador de formación Profesional Integral.

Tabla 4. (Continuación)

ACTIVO	DESCRIPCIÓN	RESPONSABLE
[S] Servicio	Recepción y respuesta de PQRS a usuarios externos e internos.	Encargado de PQRS
	Administración de materiales de formación.	Coordinador académico
	Registro, inscripción, matricula a programas de formación SENA.	Funcionario encargado de Ingreso
[SW] Antivirus	Programa informático destinado a proteger los PC de archivos maliciosos.	Soporte en Sitio
[SW] Aplicativo de Gestión.	Sofía Plus gestiona los procesos formativos.	DG a través de la oficina de sistema.
[COM] Gabinete de red	Distribución donde se organizan dispositivos de interconexión.	Soporte en Sitio
[COM] Cableado de red	Tendido de cables para conexión a los equipos de cómputo.	

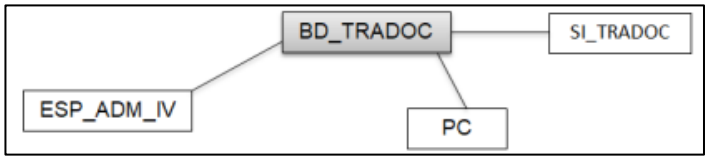
Fuente. Dependencia de Formación Profesional Integral SENA Regional Guainía

7.3.3 Dependencia de Activos. Posterior a la identificación de los activos de información y la infraestructura tecnológica, con la que cuenta la dependencia de Formación Profesional Integral del SENA Regional Guainía. Se procede a realizar la dependencia que hay entre dichos activos. Lo anterior teniendo en cuenta la metodología MAGERIT.

7.3.3.1 Dependencia de activos tipo datos / información. Se realiza la dependencia del archivo en físico con el que cuenta la oficina de formación teniendo en cuenta.

- Los funcionarios que tienen acceso
- Los equipos que lo permiten
- El sistema de información que lo genera

Figura 3: Dependencia de activos tipo datos / información

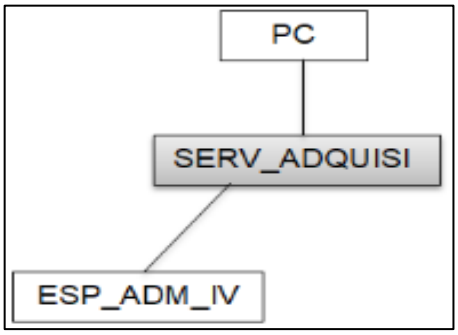


Fuente: Elaboración Propia

7.3.3.2 Dependencia de activos tipo servicios. Se realiza la dependencia del servicio tipo SERV_ADQUISI con el que cuenta la oficina de formación teniendo en cuenta.

- Los funcionarios que tienen acceso
- Los equipos que lo utilizan

Figura 4. Dependencia de activos tipo servicios 1

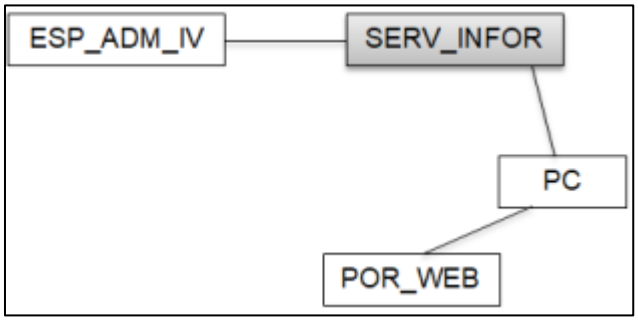


Fuente: Elaboración Propia

Se realiza la dependencia del servicio tipo SERV_INFOR con el que cuenta la oficina de formación teniendo en cuenta.

- Los funcionarios del que dependen
- Los equipos que lo utilizan
- La aplicación que lo sustenta

Figura 5. Dependencia de activos tipo servicios 2

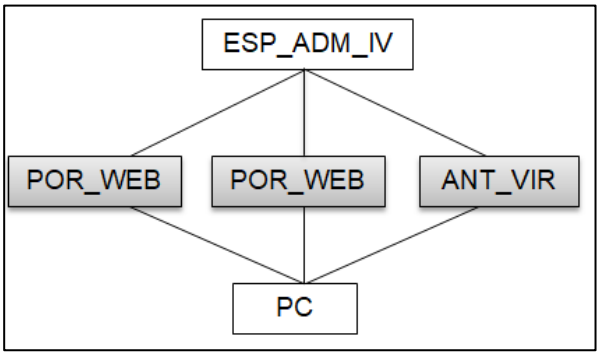


Fuente: Elaboración Propia

7.3.3.3 Dependencia de activos tipo aplicaciones. Se realiza la dependencia del activo tipo aplicación con el que cuenta la oficina de formación teniendo en cuenta.

- Los funcionarios que tiene acceso.
- Los equipos que lo utilizan

Figura 6. Dependencia de activos tipo aplicaciones

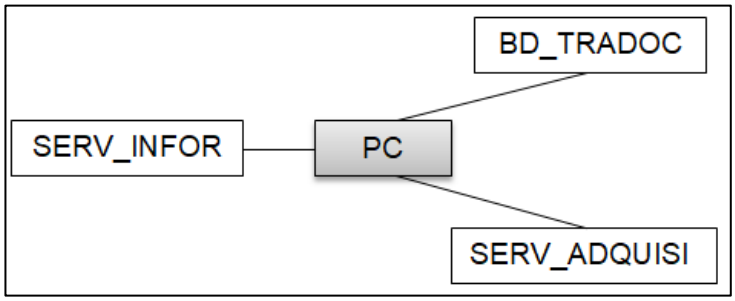


Fuente: Elaboración Propia

7.3.3.4 Dependencia de activos tipo equipamiento informático. Se realiza la dependencia del activo de información con el que cuenta la oficina de formación teniendo en cuenta.

- Los servicios que facilita.
- La información que habilita

Figura 7. Dependencia de activos tipo equipamiento informático

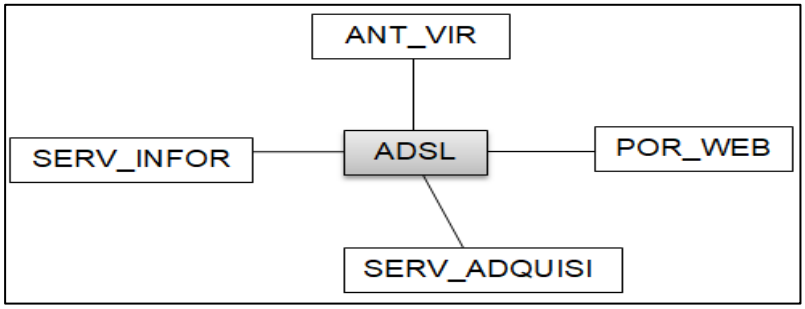


Fuente: Elaboración Propia

7.3.3.5 Dependencia de activo tipo redes de comunicaciones. Se realiza la dependencia del activo de información con el que cuenta la oficina de formación teniendo en cuenta.

- Los servicios que facilita.
- Los programas que habilita.

Figura 8. Dependencia de activo tipo redes de comunicaciones

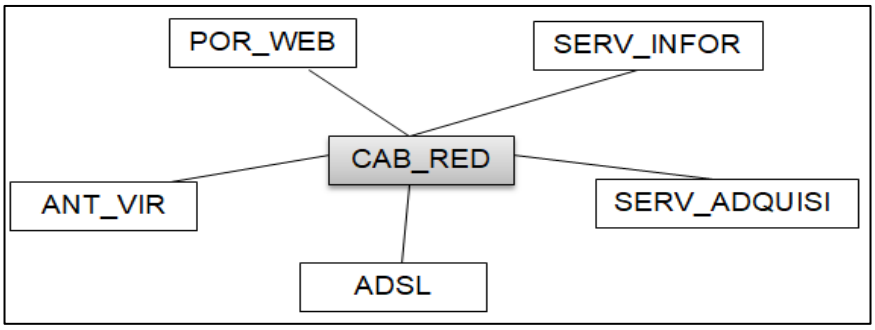


Fuente: Elaboración Propia

7.3.3.6 Dependencia de activos tipo equipamiento auxiliar. Se realiza la dependencia de activos de información según los que soporta. Teniendo en cuenta.

- Los servicios que facilita.
- Las aplicaciones que habilita
- La red de comunicación que soporta

Figura 9. Dependencia de activos tipo equipamiento auxiliar

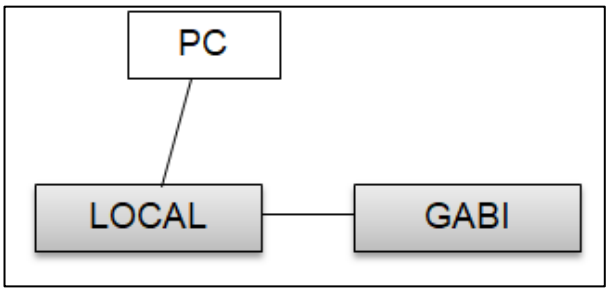


Fuente: Elaboración Propia

7.3.3.7 Dependencia de activos tipo instalaciones. Se realiza la dependencia de activos de información según los que soporta. Teniendo en cuenta.

- Los equipos de cómputo con los que cuenta.

Figura 10. Dependencia de activos tipo instalaciones

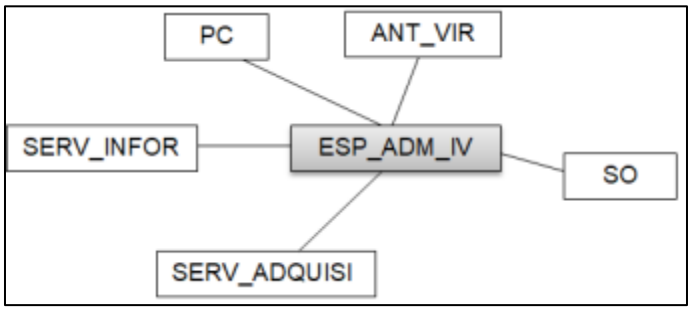


Fuente: Elaboración Propia

7.3.3.8 Dependencia de activos tipo personal. Se realiza la dependencia de activos de información según los que son soportados por él. Teniendo en cuenta.

- La información a la que tiene acceso.
- Las aplicaciones que utiliza.
- Los equipo de cómputo que maneja.
- Los servicios que maneja.

Figura 11. Dependencia de activos tipo personal



Fuente: Elaboración Propia

7.3.4 Valoración de activos. Según la metodología MAGERIT Para valorar los activos de información pertenecientes a la dependencia de Formación Profesional Integral del SENA Regional Guainía. Se tiene en cuenta la siguiente información.

