DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO

JESÚS ARMANDO CORAL OJEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO, NARIÑO
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO

JESÚS ARMANDO CORAL OJEDA

Tesis de grado para optar por el título:

Especialista En Seguridad Informática

Director de Proyecto:

Ing. Francisco Nicolás Solarte

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO, NARIÑO

2016

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

San Juan de Pasto, 11 de noviembre de 2016

DEDICATORIA

A Dios por haberme colmado de bendiciones y guiado en el camino para lograr mis objetivos a lo largo de mi formación profesional.

A mi madre Blanca Ojeda Rodríguez, quien ha sido, es y seguirá siendo mi motivo de inspiración, sostén y apoyo en mis esfuerzos de superación a lo largo de mi vida personal y profesional. A mi Abuela Judith Rodríguez y mi tía Aura Benavides por apoyarme en todo momento incondicionalmente, por motivarme a hacer frente a nuevos retos que me hicieran crecer como persona.

AGRADECIMIENTOS

A Dios en primer lugar, por haberme colmado de salud en todo momento y permitirme el concluir el desarrollo de este proyecto.

A mi familia por apoyarme incondicionalmente en todos los retos que me he propuesto, especialmente a mi Abuela Judith, a mi madre Blanca, a mi tía Aura por inculcarme que la educación es la fuente del conocimiento y que gracias a ella se logra un cambio social.

A los seres queridos que están el cielo, por contribuir en mi formación personal por medio de su experiencia y concejos.

A mi novia por su interés y motivación en creer en que soy capaz de lograr lo que me propongo.

A la vez un sincero agradecimiento a mi asesor Francisco Nicolás Solarte por haberme brindado su tiempo, apoyo y guía.

Y por último a todos los docentes de la UNAD que con mucho profesionalismo me brindaron las bases de la seguridad informática.

CONTENIDO

Pag.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del centro de estudios.

ACUERDO DE CONFIDENCIALIDAD: es un documento en los que los Funcionarios del CETEM o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del centro de estudios, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

AUTENTICACIÓN: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CENTROS DE CABLEADO: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

CENTRO DE CÓMPUTO: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo Deben cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

CIFRADO: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El

cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

CRIPTOGRAFÍA: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

CUSTODIO DEL ACTIVO DE INFORMACIÓN: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

DERECHOS DE AUTOR: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

DISPONIBILIDAD: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

EQUIPO DE CÓMPUTO: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

GUÍAS DE CLASIFICACIÓN DE LA INFORMACIÓN: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

HACKING ÉTICO: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y

sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

INCIDENTE DE SEGURIDAD: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: es una lista ordenada y documentada de los activos de información pertenecientes al centro de estudios.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MEDIO REMOVIBLE: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

PERFILES DE USUARIO: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

PLATAFORMA TECNOLÓGICA: Es en conjunto la red de datos (incluyendo sus servicios), los recursos tecnológicos y sistemas de información del centro de estudios CETEM

PROPIEDAD INTELECTUAL: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones

científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

RECURSOS TECNOLÓGICOS: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del CETEM.

REGISTROS DE AUDITORÍA: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del centro de estudios. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

RESPONSABLE POR EL ACTIVO DE INFORMACIÓN: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

SISTEMA DE INFORMACIÓN: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el CETEM o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SISTEMAS DE CONTROL AMBIENTAL: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas

características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

SOFTWARE MALICIOSO: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

TERCEROS: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos al centro de estudios.

VULNERABILIDADES: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el centro de estudios (amenazas), las cuales se constituyen en fuentes de riesgo.

RESUMEN

En la actualidad las redes de datos como parte de una plataforma tecnológica permiten agilizar gran cantidad de tareas dentro de un centro de formación para el trabajo y desarrollo humano. Como es el caso del Centro De Estudios EMSSANAR CETEM, la red de datos es fundamental para el desarrollo de labores administrativas y académicas ya que permite la comunicación interna y externa de funcionarios, docentes y estudiantes. Lastimosamente esta red es de uso público y no cuenta con las medidas de seguridad y de control físico y lógicos adecuados.

Por lo antes expuesto, el presente proyecto, tiene como propósito mostrar el proceso de diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO27001:2013 en el centro de estudios EMSSANAR CETEM de la ciudad de pasto a través de unas fases estructuradas, partiendo del análisis de riesgos sobre los activos de información relacionados con la investigación a través de la metodología MAGERIT, siguiendo con la identificación de controles implementados teniendo como referencia la ISO/IEC 27002:2013 y la escala de madurez del COBIT 4.1 y terminando con la definición de las políticas de seguridad acordes con los objetivos del negocio y valoración de los activos de información.

PALABRAS CLAVE: SGSI, Seguridad informática, Análisis y Evaluación de Riesgos, Magerit, ISO/IEC 27001:2013, ISO/IEC 27002:2013, Activo de información.

ABSTRACT

At present, data networks as part of a technological platform allow a large number of tasks to be carried out within a training center for work and human development. As is the case of the Centro de Estudios EMSSANAR CETEM, the data network is fundamental for the development of administrative and academic tasks as it allows the internal and external communication of officials, teachers and students. Unfortunately, this network is for public use and does not have adequate security and physical and logical control measures.

For the above, the present project aims to show the process of designing a safety management system for data network under the ISO27001: 2013 standard at the Centro de estudio EMSSANAR CETEM of the city of Pasto through Of structured phases, based on the analysis of risks related to the research assets related to the research through the MAGERIT methodology, followed by the identification of controls implemented with reference to ISO / IEC 27002: 2013 and the COBIT maturity scale 4.1 and ending with the definition of security policies in line with business objectives and valuation of information assets.

KEYWORDS: ISMS, IT Security, Risk Analysis and Evaluation, Magerit, ISO / IEC 27001: 2013, ISO / IEC 27002: 2013, Information Asset.

INTRODUCCIÓN

En la actualidad Colombia cuenta con una gran cantidad de instituciones que brindan formación para el trabajo y el desarrollo humano; muchas de estas instituciones ofrecen los mismos programas técnicos pero las diferencian algunos factores como: precio, calidad, atención al cliente, agilidad, servicio, entre otros. Teniendo en cuenta este nivel de competencia, lo que buscan estas instituciones educativas es estar a la vanguardia de la tecnología con el fin de mantenerse en el mercado y consolidarse como instituciones reconocidas.

Es muy común que las instituciones educativas implementen soluciones tecnológicas, con el fin de facilitar el desarrollo de sus actividades y mejorar los servicios prestados, este es el caso del Centro de Estudios EMSSANAR CETEM que actualmente cuenta con una infraestructura de red que soporta el tráfico de información tanto interna como externa.