7.3.4.1 Dimensiones de seguridad

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A_S] autenticidad de los usuarios del servicio

[A_D] autenticidad del origen de los datos

[T_S] trazabilidad del servicio

[T_D] trazabilidad de los datos

7.3.4.2 Criterios de valoración.

Tabla 5. Tabla de criterios para valoración de activos

Valor			**Criterio**
10	Muy alto	MA	Daño muy grave a la organización.
7-9	Alto	A	Daño grave a la organización.
4-6	Medio	M	Daño importante a la organización.
1-3	Bajo	B	Daño menor a la organización.

Tabla 5. (Continuación)

Valor			Criterio
0	Despreciable	D	Irrelevante a efectos prácticos.

Fuente. 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8

7.3.4.3 Valoración de activos de información. A continuación, se realiza la valoración, teniendo en cuenta la metodología MAGERIT de los activos asociados a la dependencia de Formación Profesional Integral del SENA Regional Guainía.

Tabla 6. Tabla valoración de activos dependencia de Formación.

Tipo	Activo	Dimensiones de Seguridad						
		D	I	C	A_S	A_D	T_S	T_D
DATOS / INFORMACION	[BD_TRADOC] Archivo físico donde se guarda información producida por la dependencia.	5	5	5		3		
SERVICIOS	[SERV_ADQUISI] Distribución materiales de formación a los instructores de cada programa en ejecución.	3	5	4			4	
	[SERV_INFOR] Atención a clientes internos y externos sobre PQRS y solicitudes de formación.	5	3	8		5	3	
APLICACIONES	[POR_WEB] Portal web con la que se tramitan los programas de formación.	10	8	5		4		

Tabla 6. (Continuación)

Tipo	Activo	Dimensiones de Seguridad						
		D	I	C	A_S	A_D	T_S	T_D
APLICACIONES	[SO] Sistema operativo con lo que cuentan los PC.	10	9	5		3		
	[ANT_VIR] Software antivirus con los que cuentan algunos PC.	3	6	5				
EQUIPAMIENTO INFORMATICO	[PC] Equipos de cómputo con los que cuenta la dependencia de formación.	8	4	5				
REDES DE COMUNICACIONES	[ADSL] Conexión a internet que soporta la operación de la dependencia.	10	6	5			3	
EQUIPAMIENTO AUXILIAR	[CAB_RED] Tendidos de cable para la conexión a internet de los PC.	10	4	5				
INSTALACIONES	[GABI] La dependencia posee un IDF para distribuir el cableado de Red	10	5	5				
PERSONAL	[ESP_ADM_IV] Representa los 14 funcionarios que hacen parte de la dependencia de formación.	10	8	8		5		

Fuente. 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8

7.4 FASE 2.

Establecimiento de los riesgos, vulnerabilidades y amenazas en los activos de información de la dependencia de formación.

7.4.1 Clasificación de amenaza a los activos.

De acuerdo a lo descrito en la metodología MAGERIT las amenazas a las que puede estar expuesto un activo de información o la infraestructura tecnológica de una empresa se agrupan en 4. Como se muestra a continuación.

Tabla 7. Tabla clasificación amenazas

[N] Desastres naturales	**[I] De origen industrial**	**[E] Errores y fallos no intencionados**	**[A]Ataques deliberados**
[N.1] Fuego	[I.1] Fuego	[E.1] Errores de los usuarios	[A.4] Manipulación de la configuración
[N.2] Daños por agua	[I.2] Daños por agua	[E.2] Errores del administrador	[A.5] Suplantación de la identidad del usuario
[N.3] Desastres naturales	[I.3] Contaminación mecánica	[E.3] Errores de monitorización (log)	[A.6] Abuso de privilegios de acceso
	[I.4] Contaminación electromagnética	[E.4] Errores de configuración	[A.7] Uso no previsto
	[I.5] Avería de origen físico o lógico	[E.7] Deficiencias en la organización	[A.8] Difusión de software dañino
	[I.6] Corte del suministro eléctrico	[E.8] Difusión de software dañino	[A.9] [Re-]encaminamiento de mensajes
	[I.7] Condiciones inadecuadas de temperatura o humedad	[E.9] Errores de [re-]encaminamiento	[A.10] Alteración de secuencia
	[I.8] Fallo de servicios de comunicaciones	[E.10] Errores de secuencia	[A.11] Acceso no autorizado
		[E.14] Fugas de información	[A.12] Análisis de tráfico
		[E.15] Alteración de la información	[A.13] Repudio
			[A.14] Interceptación de información (escucha)

Tabla 7. (Continuación)

[N] Desastres naturales	**[I] De origen industrial**	**[E] Errores y fallos no intencionados**	**[A]Ataques deliberados**
[N.1] Fuego [N.2] Daños por agua [N.3] Desastres naturales	[I.9] Interrupción de otros servicios o suministros esenciales [I.10]Degradación de los soportes de almacenamiento [I.11] Emanaciones electromagnéticas	[E.16] Introducción de falsa información [E.17]Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.26] Indisponibilidad del personal	[A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Fuente. 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8

7.4.2 Identificación de las amenazas de los activos. Se procede a asociar las amenazas más prominentes identificadas sobre cada activo de información de la dependencia de formación.

Tabla 8. Tabla identificación de amenazas de los activos de información.

TIPO	ACTIVO	AMENAZA
DATOS / INFORMACION	[BD_TRADOC] Archivo Central	[A.19] Divulgación de información.
		[A.11] Acceso no autorizado
		[I.7] Condiciones inadecuadas de temperatura o humedad
SERVICIOS	[SERV_ADQUISI] Administración de materiales de formación.	[A.11] Acceso no autorizado
		[A.28] Indisponibilidad del personal
	[SERV_INFOR] Atención a usuarios internos o externos y respuesta PQRS.	[E.26] Indisponibilidad del personal
		[I.7] Condiciones inadecuadas de temperatura o humedad
APLICACIONES	[POR_WEB] Plataforma Web para la gestión de la formación.	[E.4] Errores de configuración.
		[I.5] Avería de origen físico o lógico.
		[I.8] Fallo de servicios de comunicaciones
		[A.24] Denegación de servicio
		[E.21] Errores de mantenimiento / actualización de programas (software).
		[E.24] Caída del sistema por agotamiento de recursos.

Tabla 8. (Continuación)

TIPO	ACTIVO	AMENAZA
APLICACIONES	[SO] Sistema operativo que administra los PC.	[E.21] Errores de mantenimiento / actualización de programas (software).
		[E.8] Difusión de software dañino.
		[E.4] Errores de configuración.
		[E.1] Errores de los usuarios
	[ANT_VIR] Programa antivirus.	[E.21] Errores de mantenimiento / actualización de programas (software)
		[E.20] Vulnerabilidades de los programas (software).
		[E.4] Errores de configuración
		[E.1] Errores de los usuarios.
EQUIPAMIENTO INFORMATICO	[PC] Equipo de cómputo de cada funcionario de la dependencia de formación.	[N.3] Desastres naturales.
		[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[A.15] Modificación de información.
		[A.17] Corrupción de la información.
		[A.19] Divulgación de información.
		[E.21] Errores de mantenimiento / actualización de programas (software).

Tabla 8. (Continuación)

TIPO	ACTIVO	AMENAZA
EQUIPAMIENTO INFORMATICO	[PC] Equipo de cómputo de cada funcionario de la dependencia de formación.	[E.23] Errores de mantenimiento / actualización de equipos (hardware).
		[I.6] Corte del suministro eléctrico.
		[E.8] Difusión de software dañino.
	Impresora de Red Samsung.	[E.14] Fugas de información.
		[E.8] Difusión de software dañino.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[I.6] Corte del suministro eléctrico.
		[I.5] Avería de origen físico o lógico.
		[A.11] Acceso no autorizado.
REDES DE COMUNICACIONES	[ADSL] La dependencia cuenta con una conexión a internet.	[I.8] Fallo de servicios de comunicaciones.
EQUIPAMIENTO AUXILIAR	[CAB_RED] Tendido del cable de Red.	[I.8] Fallo de servicios de comunicaciones.
		[I.7] Condiciones inadecuadas de temperatura o humedad.

Tabla 8. (Continuación)

TIPO	ACTIVO	AMENAZA
INSTALACIONES	[GABI] Dentro de la dependencia se encuentra un gabinete para recepcionar y distribuir el cableado a cada equipo.	[I.6] Corte del suministro eléctrico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[N.3] Desastres naturales.
		[E.4] Errores de configuración.
PERSONAL	[ESP_ADM_IV]Personal administrativo que labora en la dependencia.	[A.7] Uso no previsto
		[A.11] Acceso no autorizado.
		[A.22] Manipulación de programas.
		[A.28] Indisponibilidad del personal
		[A.30] Ingeniería social (picaresca)

Fuente. Dependencia de Formación Profesional Integral

7.4.3 Matriz de riesgos. A continuación, se relacionan las vulnerabilidades, amenazas y riesgos. Prominentes asociadas a los diferentes activos de información y la infraestructura tecnológica con la que cuenta la dependencia de formación.