Sin embargo, este tipo de implementación de tecnologías sin la correcta gestión permite el acceso sin autorización a información privada de la empresa, la cual podría ser alterada o en el peor de los casos robada.

Teniendo en cuenta lo anterior, lo que se pretende con el presente proyecto, es diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO27001:2013 en el centro de estudios EMSSANAR CETEM de la ciudad de pasto teniendo en cuenta el contexto del negocio.

1. TÍTULO

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO

2. PROBLEMA

2.1. PLANTEAMIENTO DEL PROBLEMA

El Centro de Estudios EMSSANAR CETEM es un programa de la Fundación EMSSANAR, cuya organización empresarial se basa en la economía solidaria, con proyección nacional e internacional; que desde el sur occidente colombiano presta servicios educativos en las áreas de salud, educación técnica, comercialización de alimentos, asistencia técnica socio-empresarial y micro crédito. Su objetivo es contribuir a la generación de capital social y desarrollo sostenible de la región, a través de procesos pertinentes de educación técnica laboral bajo el modelo de competencias, que permitan la vinculación del egresado al sector productivo. [1]

El Centro de Estudios EMSSANAR CETEM cuenta con una plataforma tecnológica (en este proyecto se refiere a la red de datos, los recursos tecnológicos y sistemas de información en conjunto) que posibilita el desarrollo tanto de tareas académicas como administrativas. En este punto la red de datos del CETEM se convierte en una herramienta importante por no decir esencial, ya que soporta el tráfico de red en general.

Lastimosamente está red de datos se accede a través de una infraestructura que es de uso público al interior del centro de estudios, lo que posibilita que la información generada durante o al final de la jornada sea interceptada, robada y/o modificada sin autorización por estudiantes, docentes o administrativos y en el peor de los casos por externos.

Adicionalmente al no haber un control de usuarios que acceden a la red de datos, cada usuario puede realizar usos excesivos de ancho de banda o perpetrar algún

[1] **Tomado de:** Portafolio de Servicios Centro de Estudios EMSSANAR CETEM

tipo de ataque informático y provocar fallas que por ende entorpecen los procesos de la organización.

De continuar esta situación, el Centro de Estudios EMSSANAR CETEM perdería la confiabilidad y prestigio que se ha ganado como centro de formación para el trabajo y desarrollo humano, sin contar con la incalculable pérdida económica y de información.

2.1.1. Formulación Del Problema

De acuerdo a lo anteriormente expresado, surge el siguiente interrogante: ¿Cómo el sistema de gestión de seguridad para la red datos ayudará a mejorar la seguridad informática en Centro de Estudios EMSSANAR CETEM?

2.2. JUSTIFICACIÓN

El Centro de Estudios EMSSANAR CETEM al igual que cualquier organización sin importar su razón de ser requieren almacenar, tratar y transformar la información como un recurso valioso y predominante en el desarrollo de sus actividades académicas y administrativas , es así que ésta se convierte en atractivo sensible de ser vulnerado y atacado por quienes buscan un beneficio económico estratégico o simplemente de sabotaje, sin embargo ante estas circunstancias algunas organizaciones que mueven grandes y pequeños volúmenes de información, prestan poca atención al tema de seguridad y protección de sus datos en tal medida que no se invierten los recursos suficientes para establecer controles que fortalezcan la seguridad de la información; en este contexto el 40% de pymes en Colombia tuvieron incidentes relacionados con acceso indebido a aplicaciones y/o base de datos, que aunque no es la cifra más alta a nivel Latinoamérica, si es bastante preocupante ya que según la empresa de seguridad ESET afirman que generalmente la causa de estos incidentes es la inexistencia de controles o perfiles correctos en las redes empresariales, lo que ocasiona que personal de otras áreas o sectores logren acceder a planes confidenciales de la gerencia, administración, recursos humanos y demás[2].

En Centro de Estudios EMSSANAR CETEM el flujo de información es bastante heterogéneo al igual que usuarios que acceden a la red, lo que posibilita que se potencialicen los riesgos de robar, dañar, alterar o simplemente sabotear información. Por esta razón se hace imprescindible, y por ende justificable, que se reduzcan los riesgos de manera oportuna,

[2] ESET, (23 de Octubre de 2015). Security Report Latinoamérica 2015. Obtenido de http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

El presente proyecto se realizará para contribuir con algunas políticas de seguridad basados en la evaluación de riesgos, que puedan ser usados con el fin de reducir las amenazas o mitigar riesgos de seguridad hasta considerarlos como aceptable para la organización.

Con este proyecto, la entidad dará un primer paso para poder certificarse con el estándar ISO/IEC 27001:2013, el cual contribuirá a mejorar la competitividad en el mercado, diferenciando al Centro de Estudios EMSSANAR con otros de su sector, haciéndolo más fiable e incrementando su prestigio. Un certificado mejora la imagen y confianza de la empresa con sus clientes, lo que le sumara la posibilidad de tener más socios y así brindar capacitación y asesoramiento a otras empresas.

2.3. OBJETIVOS

2.3.1. Objetivo General

Diseñar un sistema de gestión de seguridad bajo la norma ISO27001:2013 para la red datos en el centro de estudios EMSSANAR CETEM de la ciudad de pasto.

2.3.2. Objetivos Específicos

- Aplicar la metodología Magerit para realizar el proceso de análisis de riesgos a los activos de información y tecnológicos más relevantes para el CETEM.
- Identificar las políticas de seguridad y los controles implementados en la red de datos del centro de estudios EMSSANAR CETEM de acuerdo a la norma ISO/IEC 27002.2013 y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala de madurez definida por el estándar COBIT.
- Definir un conjunto de políticas compatibles con la dirección estratégica que busque de manera constatable la satisfacción del subsistema de gestión de seguridad de la información propuesto.

2.4. MARCO REFERENCIAL

2.4.1. Antecedentes

Uno de los objetivos primordiales del Ministerio de las TIC es Diseñar, formular, adoptar y promover las políticas, planes, programas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la ley, con el fin de contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos[3].

Teniendo en cuenta que el centro de estudios de EMSSANAR CETEM indirectamente contribuye con este fin mediante la participación en la convocatoria TALENTO DIGITAL [4]por ser un centro de formación para el trabajo y desarrollo humano, es fundamental que adopte modelos de calidad para asegurar la información como lo plantea en una de sus metas[5]. Una buena práctica sugerida por Gobierno en Línea su momento fue ISO/IEC 27001:2005, sin embargo, dicha norma fue actualizada el año en 2.013.

Cada día crece a nivel mundial la cantidad de empresas que abordan proyectos de implementación de Sistemas de Gestión de Seguridad de la Información y logran certificarse en la norma ISO27001, según la encuesta anual de ISO, al finalizar el año 2015 existían 27.536 empresas certificadas, de las cuales solo 103 eran Colombianas[6].

A cerca de ese tema se han realizado diferentes trabajos de investigación en Colombia en el sector académico tales como:

---

[3] MINTIC. Objetivos y funciones , http://mintic.gov.co/portal/604/w3-article-1939.html

[4] ICETEX. Listado de programas válidos para la convocatoria “talento digital” 2013-2, https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/Fondos/list_program_Con2013-2%20TD.pdf

[5] http://www.colciencias.gov.co/sites/default/files/upload/convocatoria/Anexo1_2.pdf

[6] ISO, Survey 2015, http://www.iso.org/iso/iso_27001_iso_survey2015.xls

- **Implementación de un sistema de gestión de seguridad de la Información (SGSI) en la comunidad nuestra señora de gracia, Alineado tecnológicamente con la norma ISO 27001**

  Este trabajo es el resultado de un proyecto de investigación en la Comunidad Nuestra Señora de Gracia, de la ciudad de Bogotá, con la finalidad de implementar un SGSI en dicha institución, quienes realizaron un proceso de diagnóstico, a partir del cual concluyeron que no tenían definidas políticas y procesos adecuados para el correcto manejo de la seguridad de la información. A partir de allí elaboraron un plan piloto para elaborar políticas ajustadas a la norma ISO/IEC 27001 e implementaron un sistema de información para levantamiento de información, análisis de brechas y GAP. Por último, establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado[7].

- **Política para la seguridad de la información de la Universidad Distrital Francisco José de Caldas.**

  La Universidad Distrital Francisco José de Caldas enfrenta amenazas de seguridad que la lleva a un proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales. De tal manera ha definido una política de seguridad de la información que permite detallar el alcance de la misma, identificar, clasificar y valorar los activos de información, valorar la seguridad de los recursos humanos, determinar las responsabilidades del

[7] Implementación de un sistema de gestión de seguridad de la Información (SGSI) en la comunidad nuestra señora de gracia, Alineado tecnológicamente con la norma ISO 27001, http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

personal, valoración de seguridad física, controles de acceso, entre otras políticas[8].

2.4.2. Marco Contextual

Inicialmente la asociación mutual de la cruz hoy parte de la empresa EMSSANAR en desarrollo y cumplimiento de los principios legales, donde existen sus propios estatutos, presentó y desarrolló una interesante propuesta de capacitación en el nivel técnico, creando así el instituto denominado centro de estudios técnicos del norte de Nariño (CETEM), con el cual se espera cumplir los deberes de capacitación en educación mutual, prestar un servicio educativo a la región, brindando capacitación técnica a la juventud y desarrollo de la empresa y sus asociados a través de un proceso de planificación educativo, democrático y participativo y continuar el mejoramiento social en el área de influencia.

El centro de estudios técnicos inicia su proceso de constitución con los acuerdos no. 10 de agosto 30 de 1998, en el cual faculta a la gerente de la asociación para adelantar el trámite correspondiente para obtener licencia de funcionamiento y los convenios que sean necesarios para poner en funcionamiento la institución y el acuerdo no 11 de 4 de octubre de 1998, fija los estatutos para el funcionamiento del CETEM. Seguidamente se presenta a la secretaria de educación el proyecto para la aprobación del centro de estudios técnicos del norte de Nariño CETEM y obtener la licencia de funcionamiento. El 30 de octubre de 1998 en un acto solemne inicia sus labores el denominado centro de estudios técnicos del norte de Nariño, en el municipio de la cruz matriculándose 120 estudiantes en las tres modalidades técnicas, extendiendo posteriormente su radio de acción a los municipios vecinos de san José de Albán, san Bernardo, belén y san pablo, los cuales cuentan con las respectivas licencias de funcionamiento.

---

[8] https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

2.4.2.1. **Planeación y estructura estratégica**

2.4.2.2. **Misión:**

Somos un Centro de estudios comprometido con la formación para el trabajo y el desarrollo humano, que se rige por los principios de solidaridad, liderazgo, y responsabilidad social, brindando servicios educativos en las áreas de: sistemas, financieras y de salud que contribuyan a la formación integral de jóvenes y adultos del departamento de Nariño, con espíritu emprendedor, crítico y solidario. Contamos con un talento humano comprometido, cualificado y una infraestructura física y tecnológica acorde a las áreas de formación establecidas. Nuestro campo de acción se centra en la formación por competencias de conformidad a las exigencias del sector productivo y a la normatividad vigente del sistema educativo.

2.4.2.3. **Visión:**

En el año 2019 seremos un Centro de estudios de la economía solidaria, reconocida por su aporte a la generación de capital social y desarrollo sostenible.

2.4.2.4. **Valores**

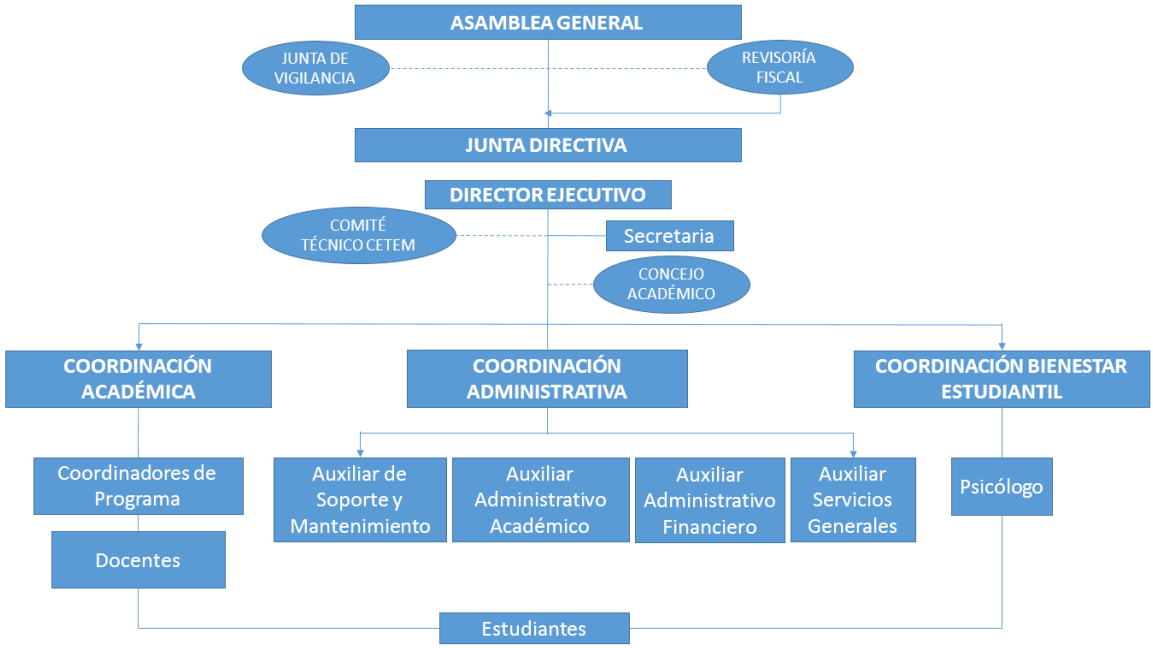
Liderazgo: Es una conducta expresada en nuestro diario vivir, caracterizada por la capacidad de logro, de innovar, de aprender, de trabajar en equipo, de proponer soluciones, donde la coherencia de nuestras decisiones y acciones, inciden de manera positiva en nuestra Organización y en la sociedad.