Tabla 9. Tabla matriz de riesgo

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
DATOS / INFORMACION	[BD_TRADOC] Archivo Central	Archivo físico donde se guarda información producida por la dependencia.	Falta de mecanismos control de acceso	[A.19] Divulgación de información	Robo, pérdida o adulteración de información.
				[A.11] Acceso no autorizado	Perdida de Información
			Inadecuada ubicación del archivo físico	[I.7] Condiciones inadecuadas de temperatura o humedad	Deterioro de los archivos

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
SERVICIOS	[SERV_ADQUISI] Administración de materiales de formación.	Distribución de materiales de formación a los instructores de cada programa en ejecución.	Mala ubicación donde se guardan los materiales de formación.	[A.11] Acceso no autorizado	Robo de materiales de formación
			Falta de mecanismos de control durante la asignación al instructor.	[A.28] Indisponibilidad del personal	Algunos programas no reciben la totalidad de materiales de formación
	[SERV_INFOR] Atención a usuarios internos o externos y respuesta PQRS.	Atención a clientes internos y externos sobre PQRS y solicitudes de formación.	No sé suministre la información apropiada y de manera pertinente	[E.26] Indisponibilidad del personal	Pérdida de confianza y acceso a la información
			Perdida de radicados.		Falta de eficiencia para general las respuesta

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
SERVICIOS	[SERV_INFOR] Atención a usuarios internos o externos y respuesta PQRS.	Atención a clientes internos y externos sobre PQRS y solicitudes de formación.	Inadecuada ubicación del funcionario	[I.7] Condiciones inadecuadas de temperatura o humedad	Inadecuada prestación del servicio
APLICACIONES	[POR_WEB] Plataforma Web para la gestión de la formación.	Se cuenta con un aplicativo llamado Sofía Plus www.senasofiaplus.edu.co	Ataques de inyección de SQL	[E.4] Errores de configuración	Caída del sistema
			Denegación al acceso	[I.5] Avería de origen físico o lógico	Falta de acceso al aplicativo
			Ataques de denegación de servicios	[I.8] Fallo de servicios de comunicaciones	Inadecuada prestación del servicio
				[A.24] Denegación de servicio	Indisponibilidad de servicio.
				[E.21] Errores de mantenimiento / actualización de programas (software)	
	[SO] Sistema operativo que administra los PC.	Sistema operativo Windows 10 Pro con los que cuentas los PC.	Falta de mantenimiento preventivo a los recursos	[E.24] Caída del sistema por agotamiento de recursos	Indisponibilidad para usar el PC

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
APLICACIONES	[SO] Sistema operativo que administra los PC.	Sistema operativo Windows 10 Pro con los que cuentas los PC.	Falta de instalación de parches de seguridad.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, pérdida o adulteración de información.
			Acceso no autorizado por la inadecuada administración de los puertos		
			Acceso no autorizado	[E.8] Difusión de software dañino	
			Habilitación de brechas de seguridad	[E.4] Errores de configuración	Inadecuada utilización de las opciones del sistema o herramientas de software
			Mal funcionamiento del sistema	[E.1] Errores de los usuarios	
	[ANT_VIR] Software Antivirus	Programa para la detección de archivos maliciosos	Inoperancia del programa dejando expuesto el PC.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, perdida o adulteración de información o del sistema
			Acceso no autorizado	[E.20] Vulnerabilidades de los programas (software)	

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
APLICACIONES	[ANT_VIR] Software Antivirus	Programa para la detección de archivos maliciosos	Deshabilitar el escaneo a páginas de internet	[E.4] Errores de configuración	Robo, perdida o adulteración de información o del sistema
EQUIPAMIENTO INFORMATICO	[PC] Equipo de Computo	Equipo de cómputo de cada funcionario de la dependencia de formación.	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[E.1] Errores de los usuarios	
			No contar con politicas de respaldo de la información	[N.3] Desastres naturales	Robo, perdida o adulteración de información
			Intermitencia en el desarrollo de las actividades a cargo.	[I.5] Avería de origen físico o lógico	Indisponibilidad en el uso del equipo
				[A.17] Corrupción de la información	
				[A.19] Divulgación de información	
			Instalación o habilitación de software malicioso	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuado funcionamiento del Equipo de computo

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
EQUIPAMIENTO INFORMATICO	[PC] Equipo de Computo	Equipo de cómputo de cada funcionario de la dependencia de formación.	Habilitación de brechas de seguridad (puertos)	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuado funcionamiento del Equipo de computo
			Inoperancia del equipo de cómputo y acceso a información.	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Deficiencia en la prestación de un servicio por el no uso del PC
			Daño parcial o permanente en el equipo de cómputo.	[I.6] Corte del suministro eléctrico	Daño en componentes físicos o corrupción de archivos
			Acceso no autorizado	[E.8] Difusión de software dañino	Afectación en la integridad de los archivos
	Impresora de Red	Samsung Multi Xpress M5370LX	Se represan los documentos impresos en la bandeja de salida	[E.14] Fugas de información	Robo o Pérdida de Información.

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
EQUIPAMIENTO INFORMATICO	Impresora de Red	Samsung Multi Xpress M5370LX	Cuando se imprime por USB esta se contamina con virus	[E.8] Difusión de software dañino	Copiar los virus a los equipos de computo
			Indisponibilidad en el funcionamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	Afectación en el uso del servicio
			Interrupción en el Servicio	[I.6] Corte del suministro eléctrico	
			Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico	
			Vulnerabilidad de tipo OpenSSL	[A.11] Acceso no autorizado	
REDES DE COMUNICACIONES	[ADSL] Internet	La dependencia cuenta con una conexión a internet.	Lentitud en el servicio de comunicación.	[I.8] Fallo de servicios de comunicaciones	Afectación en la calidad y pertinencia del servicio y/o la información.
			Intermitencia en el servicio.		
			Caída en parcial o total en el servicio.		
EQUIPAMIENTO AUXILIAR	[CAB_RED] Tendido del cable de Red.	Tendido de cable de Red, para la conexión a internet de los PC.	El tendido de cable no cumple según la normatividad vigente.	[I.8] Fallo de servicios de comunicaciones	Afectación tránsito de la información y acceso a internet

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
EQUIPAMIENTO AUXILIAR	[CAB_RED] Tendido del cable de Red.	Tendido de cable de Red, para la conexión a internet de los PC.	Corrupción en los cables de Red	[I.7] Condiciones inadecuadas de temperatura o humedad	Afectación tránsito de la información y acceso a internet
INSTALACIONES	[GABI] IDF centro de cableado	Gabinete para recepcionar y distribuir el cableado de red a cada equipo.	Caída total o parcial del servicio de internet	[I.6] Corte del suministro eléctrico	Afectación en la prestación del servicio que depende de internet.
			Deterioro en la vida útil de los componentes físicos	[I.7] Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran
			Caída total o parcial del servicio de internet	[N.3] Desastres naturales	Afectación en la prestación del servicio que depende de internet.
			Deficiencia en el acceso a las plataformas web.	[E.4] Errores de configuración	Acceso limitado a la información y deterioro en la prestación del servicio
PERSONAL	[ESP_ADM_IV] Funcionarios	Personal administrativo que labora en la dependencia.	Uso inadecuado de los permisos otorgados y recursos	[A.7] Uso no previsto	Ineficiencia en el uso de los recursos

Tabla 9. (Continuación)

TIPO	ACTIVO	DESCRIPCIÓN	VULNERABILIDAD	AMENAZAS	RIESGO
PERSONAL	[ESP_ADM_IV] Funcionarios	Personal administrativo que labora en la dependencia.	Acceder sin contar con los privilegios a equipos de cómputo o información física	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información
			Instalación y uso de programas no autorizados que pueden habilitar el ingreso de archivos maliciosos o acceso no autorizados	[A.22] Manipulación de programas	
			No asumir su Rol frente a la protección de la información.	[A.28] Indisponibilidad del personal	Afectación en la prestación del servicio, manipulación de información.
			Acceso de Información confidencial por parte de terceros no autorizados	[A.30] Ingeniería social (picaresca)	Robo, perdida o adulteración de información

Fuente. Dependencia de Formación Profesional Integral

7.4.4 Evaluación del riesgo. Posterior a la identificación de las amenazas y riesgos asociados a cada activo de información. Se realiza a través de la metodología MAGERIT la valoración de riesgos.

El impacto está dado por la frecuencia en que se puede llegar a presentar un incidente sobre un activo de información.

Tabla 10. Tabla impacto en el riesgo

IMPACTO		
Nomenclatura	**Categoría**	**Valoración**
MA	**Muy Alto**	5
A	**Alto**	4
M	**Medio**	3
B	**Bajo**	2
MB	**Muy Bajo**	1

Fuente. Curso de Análisis y gestión de Riesgos – Especialización en Seguridad Informática – UNAD. Año 2019

Tabla 11. Tabla probabilidad de ocurrencia del riesgo

PROBABILIDAD DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**Muy raro**	1

Fuente. Curso de Análisis y gestión de Riesgos – Especialización en Seguridad Informática – UNAD. Año 2019

Dentro de la valoración para determinar el riesgo que recae sobre un activo, se utiliza la siguiente formula.

RIESGO = PROBABILIDAD * IMPACTO

Tabla 12. Tabla formula del riesgo

IMPACTO	**MA**	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		PROBABILIDAD				

Fuente. Curso de Análisis y gestión de Riesgos – Especialización en Seguridad Informática – UNAD. Año 2019

Tabla 13. Tabla valoración del riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Valoración del riesgo	MA	**Crítico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente. Curso de Análisis y gestión de Riesgos – Especialización en Seguridad Informática – UNAD. Año 2019

Teniendo en cuenta las tablas relacionada con anterioridad, se calcula el nivel de riesgo al que expuesto en términos de ocurrencia e impacto. Como se muestra a continuación.

Tabla 14. Valoración de riesgos sobre los activos

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[BD_TRADOC] Archivo Central	Falta de mecanismos control de acceso	[A.19] Divulgación de información	Robo, pérdida o adulteración de información.	4	5	20	A
		[A.11] Acceso no autorizado	Perdida de Información	5	4	20	A
	Inadecuada ubicación del archivo físico	[I.7] Condiciones inadecuadas de temperatura o humedad	Deterioro de los archivos	5	5	25	MA