Solidaridad: Es un acto de conciencia interior individual y colectivo, que determina nuestro quehacer y permite dimensionar la realidad social y económica del entorno, estimulando la búsqueda compartida de soluciones que permitan contribuir al bienestar de la sociedad, el estado, la familia, nuestros clientes y el desarrollo empresarial.

Responsabilidad Social: Es el proceder empresarial que busca beneficiar de manera permanente a sus grupos de interés con procesos de desarrollo sostenible y sustentable actuando desde las dimensiones: social, económica y ambiental.

2.4.2.5. **Estructura Orgánica de la Fundación**

Figura 1. Estructura Orgánica de la Fundación CETEM



Fuente: Organigramas [En línea] <http://www.emssanar.org.co/contenidos/grupocorporativo/organigrama/ORGANIGRAMAS_EPS_2011.pdf>

2.4.2.6. **Estructura Orgánica del área de Redes y Sistemas**

Figura 2. Estructura Orgánica del área de Redes y Sistemas

Fuente: Organigramas [En línea] <http://www.emssanar.org.co/contenidos/grupocorporativo/organigrama/ORGANIGRAMAS_EPS_2011.pdf>

El área de redes y sistemas divide está bajo la responsabilidad del auxiliar de soporte y mantenimiento pero generalmente tiene la colaboración de uno o dos pensantes por cada jornada.

Funciones auxiliar de soporte y mantenimiento:

Se asemeja mucho al cargo de Jefe de Sistemas, incluyendo la función de supervisar a los pasantes, las funciones principales del auxiliar de soporte y mantenimiento son:

- Resolver problemas de información y/o equipos en general.
- Revisión y corrección de problemas en las diferentes áreas.
- Revisión de problemas de red.
- Desarrollo de reportes.
- Apoyo a usuarios en la solución de problemas informáticos.
- Apoyo de adquisición de equipos informáticos.
- Apoyo en la adquisición de software.
- Administrar el sistema Q10 Académico.
- Mantener información actualizada en el sistema SE Suite.
- Actualizar y mantener Sistema de Evaluación Docente (SED).
- Administrar el Sistema de Control de Asistencia Administrativos (SCAA).

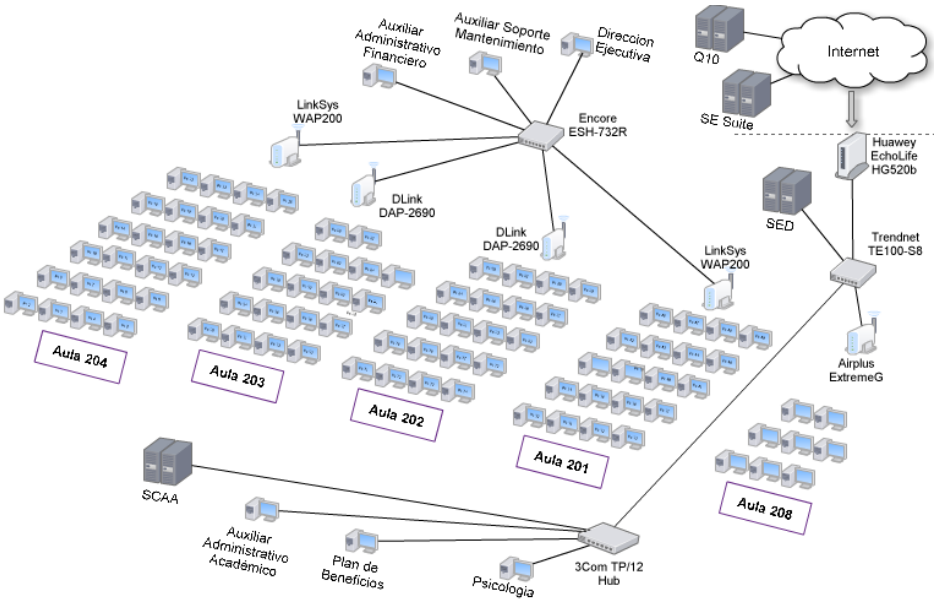
Pasante:

Su jefe inmediato es el auxiliar de soporte y mantenimiento, las funciones principales del Pasante son:

- Dar soporte a los Administrativos, Docentes y Estudiantes.
- Realizar mantenimiento preventivo y correctivo a los equipos de cómputo.
- Obtener respaldos de información.
- Actualizar inventarios de equipos.
- Revisar conectividad de red.
- A criterio de su jefe inmediato puede realizar otras funciones.
- Préstamo de equipos de cómputo y otros accesorios.

2.4.2.7. **Distribución de la red LAN - Centro de Estudios EMSSANAR CETEM**

Figura 3. Topología de red de datos del CETEM



Fuente: Esta investigación

En la Figura 6, se observa claramente el alcance tecnologico y la comunicación entre cada una de las estaciones de trabajo, que se encuentran ubicadas en las diferentes aulas y oficinas del centro de estudios EMSSANAR CETEM. Se puede apreciar que el medio de transmision en la red es mixto, es decir existen partes cableadas y partes inalambricas, ademas que no cuenta con una apropiada segmentacion de red, dejando que cualquier equipo que se conecte de manera cableada o inalambrica pueda observar tanto los dispositivos como los equipos conectados de las aulas y oficinas.

Con la informacion proporcionada por el Auxiliar de Soporte y Mantenimiento, se tiene que el numero de equipos cliente es de aproximadamente 90 equipos que se eleva de acuerdo al numero de estudiantes que traigan laptops o smartphones. Referente al cableado de la red, en la empresa se tiene un cableado estructurado categoria 5, sin embargo solo se encuentra parcialmente implantado y en algunos

casos sin tener encuenta las normas de cableado estructurado. Es importante mensionar que el crecimiento de la red no a sido de manera organizada, por lo que se tiene una red hibrida entre sectores cableados y sectores inalambricos, para satisfacer las necesidades de infraestructura tecnologica del centro de estudios EMSSANAR CETEM.

2.4.3. Marco Teórico

2.4.3.1. **Plataforma tecnológica**

Es en conjunto la red de datos (incluyendo sus servicios), los recursos tecnológicos y sistemas de información del centro de estudios CETEM.

2.4.3.2. **Seguridad Informática**

Se relaciona directamente con la seguridad de la información. La seguridad informática se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden comprometer la confidencialidad, autenticidad o integridad de la información, disminuyendo el rendimiento de los equipos e inclusive bloqueando el acceso de usuarios autorizados al sistema y daños en la información,

También se puede decir que es la disciplina de proteger y resguardar la información gestionada, administrada y operada en los dispositivos los cuales son: estaciones de trabajo, portátiles, PDA´s y equipos de comunicación.

2.4.3.3. **Seguridad de la Información**

Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla criterios de:

- Confidencialidad, garantía de que la información sea accedida por las personas convenientemente autorizadas.
- Integridad, la información debe mantenerse permanentemente correcta, compleja y protegida.

- Disponibilidad, la información debe estar disponible para su uso, cuando se lo requiera. También se considera como parte de la disponibilidad, la rapidez con que se puede ofrecer servicios o realizar operaciones.[9]

2.4.3.4. **Familia ISO/IEC 27000**

La familia ISO/IEC 27000 Estándares de seguridad de la información, provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información, generalmente aceptadas. En concreto el listado actual de normas que se encuentran en desarrollo y finalizadas son:

Tabla 1. Relación de serie de las normas ISO/IEC 27000

NORMA	DESCRIPCIÓN
ISO/IEC 27000	Proporcionará una vista general del marco normativo y un vocabulario utilizado por las normas de la serie.
ISO/IEC 27001:2013	Especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI).Publicada en 2013.
ISO/IEC 27002:2013	Código de buenas prácticas para la gestión de la seguridad de la información describe el conjunto de objetivos de control y controles a utilizar en la construcción de un SGSI (actualizada desde la ISO/IEC 17799:2005 y renombrada en el 2013 como ISO 27002:2013).
ISO/IEC 27003	Proporcionará una guía de implantación de la norma ISO/IEC 27001.
ISO/IEC 27004	Describirá los criterios de medición y gestión para lograr la mejora continua y la eficacia de los SGSI.
ISO/IEC 27005	Proporciona criterios generales para la realización de

[9] TUPIA, Manuel. Administración de la Seguridad de la información. Editorial Editex S.A. Madrid España 2009. p9
(240 Paginas).

NORMA	DESCRIPCIÓN
	análisis y gestión de riesgos en materia de seguridad.
ISO/IEC 27006:2007	Es una guía para el proceso de acreditación de las entidades de certificación de los SGSI. Publicada en 2007.
ISO/IEC 27007	Será una guía para auditar SGSI.
ISO/IEC TR 27008	Proporcionará una guía para auditar los controles de seguridad de la norma ISO 27002:2013.
ISO/IEC 27010	Proporcionará una guía específica para el sector de las comunicaciones y sistemas de interconexión de redes de industrias y Administraciones, a través de un conjunto de normas más detalladas que comenzarán a partir de la ISO/IEC 27011.
ISO/IEC 27011	Será una guía para la gestión de la seguridad en telecomunicaciones (conocida también como X.1051)
ISO/IEC 27031	Estará centrada en la continuidad de negocio
ISO/IEC 27032	Será una guía para la cyberseguridad.
ISO/IEC 27033	Sustituirá a la ISO/IEC 18028, norma sobre la seguridad en redes de comunicaciones.
ISO/IEC 27034	Proporcionará guías para la seguridad en el desarrollo de aplicaciones.
ISO/IEC 27799	No será estrictamente una parte de la serie ISO 27000 aunque proporcionará una guía para el desarrollo de SGSI para el sector específico de la salud.

Fuente: ISO 27001 – Sistema de gestión de información [En línea] < http://es.slideshare.net/JABERO241/0405-iso-27000present-final>

2.4.3.5. **ISO/IEC 27002:2013**

Se trata de la segunda edición de la norma, la cual reemplaza y cancela el SO/IEC 27002:2005. Con 14 secciones y 113 controles, esta norma contiene el Código para la práctica de la gestión de la seguridad de la información (previamente BS 7799 Parte 1 y la norma ISO/IEC 17799). Este estándar Internacional establece

los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

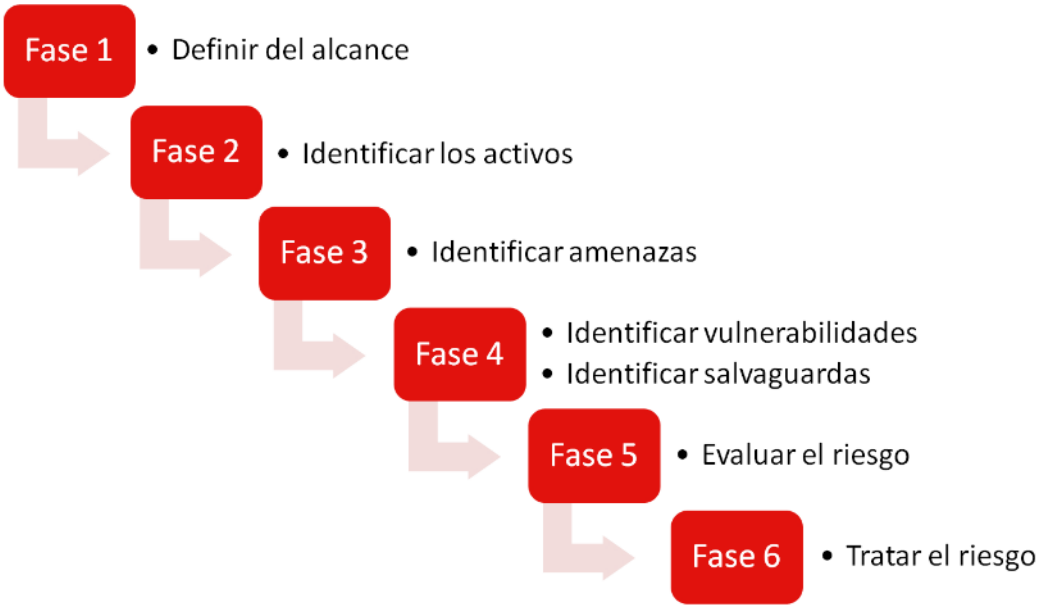
Figura 4. ISO 27002:2005 vs ISO 27002:2013

Fuente: La nueva versión ISO 27001[En línea] < http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/download/125_2f7be404f0dba27dabc8efd91bd14668.html>

2.4.3.6. **Metodologías de Análisis y Evaluación de Riesgos.**

Aunque el análisis de riesgos depende de la metodología escogida, según INCIBE[10] existen un conjunto de fases que son comunes en la mayor parte de las metodologías.