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[SERV_ADQUISI] Administración de materiales de formación.	Mala ubicación donde se guardan los materiales de formación.	[A.11] Acceso no autorizado	Robo de materiales de formación	4	4	16	A
	Falta de mecanismos de control durante la asignación al instructor.	[A.28] Indisponibilidad del personal	Algunos programas no reciben la totalidad de materiales de formación	2	4	8	B
[SERV_INFOR] Atención a usuarios internos o externos y respuesta PQRS.	No sé suministre la información apropiada y de manera pertinente	[E.26] Indisponibilidad del personal	Pérdida de confianza y acceso a la información	2	5	10	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[SERV_INFOR] Atención a usuarios internos o externos y respuesta PQRS.	Perdida de radicados.	[E.26] Indisponibilidad del personal	Falta de eficiencia para generar las respuestas	4	5	20	A
	Inadecuada ubicación del funcionario	[I.7] Condiciones inadecuadas de temperatura o humedad	Inadecuada prestación del servicio	3	4	12	M
[POR_WEB] Plataforma Web para la gestión de la formación.	Ataques de inyección de SQL	[E.4] Errores de configuración	Caída del sistema	3	5	15	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[POR_WEB] Plataforma Web para la gestión de la formación.	Denegación al acceso	[I.5] Avería de origen físico o lógico	Falta de acceso al aplicativo	3	4	12	M
	Ataques de denegación de servicios	[I.8] Fallo de servicios de comunicaciones	Inadecuada prestación del servicio	3	4	12	M
		[A.24] Denegación de servicio	Indisponibilidad de servicio.	3	4	12	M
		[E.21] Errores de mantenimiento / actualización de programas (software)		3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[SO] Sistema operativo que administra los PC.	Falta de mantenimiento preventivo a los recursos	[E.24] Caída del sistema por agotamiento de recursos	Indisponibilidad para usar el PC	3	5	15	M
	Falta de instalación de parches de seguridad.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, pérdida o adulteración de información.	2	5	10	M
	Acceso no autorizado por la inadecuada administración de los puertos						
	Acceso no autorizado	[E.8] Difusión de software dañino		3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[SO] Sistema operativo que administra los PC.	Habilitación de brechas de seguridad	[E.4] Errores de configuración	Inadecuada utilización de las opciones del sistema o herramientas de software	4	4	16	A
	Mal funcionamiento del sistema	[E.1] Errores de los usuarios		3	4	12	M
[ANT_VIR] Software Antivirus	Inoperancia del programa dejando expuesto el PC.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, perdida o adulteración de información o del sistema	3	4	12	M
	Acceso no autorizado	[E.20] Vulnerabilidades de los programas (software)		3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[ANT_VIR] Software Antivirus	Deshabilitar el escaneo a páginas de internet	[E.4] Errores de configuración	Robo, perdida o adulteración de información o del sistema	2	4	8	M
	Equipo expuesto a la difusión de software malicioso y acceso no autorizados	[E.1] Errores de los usuarios		3	4	12	M
[PC] Equipo de Computo	No contar con politicas de respaldo de la información	[N.3] Desastres naturales	Robo, perdida o adulteración de información	1	5	5	B
	Intermitencia en el desarrollo de las actividades a cargo.	[I.5] Avería de origen físico o lógico	Indisponibilidad en el uso del equipo	3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[PC] Equipo de Computo	Fallos en la operatividad del equipo	[I.7] Condiciones inadecuadas de temperatura o humedad	Indisponibilidad en el uso del equipo	4	4	16	A
	Falta de politicas de control de acceso	[A.15] Modificación de información	Robo, perdida o adulteración de información	3	4	12	M
		[A.17] Corrupción de la información		3	5	15	M
		[A.19] Divulgación de información		2	5	10	M
	Instalación o habilitación de software malicioso	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuado funcionamiento del Equipo de computo	3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[PC] Equipo de Computo	Habilitación de brechas de seguridad (puertos)	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuado funcionamiento del Equipo de computo	3	4	12	M
	Inoperancia del equipo de cómputo y acceso a información.	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Deficiencia en la prestación de un servicio por el no uso del PC	4	4	16	A
	Daño parcial o permanente en el equipo de cómputo.	[I.6] Corte del suministro eléctrico	Daño en componentes físicos o corrupción de archivos	2	5	10	M
	Acceso no autorizado	[E.8] Difusión de software dañino	Afectación en la integridad de los archivos	3	4	12	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
Impresora de Red	Se represan los documentos impresos en la bandeja de salida	[E.14] Fugas de información	Robo o Pérdida de Información.	3	4	12	M
	Cuando se imprime por USB puede llegarse a infectar con virus	[E.8] Difusión de software dañino	Propagación de códigos maliciosos a los equipos de cómputo, ocasionando pérdida o alteración en la información	4	5	20	A
	Indisponibilidad en el funcionamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	Afectación en el uso del servicio	3	5	15	M
	Interrupción en el Servicio	[I.6] Corte del suministro eléctrico		2	5	10	M

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
Impresora de Red	Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico	Afectación en el uso del servicio	2	3	6	B
	Vulnerabilidad de tipo OpenSSL	[A.11] Acceso no autorizado		3	3	9	B
[ADSL] Internet	Lentitud en el servicio de comunicación.	[I.8] Fallo de servicios de comunicaciones	Afectación en la calidad y pertinencia del servicio y/o la información.	3	3	9	B
	Intermitencia en el servicio.						
	Caída en parcial o total en el servicio.						
[CAB_RED] Tendido del cable de Red.	El tendido de cable no cumple con lo emanado en la normatividad vigente.	[I.8] Fallo de servicios de comunicaciones	Afectación en el tránsito de la información y acceso a internet	2	3	6	B

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[CAB_RED] Tendido del cable de Red.	Deterioro en los cables de Red	[I.7] Condiciones inadecuadas de temperatura o humedad	Afectación en el tránsito de la información y acceso a internet	4	2	8	B
[GABI] IDF centro de cableado	Caída total o parcial del servicio de internet	[I.6] Corte del suministro eléctrico	Afectación en la prestación del servicio que depende de internet.	2	4	8	B
	Deterioro en la vida útil de los componentes físicos	[I.7] Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran	4	5	20	A
	Caída total o parcial del servicio de internet	[N.3] Desastres naturales	Afectación en la prestación del servicio que depende de internet.	1	5	5	B

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[GABI] IDF centro de cableado	Deficiencia en el acceso a las plataformas web.	[E.4] Errores de configuración	Acceso limitado a la información y deterioro en la prestación del servicio	1	5	5	B
[ESP_ADM_IV] Funcionarios	Uso inadecuado de los permisos otorgados y de los recursos disponible	[A.7] Uso no previsto	Ineficiencia en el uso de los recursos	2	4	8	B
	Acceder sin contar con los privilegios a equipos de cómputo o información física	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	2	4	8	B
	Instalación y uso de programas no autorizados que pueden habilitar el ingreso de archivos maliciosos o acceso no autorizados	[A.22] Manipulación de programas		3	3	9	B

Tabla 14. (Continuación)

				Valoración del Riesgo			
Activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[ESP_ADM_IV] Funcionarios	No asumir su Rol frente a la protección de la información.	[A.28] Indisponibilidad del personal	Afectación en la prestación del servicio, manipulación de información.	3	3	9	B
	Acceso de Información confidencial por parte de terceros no autorizados	[A.30] Ingeniería social (picaresca)	Robo, perdida o adulteración de información	3	2	6	B

Fuente: Elaboración Propia

7.4.5 Análisis de resultados de la matriz de riesgos. A continuación, se presenta el análisis realizado con respecto a aquellos riesgos de tipo crítico, importante y medio.

Riesgos de nivel crítico

Se identifica que es importante para el archivo central de la dependencia formación profesional integral del Sena Regional Guainía. Implementar controles que basados en la norma ISO 27002:3013 permitan mitigar los riesgos de acceso no autorizados y condiciones de humedad que se presentan. Lo anterior con la premisa de proteger los archivos allí almacenados y permitiendo así que estos puedan volver a ser consultados según la necesidad de acceso a la información por parte de los funcionarios de la dependencia o en su defecto cuando son requeridos para dar respuesta a PQRS que se radican.

Riesgos de nivel importante

Se identifica que se presentan riesgos significativos sobre muchos de los activos de información de la dependencia. Iniciando por la falta de control al momento de acceder al archivo central. Ya que no se cuenta con medidas tendientes a evitar que se sustraigan archivos sin previa autorización lo que ocasiona perdida de archivos y que algunos funcionarios de la dependencia accedan a información que por el principio de confidencialidad no deberían conocer.

Se evidencia que se debe capacitar al personal sobre buenas prácticas de uso de los recursos informáticos de la oficina, ya que se identifica que algunos funcionarios instalan software sin la debida autorización, lo que puede generar brechas de seguridad. Por otra parte, la falta de actualización del sistema operativo y del antivirus representa una práctica cotidiana que genera indisponibilidad en el personal por la lentitud en algunos PC y por la propagación de virus entre la impresora y los PC por uso de la memoria USB al imprimir con ella y no ser vacunada al insertarse en los equipos. Lo que evidencia una clara falta de políticas de seguridad y capacitación al personal sobre aspectos de seguridad informática.

Los equipos de cómputo presentan años de uso y no cuentan con una hoja de vida. Con relación a los mantenimientos y actualizaciones al hardware de los efectuados, lo que también genera indisponibilidad de algunos funcionarios ya que sus equipos no funcionan a la velocidad que les permitan realizar las acciones asignadas de manera eficiente. De allí que se debe generar un plan de

actualización y mantenimiento por el personal de soporte en sitio y poder subsanar las deficiencias que se han presentado.

Por otra parte, se evidencia en algunos momentos indisponibilidad de algunos funcionarios para realizar las acciones asignadas en ciertas ocasiones, aduciendo condiciones de temperatura inadecuadas que afectan su concentración y que han generado enfermedades gripales. Es de allí que se debe regular la temperatura a través de un consenso que permita que todos estén cómodos y puedan desarrollar sus actividades bajo protocolos de seguridad de la información conforme lo exige la normatividad.

Riesgos de nivel medio

Se evidencia situaciones que poden en riesgo a los activos de información que hace parte de la dependencia de formación, como es las condiciones inadecuadas de temperatura, lo que afecta al personal, el hardware y el archivo central de la oficina. Igualmente se identifica la falta de preparación de los funcionarios con relación al manejo de software ya que muchos de ellos no saben cómo actualizar el antivirus, otros instalan programas ajenos a sus funciones. Lo que representa una brecha de seguridad que de ser aprovechada por personal mal intencionado podría afectar la integridad de la información.

No se cuanta son sistema regulado o UPS que permita un suministro ininterrumpido al momento que falla el fluido eléctrico. Lo que se convierte en un riesgo para los equipos de cómputo y pérdida de información cuando se está trabajando y se suspende la energía de manera abrupta.

Luego de realizar de análisis de riesgo se logró evidenciar que de las amenazas asociadas a los activos de información de la dependencia de formación. 25 de ellos que equivale a un 50 % de los riesgos están en nivel a **Apreciable**. Sobre activos como: los equipos de cómputo, tendido de cable y el IDF, 15 que equivale al 30% están en nivel **Bajo.** Sobre los activos relación al recurso humano y a los servicios web, 9 que corresponde al 18% se encuentran en nivel **Importante.** Sobre activos de tipo aplicación y 1 que equivale al 2% se encuentra en un nivel **Crítico.** Sobre el activo del archivo central de la dependencia. Lo anterior permita establecer estrategias tendientes a la protección de los activos de información y la infraestructura tecnológica que soporta el funcionamiento de la dependencia. Enfocadas a eliminar o en su defecto minimizar las amenazas o vulnerabilidades a la que pueden estar expuesto de ataque de actores internos o externos que busquen afectar la integridad, confidencialidad y disponibilidad de la información.

7.5 FASE 3

Diseño de un plan de tratamiento de riesgos y vulnerabilidades detectados a los activos de información.

7.5.1 Plan tratamiento de riesgo. Ya previa identificación de las amenazas a los que están expuestos los activos de información y la infraestructura tecnológica de la dependencia de Formación Profesional Integral del Sena Regional Guainía. A través de la gestión del riesgo realizada, se procede a realizar el plan de tratamiento de riesgo donde se asigna una salvaguarda sobre cada activo de información.

Tabla 15. Plan de tratamiento de riesgo

						Valoración del Riesgo				**Plan de Tratamiento de Riesgo**		
Tipo	**Activo**	**Descripción**	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**	**Tratamiento**	**Control ISO 27002:2013**	**Salvaguarda Propuesta**
DATOS / INFORMACION	[BD_TRADOC] Archivo Central	Archivo físico donde se guarda información producida por la dependencia.	Falta de mecanismos control de acceso	[A.19] Divulgación de información	Robo, pérdida o adulteración de información.	4	5	20	A	Mitigar el Riesgo	9.1.1 Política de control de accesos.	Definir política de control acceso al archivo central de la dependen

				[A.11] Acceso no autorizado	Perdida de Información	5	4	20	A			cia a través de mecanismos eficientes que permita el ingreso solo a personal autorizado. Según su cargo
			Inadecuada ubicación del archivo físico	[I.7] Condiciones inadecuadas de temperatura o humedad	Deterioro de los archivos	5	5	25	MA	Mitigar el Riesgo	11.1.4 Protección contra amenazas externas y del ambiente	Controlar el exceso de temperatura producto de la humedad. Reubicar el archivo central en otro sitio

SERVICIOS	[SERV_ADQUISI] Administración de materiales de formación.	Distribución de materiales de formación a los instructores de cada programa en ejecución.	Mala ubicación donde se guardan los materiales de formación.	[A.11] Acceso no autorizado	Robo de materiales de formación	4	4	16	A		11.1.2 Controles físicos de entrada	Establecer medidas de control para el acceso al sitio donde se guarda los materiales
			Falta de mecanismos de control durante la asignación al instructor.	[A.28] Indisponibilidad del personal	Algunos programas no reciben la totalidad de materiales de formación	2	4	8	B	Mitigar el Riesgo	12.1.1 Documentación de procedimientos operacionales	Establecer plan de asignación y/o distribución de los materiales de formación.
	[SERV_INFOR] Atención a usuarios internos	Atención a clientes internos y externos sobre PQRS y solicitudes	No se suministre la información apropiada y	[E.26] Indisponibilidad del personal	Pérdida de confianza y acceso a la inform	2	5	10	M		7.2.2 Concienciа, educación y entrenamient	Definir un plan de capacitación al personal sobre seguridad

	o externos y respuesta PQRS.	de formación.	de manera pertinente		ación						o de seguridad de la información	de la información y continuidad del negocio.
			Perdida de radicados.		Falta de eficiencia para general las respuesta	4	5	20	A	Mitigar el Riesgo	16.1.3 Reporte de debilidades de seguridad de la información	Definir protocolos de atención al cliente y custodia de los documentos
			Inadecuada ubicación del funcionario	[I.7] Condiciones inadecuadas de temperatura o humedad	Inadecuada prestación del servicio	3	4	12	M		11.1.4 Protección contra amenazas externas y del ambiente	Establecer plan de control con relación al aire acondicionado y al exceso de luz natural

APLICACIONES	[POR_WEB] Plataforma Web para la gestión de la formación.	Se cuenta con un aplicativo llamado Sofia Plus www.senasofiaplus.edu.co	Ataques de inyección de SQL	[E.4] Errores de configuración	Caída del sistema	3	5	15	M	Mitigar el Riesgo	12.3.1 Respaldo de información	Definir plan de respaldo de la información e incorporación de un WAF
			Denegación al acceso	[I.5] Avería de origen físico o lógico	Falta de acceso al aplicativo	3	4	12	M		11.2.4 Mantenimiento de equipos	Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro.
			Ataques de denegación de servicios	[I.8] Fallo de servicios de comunicaciones	Inadecuada prestación del servicio	3	4	12	M	Mitigar el Riesgo	14.1.2 Aseguramiento o de servicios de aplicación en redes públicas	Instalar IPS Instalar y configurar adecuado firewall y Router.

				[A.24] Denegación de servicio	Indisponibilidad de servicio.	3	4	12	M		13.1.1 Controles de redes	
				[E.21] Errores de mantenimiento / actualización de programas (software)		3	4	12	M	Mitigar el Riesgo	11.2.4 Mantenimiento de equipos	Establecer plan de mantenimiento y actualización de software
	[SO] Sistema operativo que administra los PC.	Sistema operativo Windows 10 Pro con los que cuentas los PC.	Falta de mantenimiento preventivo a los recursos	[E.24] Caída del sistema por agotamiento de recursos	Indisponibilidad para usar el PC	3	5	15	M			Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro

			Falta de instalación de parches de seguridad.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, pérdida o adulteración de información.	2	5	10	M	Mitigar el Riesgo		Definir plan de mantenimiento y actualización del sistema operativo
			Acceso no autorizado por la inadecuada administración de los puertos								9.1.1 Política de control de accesos.	Implementar politicas de control de acceso y configuración del firewall
			Acceso no autorizado	[E.8] Difusión de software dañino		3	4	12	M	Mitigar el Riesgo	12.2.1 Controles contra software malicioso	Instalar software antivirus, Antispyware y mantener actualizada la base de datos.

			Habilitación de brechas de seguridad	[E.4] Errores de configuración	Inadecuada utilización de las opciones del sistema o herramientas de software	4	4	16	A		7.2.2 Concienciа, educación y entrenamiento de seguridad de la información	Plan de capacitación sobre el uso adecuado de los recursos informáticos y aplicación de politicas de seguridad
			Mal funcionamiento del sistema	[E.1] Errores de los usuarios		3	4	12	M	Mitigar el Riesgo		
	[ANT_VIR] Software Antivirus	Programa para la detección de archivos maliciosos	Inoperancia del programa dejando expuesto el PC.	[E.21] Errores de mantenimiento / actualización de programas (software)	Robo, perdida o adulteración de información o del sistema	3	4	12	M		11.2.4 Mantenimiento de equipos	Definir plan de mantenimiento, actualización del sistema operativo y programas asociados

			Acceso no autorizado	[E.20] Vulnerabilidades de los programas (software)		3	4	12	M	Mitigar el Riesgo	11.2.4 Mantenimiento de equipos	Definir plan de actualización y verificación de su correcto funcionamiento
			Deshabilitar el escaneo a páginas de internet	[E.4] Errores de configuración		2	4	8	M		7.2.2 Concientia, educación y entrenamiento de seguridad de la información	Definir plan de capacitación sobre la adopción de politicas de seguridad para proteger la información y los equipos.
			Equipo expuesto a la difusión de softwa	[E.1] Errores de los usuarios		3	4	12	M	Mitigar el Riesgo		

			re malicioso y acceso no autorizados									
EQUIPAMIENTO INFORMATICO	[PC] Equipo de Computo	Equipo de cómputo de cada funcionario de la dependencia de formación.	No contar con politicas de respaldo de la información	[N.3] Desastres naturales	Robo, perdida o adulteración de información	1	5	5	B	Mitigar el Riesgo	12.3.1 Respaldo de información	Realizar plan de respaldo de la información producida en la dependencia de formación.
			Intermitencia en el desarrollo de las actividades a cargo.	[I.5] Avería de origen físico o lógico	Indisponibilidad en el uso del equipo	3	4	12	M		11.2.4 Mantenimiento de equipos	Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro

			Fallos en la operatividad del equipo	[I.7] Condiciones inadecuadas de temperatura o humedad		4	4	16	A	Mitigar el Riesgo	11.1.4 Protección contra amenazas externas y del ambiente	Plan de mitigación por el exceso de luz natural que afecta los equipos
			Falta de politicas de control de acceso	[A.15] Modificación de información	Robo, perdida o adulteración de información	3	4	12	M		9.2.3 Gestión de derechos de acceso privilegiados	Establecer politicas de control de acceso y privilegios. Según Rol del funcionario
				[A.17] Corrupción de la información		3	5	15	M	Mitigar el Riesgo	9.1.1 Política de control de acceso	

				[A.19] Divulgación de información		2	5	10	M			
			Instalación o habilitación de software malicioso	[E.21] Errores de mantenimiento / actualización de programas (software)	Inadecuado funcionamiento del Equipo de computo	3	4	12	M	Mitigar el Riesgo	12.2.1 Controles contra software malicioso	Contar con un plan de instalación y actualización tanto del sistema operativo como de las aplicaciones y antivirus.
			Habilitación de brechas de seguridad (puertos)								11.2.4 Mantenimiento de equipos	Configuración del Firewall. Según privilegios de acceso de los usuarios

			Inoperancia del equipo de cómputo y acceso a información.	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Deficiencia en la prestación de un servicio por el no uso del PC	4	4	16	A	Mitigar el Riesgo		Plan de mantenimiento y verificación de los dispositivos, para prevenir fallas y deterioro
			Daño parcial o permanente en el equipo de cómputo.	[I.6] Corte del suministro eléctrico	Daño en componentes físicos o corrupción de archivos	2	5	10	M		11.2.2 Servicios de suministro	Instalar UPS o sistema regulado para garantizar el fluido eléctrico y no sé presente perdida de información y afectaciones a los equipos de

												computo
			Acceso no autorizados	[E.8] Difusión de software dañino	Afectación en la integridad de los archivos	3	4	12	M	Mitigar el Riesgo	9.2.3 Gestión de derechos de acceso privilegiados	Definir politicas de privilegios para el acceso e instalación de software
	Impresora de Red	Samsung Multi Xpress M5370LX	Se represan los documentos impresos en la bandeja de salida	[E.14] Fugas de información	Robo o Pérdida de Información.	3	4	12	M		9.3.1 Uso de información secreta para la autenticación	Adoptar politicas de custodio de la información y privacidad de los documentos que se encuentren la bandeja de salida

												de la impresora
			Cuando se imprime por USB esta se contamina con virus	[E.8] Difusión de software dañino	Copiar los virus a los equipos de computo	4	5	20	A	Mitigar el Riesgo	12.2.1 Controles contra software malicioso	Eliminar el virus de la impresora y controlar el uso de memoria USB para imprimir evitando así la propagación de archivos maliciosos en los equipos.