Figura 5. Fases análisis de riesgos



Fuente: ¡Fácil y sencillo! Análisis de riesgos en 6 pasos [En línea] < https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

- **Fase 1. Definir el alcance:** El primer paso a la hora de llevar a cabo el análisis de riesgos es establecer el alcance del estudio, ya sea un área estratégica o limitarlo a un departamento, proceso o sistema.
- **Fase 2. Identificar activos:** Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

[10] INCIBE, ¡Fácil y sencillo! Análisis de riesgos en 6 pasos, https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

- **Fase 3. Identificar amenazas:** Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos.
- **Fase 4. Identificar vulnerabilidades y salvaguardas:** La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.
- **Fase 5. Tratar riesgo:** Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

2.4.3.7. **MAGERIT 3**

MAGERIT, desarrollada en España por el Consejo Superior de Administración Electrónica es, al igual que AS/NZS, una metodología para administrar riesgos, que persigue los siguientes objetivos:

- Hacer saber a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo.
- Ofrecer un método para analizar los riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Apoyar la preparación a la empresa para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

El análisis de riesgos propuesto por MAGERIT 3 es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la empresa.
- Determinar las amenazas a la que están expuestos aquellos activos.

- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza.
- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información.
- Valorar las amenazas potenciales.
- Estimar el riesgo.

Diagnostico e identificación de los riesgos.

Este proceso surge de la utilización de las herramientas o las metodologías apropiadas en las cuales se pueden encontrar la forma metódica para efectuar el análisis en base a la organización en la que se pretenda análisis en este sentido se tienen en cuenta tres variables fundamentales sobre las cuales se basa la operación de análisis: activos, las amenazas y las vulnerabilidades son el objeto para identificar los riesgos, dado que una brecha no detectada permite la entrada al sistema de posibles amenazas.[11] En la figura 3, se ilustra el proceso a seguir en la gestión de riesgos.

- El hallazgo del peligro consiste en especificar el acontecimiento adverso que genera motivo de preocupación.
- Para la evaluación del riesgo hay que tener en cuenta la probabilidad (real y no sólo la posibilidad) de que se genere el peligro, las consecuencias si se materializa y el grado de incertidumbre.
- La gestión del riesgo consiste en la definición y aplicación del mejor control para reducir o eliminar la probabilidad de que se genere el peligro.

[11] GOMEZ, R. D. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería

- La comunicación del riesgo es el intercambio franco de información y asesorías aclaratorias que generan una mejor comprensión y adopción de medidas.[12]

Figura 6. Gestión de Riesgos

Fuente: Sistema de Gestión de la Seguridad de la Información [En línea] <http://www.iso27000.es/download/doc_sgsi_all.pdf>

2.4.3.8. **Modelo de Madurez COBIT 4.1**

COBIT es un framework (también llamado marco de trabajo) de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a

[12]ISO27000.ES (2013). Sistema de Gestión de la Seguridad de la Información, http://www.iso27000.es/download/doc_sgsi_all.pdf

los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

En el presente proyecto se tendrá en cuenta el modelo de madurez que está clasificado en 5 niveles que puede alcanzar una institución de acuerdo a la administración de riesgos TI.[13]

0 No Existente

Cuando la organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos.

La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para presentar servicios de TI.

1 Inicial /Ad Hod

Cuando se realizan evaluaciones informales de riesgos tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto, es decir que existe un entendimiento emergente que los riesgos de TI son importantes y necesitan ser considerados.

2 Repetible pero intuitivo

Cuando la administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.

3 Definido

Cuando la administración de riesgos sigue un proceso definido, el cual esta documentado.

4 Administrado y Medible

---

[13] Cobit 4.1, http://datateca.unad.edu.co/contenidos/210114/cobiT4.1spanish.pdf

Cuando los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI, otorgado por parte de la gerencia de presupuesto para un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular.

5 Optimizado

Cuando la administración de riesgos altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios TI y cuando la dirección evalúa las estrategias de mitigación de riesgos de manera frecuente.

2.4.4. Marco Conceptual

Probabilidad

Para determinar la probabilidad de ocurrencia es posible de la forma cualitativa o cuantitativamente, considerando que la medida no debe contemplar la existencia de acciones de control.

Amenazas

Son acciones que pueden generar consecuencias negativas en la operación de la organización. Se referencian como amenazas a las fallas, los ingresos no autorizados, los virus, los desastres ocasionados por fenómenos naturales o ambientales, etc.

Vulnerabilidades

Son ciertas condiciones a las que se exponen los activos, están presentes en su entorno, facilitan que las amenazas se materialicen y se conviertan en vulnerabilidad.

Riesgos

La ISO 27002:20013 plantea que el riesgo es la combinación de la probabilidad de un evento y sus posibles consecuencias, esta definición es la que se tomó en cuenta para el desarrollo del presente proyecto14.

Activos

Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes, las comunicaciones y la información en sí misma.

Impactos

Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.

2.4.5. Marco Legal

- ✓ Ley 527 de Agosto de 1999 Comercio electrónico. Por medio del cual se define y reglamenta el acceso y usos de los mensajes de datos del comercio electrónico y de las firmas digitales y se establece las entidades de la certificación y se dictan otras disposiciones.[15]
- ✓ Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data que se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (15Ma). Esta ley

---

[14] ISO 27001:2013 Information technology – Security techniques – Information security management systems - Requirements. 2nd Edition

[15] http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

se refiere al que todo individuo puede conocer, actualizar y rectificar toda información que se relacione con él, la cual se encuentra almacenada en centrales de información.[16]

- ✓ Ley 1273 de 2009 Protección de la Información y de los Datos en Colombia. 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.[17].
- ✓ Ley 1341 de 2009. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.[18]
- ✓ Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.[19]

---

[16]http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

[17]http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[18]http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[19] http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

2.4.6. Marco Metodológico

El desarrollo del proyecto abarca una serie de fases definidas que comprenden actividades que aseguran el cumplimiento del objetivo final del proyecto.