			Indisponibilidad en el funcionamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	Afectación en el uso del servicio	3	5	15	M		11.1.4 Protección contra amenazas externas y del ambiente	Definir un plan para controlar la baja temperatura producido humedad
			Interrupción en el Servicio	[I.6] Corte del suministro eléctrico		2	5	10	M	Mitigar el Riesgo	11.2.2 Servicios de suministro	Conectar a una UPS o al sistema regulado para evitar afectación por fallas en el fluido eléctrico
			Falta de mantenimiento preventivo	[I.5] Avería de origen físico o lógico		2	3	6	B		11.2.4 Mantenimiento de equipos	Definir plan de mantenimiento y verificaciones del hardware para

												supervisar su buen fruncimiento y controlar averías de presentarse
			Vulnerabilidad de tipo OpenSSL	[A.11] Acceso no autorizado		3	3	9	B	Mitigar el Riesgo		Definir politicas de actualización del software y controles de seguridad para evitar este tipo vulnerabilidad
REDES DE COMUNICACIONES	[ADSL] Internet	La dependencia cuenta con una conexión a internet.	Lentitud en el servicio de comunicación.	[I.8] Fallo de servicios de comunicacione	Afectación en la calidad y pertinencia	3	3	9	B		15.1.1 Política de seguridad de la inform	Negociar con el proveedor una ampliación en el ancho de

			Intermitencia en el servicio. Caída en parcial o total en el servicio.	s	del servicio y/o la información.					Mitigar el Riesgo	ación en las relaciones con el proveedor	banda, el cual permita mejorar el tiempo de cargue de las aplicaciones web y dar respuesta eficiente a las tarea asignadas que dependen de este servicio
EQUIPAMIENTO AUXILIAR	[CAB_RED] Tendido del cable de Red.	Tendido de cable de Red, para la conexión a internet de los PC.	El tendido de cable no cumple con lo emanado en la normatividad	[I.8] Fallo de servicios de comunicaciones	Afectación en el tránsito de la información y acceso a internet	2	3	6	B	Mitigar el Riesgo	11.2.3 Seguridad del cableado	Garantizar una distribución del tendido de cable conforme lo exige la norma. Para garantizar un servicio

			vigente.									adecuado.
			Deterioro en los cables de Red	[I.7] Condiciones inadecuadas de temperatura o humedad		4	2	8	B			Proporcionar a través de canaletas la seguridad requerida para los cables de red y no se afecten por la humedad.
INSTALACIONES	[GABI] IDF centro de cableado	Gabinete para recepcionar y distribuir el cableado de red a cada equipo.	Caída total o parcial del servicio de internet	[I.6] Corte del suministro eléctrico	Afectación en la prestación del servicio que depende de de internet.	2	4	8	B	Mitigar el Riesgo	11.2.2 Servicios de suministro	Instalar banco de UPS para garantizar el fluido eléctrico y protección del hardware

			Deterioro en la vida útil de los componentes físicos	[I.7] Condiciones inadecuadas de temperatura o humedad	Funcionamiento inadecuado de los componentes que lo integran	4	5	20	A		11.1.4 Protección contra amenazas externas y del ambiente	Definir un plan que determine las condiciones de seguridad para que no sé afecte el gabinete por la humedad
			Caída total o parcial del servicio de internet	[N.3] Desastres naturales	Afectación en la prestación del servicio que depende de de internet.	1	5	5	B	Mitigar el Riesgo	17.1.1 Planificación de la continuidad de la seguridad de la información	Definir un plan de contingencia para el acceso a la información y continuidad del negocio

			Deficiencia en el acceso a las plataformas web.	[E.4] Errores de configuración	Acceso limitado a la información y deterioro en la prestación del servicio	1	5	5	B		7.2.2 Concienciа, educación y entrenamiento de seguridad de la información	Establecer un plan de configuración, actualización y verificación de buenas prácticas para el acceso a la información a través de politicas de seguridad y acceso a la información.
PERSONAL	[ESP_ADM_IV] Funcionarios	Personal administrativo que labora en la dependencia.	Uso inadecuado de los permisos otorga	[A.7] Uso no previsto	Ineficiencia en el uso de los recursos	2	4	8	B	Mitigar el Riesgo	9.2.3 Gestión de derechos de acceso	Establecer plan de capacitación al personal de la dependen

			dos y de los recursos disponible								privilegiados	cia sobre politicas de seguridad y uso adecuado de los recursos TIC
			Acceder sin contar con los privilegios a equipos de cómputo o información física	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	2	4	8	B		9.1.1 Política de control de acceso	Definir politicas de control de acceso y otorgamiento de privilegios en función al Rol.
			Instalación y uso de programas no autorizados que	[A.22] Manipulación de programas		3	3	9	B	Mitigar el Riesgo	7.2.2 Concienciа, educación y entrenamiento de seguri	Establecer plan de capacitación al personal de la dependencia sobre politicas

			pueden habilitar el ingreso de archivos maliciosos o acceso no autorizados								dad de la información	de seguridad y uso adecuado de los recursos TIC
			No asumir su Rol frente a la protección de la información.	[A.28] Indisponibilidad del personal	Afectación en la prestación del servicio, manipulación de información.	3	3	9	B			Establecer plan de capacitación al personal de la dependencia sobre politicas de seguridad de la

			Acceso de Información confidencial por parte de terceros no autorizados	[A.30] Ingeniería social (picaresca)	Robo, perdida o adulteración de información	3	2	6	B	Mitigar el Riesgo		información y uso adecuado de los recursos TIC. Igualmente la normatividad sobre la protección de los datos personales

Fuente: Elaboración Propia

7.5.2 Declaración de aplicabilidad. A continuación, se relacionan los controles que teniendo en cuanta la norma ISO 27001:2013 son necesarios a aplicarse dentro de la dependencia de formación, con el objetivo de mitigar todos y cada uno de las brechas de seguridad detectados a través de la tabla 14 matriz de riesgo.

Tabla 16. Documento de aplicabilidad

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X		Definir a través de la estructuración de un documento. Políticas de seguridad con buenas prácticas para la protección de los activos de información y la infraestructura tecnología de la dependencia de formación.
Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	X		Establecer a partir del modelo PHVA auditoria a las políticas de seguridad implantadas, para medir su efectividad y tomar acciones de mejora a que haya lugar.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	X		De acuerdo al manual de funciones se debe asumir un grado de responsabilidad con relación al tratamiento y activos de información. Por parte del personal.
Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	X		Definir con relación a las responsabilidades de cada funcionario su rol frente a la adopción de políticas para proteger la información.
Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	X		Definir los canales de comunicación para el reporte de incidentes de seguridad detectados al personal de soporte de soporte técnico.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	X		No se evidencia grupos de interés, no se registra notificaciones de seguridad, vulnerabilidades y parches
Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	X		Implementar un formato con cláusulas y/o acuerdos de confidencialidad y actas de entrega de cargos que registren la entrega de credenciales y demás.
Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	X		Aunque se envían correos con recomendaciones de seguridad. No sé evidencia un compromiso por parte de la directiva del centro destinados politicas de seguridad para proteger los activos de información.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	X		Definir un plan de capacitación al personal de la dependencia de formación. Sobre politicas de seguridad informática y su importancia dentro de una empresa.
Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X		Firmar acuerdos de confidencialidad por parte del talento humano cuando ingresa a la dependencia, y realizar las acciones a que haya lugar por la violación de las políticas de seguridad implantados.
Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X		Definir clausulas en los contratos, relacionados a la seguridad informática. Evitando la divulgación de información confidencial.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X		Establecer un documento que permita mantener actualizado los activos de la dependencia de formación.
Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	X		Asignación con base al rol de cada funcionario los activos de información necesarios para el desarrollo de sus actividades.
Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X		Se debe implementar un plan de sensibilización sobre el uso adecuado de los activos de la dependencia.
Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X		Definir politicas claras sobre el tratamiento y custodia de la información almacenada en archivo central y equipos de la dependencia de formación.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		Definir protocolos de identificación de la información. Según políticas de seguridad y manejo de la información.
Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		Definir políticas de seguridad informática para definir el procedimiento y buenas prácticas para el manejo adecuado de los activos de información.
Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	X		Definir buenas prácticas para el uso adecuado de memorias USB y dispositivos móviles.
Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	X		Definir a través de protocolos filtros evitando accesos no autorizados.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X		Implementar políticas de control de acceso a los activos de información existentes en la dependencia de formación.
Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	X		Definir políticas de control de acceso y asignación de privilegios según funciones asignadas al personal.
Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X		Asignar credenciales cumpliendo una serie de características específicas.
Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X		Definir un plan de tratamiento adecuado de la información. Según normatividad legal vigente.
Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X		Establecer privilegios a los funcionarios de acuerdo a las políticas de control de acceso a definir.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X		Definir durante el acceso a la información preguntas de seguridad como filtros, para que solo el usuario tenga acceso a la información, buscando el ingreso seguro.
Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X		Establecimiento de claves seguras. Que incluyan grado de complejidad.
Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X		Ingreso a funcionarios autorizados al archivo central y a equipos de cómputo de la dependencia de formación.
Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	X		Implementar sistemas de seguridad dentro del perímetro como: cámaras de seguridad dentro del archivo central.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X		Implementar sistemas de seguridad dentro del perímetro como: cámaras de seguridad dentro del archivo central.
Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.			
Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X		Definir protocolo para la instalación de sistemas de ventilación, detectores de humo, extintores y así mitigar la afectación de los activos de información de presentarse dicho fenómeno.
Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X		Construcción de un plan de trabajo seguro en tú puesto de trabajo, eliminado factores externos que pueden afectar a los funcionarios.
Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	X		Ubicar los equipos de cómputo e impresora en un espacio adecuado, para que no los afecte la humedad y el exceso de luz natural.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X		Instalar UPS y sistemas regulados para todos los equipos de cómputo, impresora y el IDF. Lo anterior para proteger los equipos contra fallas producidos por fluido eléctrico.
Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X		Organizar el cableado en canaletas para protegerlo contra deterioro y condiciones inadecuadas de temperatura producido por la humedad.
Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X		Definir por parte soporte técnico un plan de mantenimiento preventivos y correctivos periódicos para prolongar el buen funcionamiento de los quipos y evitar mal funcionamiento
Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	X		Establecer un mecanismo de control para el retiro de activos pertenecientes a la dependencia de formación.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X		Según las políticas del Sistema de Gestión de Seguridad Ocupacional, se opta por tener los puestos de trabajo, limpio.
Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X		Definir un plan de actualización del antivirus y el sistema operativo para prevenir los archivos maliciosos en equipos de cómputo e impresora.
Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X		Definir dentro de las políticas un mecanismo para efectuar copias de respaldo de la información física y digital.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X		Establecer por parte del responsable de soporte técnico la revisión de los logs de: equipos, antivirus y registros de actividades por usuario.
Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X		Definir restricciones sobre la instalación de software de terceros, configurar privilegios y capacitar al personal sobre políticas de seguridad.
Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X		Implementar procedimiento de reporte de incidentes. Igualmente definir un plan de contingencia diseñado de acuerdo a las condiciones del centro y la dependencia de formación.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X		Definir restricciones sobre la instalación de software de terceros de acuerdo a configurar permisos de usuarios y roles.
Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		Contar con un plan de auditoria para evaluar el funcionamiento de la red de datos, velando por condiciones óptimos de ubicación, ambientales y de suministro de fluido eléctrico regulado.
Acuerdos de confidencialidad o de no divulgación.	Control: Se deben identificar revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X		Implementación de protocolo de confidencialidad para el manejo de información.
Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X		Definir dentro de las políticas de seguridad de información los roles y responsabilidades asignados a cada funcionario de la dependencia de formación.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X		Reportar incidentes de seguridad detectadas por los funcionarios por los canales definidos para tal acción al responsable de soporte técnico.
Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X		
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	X		Plan de auditoria para evaluar la efectividad de los controles implementados.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X		Definición de políticas claras, buscando así los registros de protección de extravío, destrucción, falsificación y/o liberación no autorizada. De acuerdo con los requisitos legislativos
Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	X		Implementar políticas seguridad para asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación.
Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	X		Definir un plan de auditoria fundamentado en el modelo PHVA y tomar acciones de mejora de ser necesario.

Tabla 16. (Continuación)

		Control Seleccionado		
Objetivo del Control	**Descripción del Control**	**si**	**no**	**Justificación**
Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X		Alinear todas las acciones al cumplimiento de la normatividad para la protección de la información, tratamiento de datos personales y activos de información.
Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X		Definir un plan de revisión u auditoria y velar por el cumplimiento de las políticas de seguridad de la información.

Fuente: Materia Riesgo y Controles Informáticos. Especialización en seguridad informática. UNAD. Año 2019

Cabe anotar que hubo controles que por la dinámica de las actividades que se realizan dentro de la dependencia de formación y su tamaño no están relacionados dentro del documentos de aplicabilidad como son: controles criptográficos y controles relacionados a desarrollo de software.

8. CONCLUSIÓN

Una vez desarrollado el proyecto aplicado. “Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del Sena regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT”. Se puede concluir la necesidad de establecer las condiciones de seguridad necesarias para proteger los activos de información con los que la dependencia de Formación Profesional Integral del SENA Regional Guainía. Utiliza diariamente para el cumplimiento de la meta institucional asignada por Dirección General. Lo anterior identificando las vulnerabilidades, amenazas y riesgos asociados a cada activo y de allí definir las salvaguardas y controles pertinentes para realizar un tratamiento adecuado a dicho riesgo.

Las medidas de seguridad adoptadas se recomiendan en el entendido de garantizar la continuidad del negocio, a partir de velar porque no sé afecte la integridad, confidencialidad y disponibilidad de los activos de información asociados a la dependencia de formación.

Una apropiada y eficiente aplicación de la gestión del riesgo provee los insumos necesarios para minimizar o en su defecto eliminar los peligros que rodean no solo la información, sino también demás activos hardware y software con los que cuenta la dependencia de formación.

Definir un plan de auditoria que basada en el modelo PHVA permita evaluar la eficiencia de los controles y salvaguardas adoptados, para mitigar el riesgo sobre cada activo de información. Determinar si el control adoptado fue o no el apropiada, permitirá de manera temprana realizar las acciones de mejora a que haya lugar.

Establecer un plan de capacitación a los funcionarios de la dependencia de formación sobre los protocolos de seguridad de la información y su importancia. Los cuales fueron definidos en las políticas de seguridad de la información, con el ánimo que estos sean aplicados, contribuyendo al tratamiento adecuado de los datos personales de los aprendices, instructores y funcionarios, basados en la normatividad legal vigente.

Siendo la información un activo valioso para la dependencia de formación. Debe en la medida de lo posible adoptar todos y cada una de las recomendaciones planteadas con el desarrollo de este proyecto. Ya que van orientadas a garantizar la confiabilidad e integridad de la información producida allí bajo estándares de seguridad internacional a través de los controles definidos en la ISO 27001:2013.

9. RECOMENDACIONES

Adoptar los controles y medidas de seguridad que permita apegados en la normatividad legal vigente. La protección de los activos de información y la infraestructura tecnológica con los que cuenta la dependencia de formación. Estableciendo mecanismos de autenticación para el acceso solo de personal autorizado.

Definir acciones tendientes a garantizar la continuidad del negocio. A través de procedimientos para la generación de copias de seguridad de la información como mecanismo para salvaguardar los datos digitales o físicos, en caso de afectaciones a la infraestructura tecnológica de la organización. Ya sea de origen natural o intencionada y puede luego ser consultada y restablecido el servicio.

Velar por la implementación de políticas de seguridad de la información, el cual contenga buenas prácticas y acciones precisas tendientes a proteger la integridad, confidencialidad y disponibilidad de la información de la empresa.

Establecer lineamientos para la protección de los datos y los equipos de escritorio, a través de la prohibición de la instalación de software no autorizado, los cuales sirvan de puente para abrir puertos para ingresar a los equipos o a la red de la empresa. Igualmente, para evitar que se sustraiga información y/o impidiendo el alojamiento de archivos maliciosos que traen mucho de estos programas que afectan el buen funcionamiento de las máquinas.

Mantener plan de capacitación a los funcionarios para que apliquen y conozcan los procedimientos seguros a tener en cuenta durante el desarrollo de las actividades cotidianas enfocados a la protección de la información.

10. BIBLIOGRAFÍA

ALVAREZ SOSA, Yenny Maribel. Diseño De Una Metodología Para El Análisis De Riesgo En Los Sistemas De Gestión De Seguridad De Información (Marisgsi) En Las Universidades De Barquisimeto Estado Lara. Trabajo De Grado Magister Scientiarum En Ciencias De La Computación. Barquisimeto: Universidad Centroccidental “Lisandro Alvarado”. 2013. 2-34p

LOPEZ, Jhon Alexander y ZULUAGA TAMAYO, Andrés Fabián. Desarrollo De Una Metodología Para El Control De Riesgos Para Auditoria De Base De Datos. Tesis De Grado Ingeniería De Sistemas Y Computación. Pereira: Universidad Tecnológica De Pereira. 2013. 5-51p.

MATALOBOS VEIGA, Juan Manuel. Análisis de Riesgo de Seguridad Informática. Trabajo de Grado analista de sistemas de información. Madrid. Universidad Politécnica de Madrid. 2009. 46-55p.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (23, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá D.C. El Ministerio, 2013. 11 p.

VÁSQUEZ GAONA, karina del Rocio. APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANALISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A EN LA CIUDAD DE MACHALA. Tesis de grado para la obtención del título Ingeniera de sistemas. Cuenca: Universidad Politécnica Salesina. Sede cuenca. Facultad de Ingeniería. 2013. 53-79p.

DUARTE MARTINEZ, Maria Carolina. DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA. Trabajo de grado presentado como requisito para optar al título de: Especialista en Seguridad Informática. Cúcuta: Universidad Nacional

Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2019. 29-56p.

NECTEC. ¿Qué es seguridad informática?; Bogotá: NECTEC. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: https://www.netec.com/que-es-seguridad-informatica

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. Suiza: ISO. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN; Suiza: ISO. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/iso-27001/

UNIVERSIDAD PILOTO DE COLOMBIA. La Importancia de Realizar un Análisis de Riesgo en las empresas; Bogotá: UPC. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: http://polux.unipiloto.edu.co:8080/00003266.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Revista Especializada en Ingeniería**.** Metodologías Para el Análisis de Riesgos en los SGSI; Bogotá: UNAD. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ESCUELA EUROPEA DE EXCELENCIA. Gestión de Riesgos: Identificación y Análisis de Riesgos; Madrid. [Sitio Web]; [Consultado el 15 de abril de 2020]; Disponible en: https://www.escuelaeuropeaexcelencia.com/2016/07/gestion-de-riesgos-identificacion-analisis/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Guía de Gestión de Riesgos. Gestión y Privacidad de la Información; Bogotá: MINTIC. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Revista Especializada en Ingeniería**.** Metodologías Para el Análisis de Riesgos en los SGSI; Bogotá: UNAD. [Sitio Web]. [Consultado el 15 de abril de 2020]. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

REAL ACADEMIA DE LA LENGUA. Diccionario de la lengua española; España: RAE. [Sitio Web]; [Consultado el 15 de abril de 2020]; Disponible en: https://dle.rae.es/seguridad?m=form

UNIVERSIDAD NACIONAL DE LUJÁN. Departamento de seguridad Informática. Amenazas a la seguridad de la Información; Argentina. [Sitio Web]; [Consultado el 15 de abril de 2020]; Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

UNIVERSIDAD NACIONAL DE LUJÁN. Departamento de seguridad Informática. Amenazas a la seguridad de la Información; Argentina. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/15

ECURED. Ataque Informático; Cuba: ECURED. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

INTERNATIONAL BUSINESS MACHINES CORPORATION. Identificación y Autenticación; Nueva York: IBM. [Sitio Web]; [Consultado el 16 de abril de 2020]. Disponible en:https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm

INTERNATIONAL BUSINESS MACHINES CORPORATION. Integridad de datos. Nueva York: IBM. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009780_.htm

TECNOSEGURO. ¿Qué es un Sistema de Control de Acceso? [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en:https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

CENTRO EUROPEO DEL CONOCIMIENTO PARA LA TECNOLOGÍA DE LA INFORMACIÓN. Base de datos: España: EKCIT. [Sitio Web]; [Consultado el 15 de abril de 2020). Disponible en: https://www.ticportal.es/glosario-tic/base-datos-database

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 27001 seguridad de la información .ISO 27001 gestión de la seguridad de la información; Suiza: ISO. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: https://www.normas-iso.com/iso-27001/

INFOSEGUR. Seguridad Informática. Objetivos de la seguridad informática; Ecuador: INFOSEGUR. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: https://infosegur.wordpress.com/tag/confidencialidad/

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. Temas relacionados con los SGSI y la seguridad de la información. Suiza: ISO. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: http://www.iso27000.es/

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. Serie "27000". Requisitos de la norma ISO/IEC 27001. Suiza: ISO. [Sitio Web]; [Consultado el 15 de abril de 2020]. http://www.iso27000.es/iso27000.html

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. Serie "27000". Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. Suiza: ISO. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: http://www.iso27000.es/iso27000.html

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. Serie "27000". Guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los Sistemas de Gestión de la Seguridad de la Información. Suiza: ISO. [Sitio Web]; [Consultado el 15 de abril de 2020]. Disponible en: http://www.iso27000.es/iso27000.html

ANEXOS

Anexo A. Formato acuerdo de confidencialidad

LOGO EMPRESA V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE JEYSSER AURELIO PALACIOS PALACIOS Y EL SENA REGIONALGUAINÍA

Por la **parte reveladora**
Nombre: SENA Regional Guainía
Dirección: Trans 6ª N°29ª- 55 Vial al Coco, Inírida-Guainía
Teléfono: 3115998400
E-mail: fgonzalezt@sena.edu.co

Por la parte **receptora de la información**
Nombre: Jeysser Aurelio Palacios Palacios
Dirección: Cra 6B N°33-34 Primavera 2, Inírida-Guainía
Teléfono: 3216042960
E-mail: jeysser@misena.edu.co

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la empresa SENA Regional Guainía, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto aplicado con el título: "Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT".