Para el diseño de un sistema de gestión de seguridad para la red datos del centro de estudios EMSSANAR CETEM de la ciudad de pasto se ha tenido en cuenta el estándar para la seguridad de la información ISO/IEC 27001:2013 a fin de aplicarlas en todas las fases del trabajo. Este estándar define los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

2.4.6.1. **Tipo de investigación**

El enfoque de la investigación es cuantitativo ya que se pretende hacer la medición de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información.

Es una investigación de tipo explicativa porque se trata de explicar la relación existente entre las vulnerabilidades existentes y los ataques que pueden presentarse en el sistema de información a causa de esas vulnerabilidades.

Es descriptiva porque trata de describir cómo se lleva a cabo el proceso de análisis y evaluación de los riesgos haciendo uso de la metodología MAGERIT.

2.4.6.2. **Metodología de desarrollo**

El proyecto está enfocado al diseño de un Sistema de Gestión de Seguridad de la Información SGSI bajo la norma ISO/IEC 27001:2013, que permita definir las políticas de seguridad orientadas a la disminución de riesgos para la red de datos del centro de estudios EMSSANAR CETEM de la ciudad de pasto, y a satisfacer los requerimientos necesarios para la prestación de un buen servicio con eficiencia y calidad.

Para el desarrollo satisfactorio del proyecto se identificaron las siguientes actividades por cada objetivo específico de proyecto:

Objetivo 1: Aplicar la metodología Magerit para realizar el proceso de análisis de riesgos a los activos de información y tecnológicos más relevantes para el CETEM.

- **Recopilación y análisis de información:** Esta actividad busca recolectar la mayor cantidad de información posible con respecto al estado actual, estudios o proyectos que tengan relación con el análisis de riesgos y en general en materia de seguridad informática en la centro de estudios.
- **Diseño de un plan de trabajo:** Esta actividad hace referencia a la construcción de un cronograma de actividades general que establezca límites de tiempo y asignación de tareas para lograr el desarrollo del proyecto.
- **Reconocimiento de activos de información valiosos:** Esta actividad permite identificar, clasificar, valorar y seleccionar los activos de información y tecnológicos más relevantes para esta investigación.
- **Identificación de amenazas:** Utilizando el catálogo de amenazas del MAGERIT identificar cuales se encuentran presentes en los activos de información y tecnológicos seleccionados.
- **Identificación de vulnerabilidades:** A través de observación directa con la supervisión de un delegado del AREA DE REDES Y SISTEMAS y a través de Hacking ético encontrar el estado actual de los activos de información y tecnológicos seleccionados desde el punto de vista de seguridad de la información.
- **Evaluación de riesgos:** Se califica la probabilidad y el alcance del daño producido sobre los activos de información y tecnológicos seleccionados en caso de que se llegue a materializar una amenaza.
- **Tratamiento de riesgos:** Se toma decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la organización.

Objetivo 2: Identificar las políticas de seguridad y los controles implementados en la red de datos del centro de estudios EMSSANAR CETEM de acuerdo a la norma ISO/IEC 27002.2013 y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala de madurez definida por el estándar COBIT.

- **Lectura de documentos normativos:** Se realiza lectura de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013.
- **Elaboración lista de chequeo:** Se seleccionan los dominios y controles a evaluar de la norma ISO/IEC 27002:2013.
- **Verificación controles ISO/IEC 27002:2013**: Se le asigna un valor a cado control de la norma de acuerdo al nivel de madurez establecido por COBIT 4.1

Objetivo 3: Definir un conjunto de políticas compatibles con la dirección estratégica que busque de manera constatable la satisfacción del subsistema de gestión de seguridad de la información propuesto.

- **Lectura de políticas de seguridad:** Se realiza lectura de varias políticas de seguridad de otras instituciones y documentos afines.
- **Definición de políticas de seguridad:** De acuerdo a los dominios y controles evaluados se definen las políticas de seguridad del CETEM a implementarse.
- **Presentación de las políticas**: Se le da a conocer las políticas definidas al AREA DE REDES Y SISTEMAS.

3. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO

3.1. APOYO DE LA DIRECCIÓN EJECUTIVA

Para la consecución de un proyecto de este tipo es esencial el apoyo y colaboración de la dirección y el personal involucrados en los diferentes procesos internos, siendo de mucha importancia el suministro de información veraz, concreta y a tiempo necesaria para el desarrollo de las actividades contempladas en este proyecto, por esta razón hay un compromiso desde la dirección de bridar el apoyo necesario, en la medida requerida para la consecución del proyecto.

3.2. ALCANCE

El alcance de proyecto incluye:

- Definición de los activos del Centro de Estudios EMSSANAR CETEM que necesitan protegerse de acuerdo a la norma ISO 27001.
- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en el Centro de Estudios EMSSANAR CETEM.
- Verificación de controles de seguridad de la información que se llevan a cabo en el Centro de Estudios EMSSANAR CETEM teniendo en cuenta la norma ISO 27002.
- Estructuración del Sistema de Gestión de Seguridad de la Información para el Centro de Estudios EMSSANAR CETEM.

Los dominios, objetivos de control y controles que contempla la norma ISO 27002 son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información

- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes en la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

El presente proyecto está orientado a proponer una serie de Políticas de Seguridad de la Información para el Centro de Estudios EMSSANAR CETEM.

La norma ISO/IEC 27001 no impone ninguna metodología referente a análisis y evaluación de riesgos, debido a que existen varias aceptadas internacionalmente, por esta razón la institución está en libertad de elegir la que más se acople a sus necesidades o crear su propia metodología acoplando cualquiera de ellas.

La metodología para análisis y evaluación de riesgos utilizada en este proyecto fue MAGERIT debido a que esta fue creada específicamente para determinar qué valor está en juego con respecto a las Tecnologías de la Información y Comunicaciones (TIC) frente a los riesgos que estas están sometidos dentro de la institución con el fin de mitigarlos implementando controles apropiados y oportunos.

Esta metodología persigue una aplicación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT, está conformado por tres libros: El primero es el Método, en el que se describe la estructura del análisis y de la gestión de riesgos.