2. Que la información de propiedad del SENA Regional Guainía ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación "Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Para el diseño de una propuesta de aseguramiento de la información basada en la

metodología MAGERIT", Jeysser Aurelio Palacios Palacios que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad del SENA Regional Guainía.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al SENA Regional Guainía, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadisticos y de mejoramiento del SENA Regional Guainía.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

   Modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto investigación "Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT" lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de

productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma SENA Regional Guainía, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte del SENA Regional Guainía.

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: Características de equipos de cómputo, sistema operativo, infraestructura de redes, impresora, sistema eléctrico y cargo del responsable de cada sesión.

10. La información capturada por la **parte receptora** se observará como cifras para información cualitativa, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad todo el personal del SENA Regional Guainía, no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de SENA Regional Guainía, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante Jeysser Aurelio Palacios Palacios, se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa SENA Regional Guainía para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar

específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes Jeysser Aurelio Palacios Palacios – SENA Regional Guainía se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de Jeysser Aurelio Palacios Palacios.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (20) días del mes de (Marzo) de 2020

Como Parte Receptora:	**Por la parte reveladora:**
Jeysser Aurelio Palacios Palacios	Fernando Gonzalez Torres
Estudiante UNAD.	SENA Regional Guainía
C.C. No. 1077425096 de Quibdó	C.C. No.17.347.145 de Villavicencio

Anexo B. Formato solicitud de autorización

V0.1

Inírida, 20 de marzo de 2020

Señor:
FERNANDO GONZALEZ TORRES
Coordinador de Formación Profesional integral

Asunto: Autorización para la ejecución del proyecto titulado: Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a SENA Regional Guainía, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de Formación Profesional Integral del Sena Regional Guainía. Para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT. El cual se encuentra avalado por parte la Institución de educación superior "UNAD".

V0.1

El proyecto en su objetivo general describe lo siguiente: Implementar una metodología para identificar los riesgos, vulnerabilidades y amenazas asociados a los activos de información de la dependencia de Formación Profesional Integral de SENA Regional Guainía; al mismo tiempo será apoyado por los objetivos específicos:

- Realizar la identificación de los activos de información presentes en la Dependencia Formación Profesional Integral del SENA Regional Guainía.
- Definir los riesgos, vulnerabilidades y amenazas de los activos de información de la dependencia de formación.
- Diseñar un plan de tratamiento de riesgos y vulnerabilidades detectados a los activos de información.

Para obtener como resultado un alto impacto en la seguridad de la empresa SENA Regional Guainía.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por SENA Regional Guainía.
- La empresa SENA Regional Guainía deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.

V0.1

- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Inírida, a los (20) días del mes de (marzo) de 2020

Cordialmente,

JEYSSER AURELIO PALACIOS PALACIOS
Estudiante UNAD.

FERNANDO GONZALEZ TORRES
Coordinador de Formación Profesional integral

Anexo C. Formato FUS

"Asegúrese de consultar la versión vigente de este formato en http://sig.unad.edu.co"

UNAD Universidad Nacional Abierta y a Distancia	FORMATO ÚNICO DE SOLICITUDES	CÓDIGO: F-7-2-1
	PROCEDIMIENTO RELACIONADO: INSCRIPCIÓN Y MATRÍCULA	VERSIÓN: 3-03-10-2019
		PÁGINAS: Página 1 de 1

1. FECHA DE RADICACIÓN: 20/03/2019
2. CENTRO EN DONDE SE RADICA:

DATOS ESTUDIANTE

3. Documento de identidad: 1077425096 4. Programa: Esp. Seguridad Informática
5. Nombres y apellidos: Jeysser Aurelio Palacios Palacios
6. Correo electrónico institucional: japalaciospa@unadvirtual.edu.co
7. Correo electrónico alternativo: jeysser@misena.edu.co
8. Número telefónico móvil: 3216042960 9. Número telefónico fijo: NA

10. **TIPO DE SOLICITUD:**

Novedades		Actualización de datos		Opciones de trabajo de grado	
Adición de cursos		Autorización máx o min créditos		Diplomado profundización	
Aplazamiento de cursos		Cambio de programa		Créditos de posgrado	
Cancelación de cursos		Certificación o Constancia		Proyecto aplicado	X
Cambio de cursos		Examen de suficiencia		Proyecto de investigación	
Aplazamiento periodo		Homologación		Monografía	
Cancelación de periodo		Solicitud Reingreso		Pasantía	
Legalización de aplazamiento		Traslado de centro		Continuidad Académica	

11. JUSTIFICACIÓN PARA LA SOLICITUD: Solicitud aprobación de propuesta opción de grado.

DATOS DE LOS CURSOS CON NOVEDADES

12. Curso académico	13. Código	14. Créditos	15. Novedad

DATOS DEL RECIBO DE PAGO

16. ANEXA RECIBO DE PAGO: SI [ ] NO [X]
17. No. de factura: 18. Valor:
19. Banco: 20. Fecha de consignación:
21. APROBACIÓN: SI [ ] NO [ ]
22. OBSERVACIONES

23. Firma del Estudiante	24. Firma funcionario RCONT	25. Nombre, firma y número de documento asesor académico
Palacios		HERNANDO JOSE PELA H. CC. 76328110

Anexo D. Formato RAE

Fecha de Realización:	19/05/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Proyecto Aplicado
Título:	Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del Sena Regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT.
Autor(es):	Palacios Palacios, Jeysser Aurelio
Palabras Claves:	Análisis, Riesgo, Seguridad, Controles, Integridad.
Descripción:	Con el desarrollo del presente proyecto aplicado se busca a través de la aplicación de una metodología de gestión de Riesgo como es MAGERIT. Se realice un inventario de los activos de información con los que cuenta la dependencia de Formación Profesional Integral del SENA Regional Guainía. Para posteriormente identificar los riesgos, vulnerabilidades y amenazas asociados a dichos activos de información. Y a partir de este se puedan definir los controles y salvaguardas necesarias enfocadas a proteger los activos de información y la infraestructura tecnológica de la dependencia.

Fuentes bibliográficas destacadas:

ALVAREZ SOSA, Yenny Maribel. Diseño De Una Metodología Para El Análisis De Riesgo En Los Sistemas De Gestión De Seguridad De Información (Marisgsi) En Las Universidades De Barquisimeto Estado Lara. Trabajo De Grado Magister Scientiarum En Ciencias De La Computación. Barquisimeto: Universidad Centroccidental “Lisandro Alvarado”. 2013. 2-34p

LOPEZ, Jhon Alexander y ZULUAGA TAMAYO, Andrés Fabián. Desarrollo De Una Metodología Para El Control De Riesgos Para Auditoria De Base De Datos. Tesis De Grado Ingeniería De Sistemas Y Computación. Pereira: Universidad Tecnológica De Pereira. 2013. 5-51p.

MATALOBOS VEIGA, Juan Manuel. Análisis de Riesgo de Seguridad Informática. Trabajo de Grado analista de sistemas de información. Madrid. Universidad Politécnica de Madrid. 2009. 46-55p.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información

y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.
COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (23, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá D.C. El Ministerio, 2013. 11 p.

VÁSQUEZ GAONA, karina del Rocio. APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANALISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A EN LA CIUDAD DE MACHALA. Tesis de grado para la obtención del título Ingeniera de sistemas. Cuenca: Universidad Politécnica Salesina. Sede cuenca. Facultad de Ingeniería. 2013. 53-79p.

DUARTE MARTINEZ, Maria Carolina. DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA. Trabajo de grado presentado como requisito para optar al título de: Especialista en Seguridad Informática. Cúcuta: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2019. 29-56p.

Contenido del documento:

	7.5.2 Declaración De Aplicabilidad. 8. Conclusión 9. Recomendaciones 10. Bibliografía Anexos
Marco Metodológico:	Para poder solución a cada una de las actividades inmersas dentro de los objetivo definidos y en función al problema planteado. Se trabajó aplicando la secuencia de actividades que contempla la metodología MAGERIT. Proporcionado los insumos que permitieron a partir del hacer, hallar los resultados esperados para el aseguramiento de los activos de información asociados a la dependencia de Formación Profesional Integral del SENA Regional Guainía.
Conceptos adquiridos :	Con el desarrollo de este proyecto aplicado se abordaron procedimientos que permitieron clarificar conocimientos con relación a los controles de la norma ISO 27002:2013 para la protección de los activos de información, la gestión de riesgo para la identificación de amenazas. Igualmente se trabajaron conceptos relacionados con la integridad, la confidencialidad y disponibilidad de los datos, ataques y salvaguardas que los afectan.
Conclusiones:	Una vez desarrollado el proyecto aplicado. “Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del Sena regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT”. Se puede concluir la necesidad de establecer las condiciones de seguridad necesarias para proteger los activos de información con los que la dependencia de Formación Profesional Integral del SENA Regional Guainía. Utiliza diariamente para el cumplimiento de la meta institucional asignada por Dirección General. Lo anterior identificando las vulnerabilidades, amenazas y riesgos asociados a cada activo y de allí definir las salvaguardas y controles pertinentes que permitan realizar un tratamiento adecuado a dicha riesgo. Las medidas de seguridad adoptadas se recomiendan en el entendido de garantizar la continuidad del negocio, a partir de velar porque no sé afecte la integridad, confidencialidad y disponibilidad de los activos de información asociados a la dependencia de formación. Una apropiada y eficiente aplicación de la gestión del riesgo provee los insumos necesarios para minimizar o en su defecto eliminar los peligros que rodean no solo la información, sino

	también demás activos hardware y software con los que cuenta la dependencia de formación. Definir un plan de auditoria que basada en el modelo PHVA permita evaluar la eficiencia de los controles y salvaguardas adoptados, para mitigar el riesgo sobre cada activo de información. Determinar si el control adoptado fue o no el apropiada permitirá de manera temprana realizar las acciones de mejora a que haya lugar. Establecer un plan de capacitación a los funcionarios de la dependencia de formación sobre los protocolos de seguridad de la información y su importancia. Los cuales fueron definidos en las políticas de seguridad de la información, con el ánimo que estos sean aplicados contribuyendo al tratamiento adecuado de los datos personales de los aprendices, instructores y funcionarios, basados en la normatividad legal vigente. Siendo la información un activo valioso para la dependencia de formación. Debe en la medida de lo posible adoptar todos y cada una de las recomendaciones planteadas con el desarrollo de este proyecto. Ya que van orientadas a garantizar la confiabilidad e integridad de la información producida allí bajo estándares de seguridad internacional a través de los controles definidos en la ISO 27001:2013.