El análisis de riesgos es una aproximación sistemática para determinar el riesgo siguiendo unos pasos:

- Definir los activos de información importantes para la organización.
- Definir las amenazas y vulnerabilidades existentes para los activos de información seleccionados.
- Verificar los controles de seguridad de la información que se llevan a cabo en la organización.
- Estimar el impacto sobre un activo de información derivado de la materialización de una amenaza.
- Estimar el riesgo (Riesgo = Probabilidad x Impacto).

El segundo es un Catálogo de Elementos que ofrece unas pautas y elementos estándar en cuanto a tipos de activos, dimensiones de valoración de los activos, escala de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información. Y por último una Guía de Técnicas y ejemplos de cómo llevar a cabo el análisis de riesgos por medio de tablas, algoritmos, arboles de ataque, técnicas gráficas, etc. Este documento de técnicas convierten está metodología en un factor diferenciador con respecto a otras metodologías.

MAGERIT es muy útil para las organizaciones que inician con la gestión de seguridad de la información, porque permite enfocar esfuerzos en los riesgos que pueden ser más críticos.

En la metodología Magerit se desarrollan cinco procesos principales que son:

- P1. La planificación
- P2. Identificación y valoración de activos
- P3. Identificación de amenazas y vulnerabilidades

- P4. Evaluación de riesgos
- P5. Tratamiento de riesgos

3.2.1. Proceso P1: Reconocimiento del entorno y planificación

3.2.1.1. **Actividad 1: Planificación.**

Esta etapa brindara las pautas necesarias para el desarrollo del análisis de riesgos como parte del DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO.

- **Estudio de Oportunidad.**

Esta actividad tiene como objetivo específico, realizar un diagnóstico del estado de seguridad en que se encuentran activos de información y tecnológicos más relevantes para esta investigación dentro del centro de estudios EMSSANAR CETEM de la ciudad de pasto, además de motivar a la alta dirección para implementar un SGSI.

- **Definición del Alcance y Objetivos del Proyecto**

Después de haber recibido el aval para la realización del proyecto, se definen los límites y el dominio de trabajo y los objetivos para desarrollar exitosamente el proyecto.
Los objetivos han sido planteados con el propósito de realizar un análisis de riesgos que permita el Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO27001:2013 en el centro de estudios EMSSANAR CETEM de la ciudad de pasto.

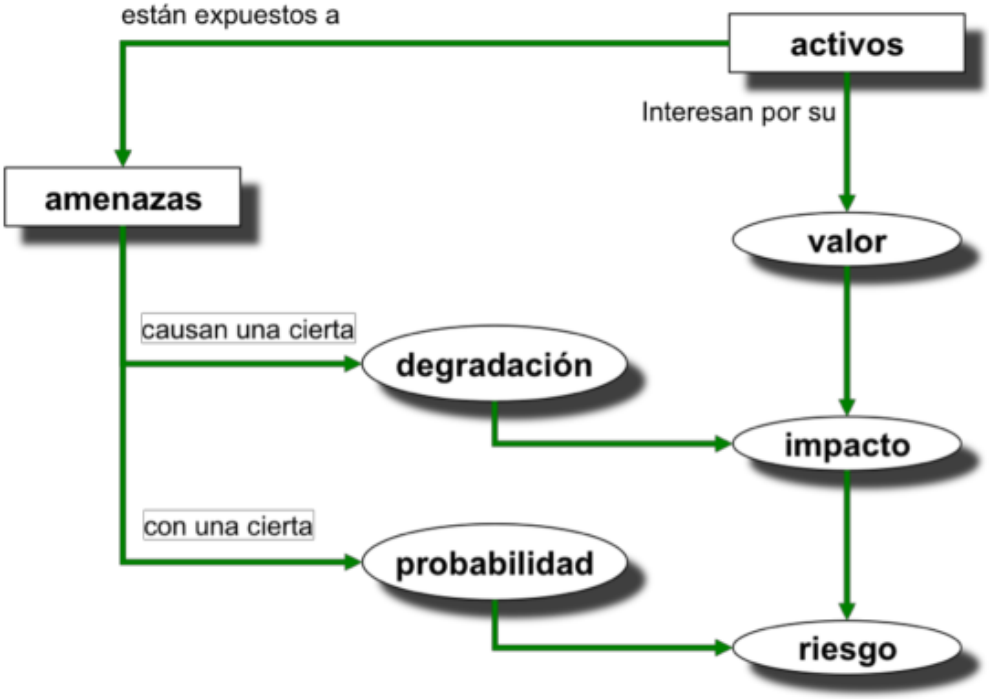
- **Planificación del Proyecto**

Se realiza un cronograma de actividades estableciendo el tiempo aproximado de dedicación por actividad que permita el desarrollo exitoso del proyecto.

- **Lanzamiento del Proyecto.**

Con el permiso de la Directora ejecutiva y colaboración del Auxiliar de Soporte y mantenimiento del Centro de Estudios EMSSANAR CETEM se inicia el proceso de análisis de riesgos y se adopta la técnica de observación directa para la recolección de la información siendo estas las más apropiadas, ya que se tiene la ventaja de que los integrantes del equipo de trabajo está directamente involucrado con los procesos y sistemas informáticos existentes en la institución.

Figura 7. Elementos del análisis de riesgos



Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro 1

Al igual que cualquier organización y/o empresa el Centro de Estudios EMSSANAR CETEM, está expuesta a múltiples riesgos razón por la cual debe considerar y dar importancia a los cambios o alteraciones que lleguen a afectar activos de información y tecnológicos evitando acciones negativas al normal funcionamiento.

En este punto es necesario aplicar una metodología que permita realizar un análisis de riesgos de manera sistemático y principalmente alineado a los estándares ISO en particular a la norma 27001, por esta razón se escogió la metodología de análisis de riesgos Magerit.

3.2.2. Proceso P2: Identificación y valoración de los Activos.

3.2.2.1. **Actividad 2: Clasificación de los Activos.**

Los activos presentes en Centro de Estudios EMSSANAR CETEM, son identificados y clasificados tomando como base el Libro II de la metodología MAGERIT versión 3 , en donde nos presenta el catálogo de elementos (Ver ANEXO B. TIPOS DE ACTIVOS SEGÚN MAGERIT):

Tabla 2. Activos esenciales [essential]

Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a la entidad**	**Nombre activo de acuerdo a la entidad**
[vr]	Datos vitales	1. [Inf_Prog_Academicos_ESS]	Información de los programas académicos que ofrece el Centro de Estudios.
[per]	Datos de Carácter Personal	2. [Inf_Academica_Alumnos_ESS]	Información académica de los alumnos de las diferentes promociones.

[per]	Datos de Carácter Personal	3. [Inf_ContableYfinanciera_ESS]	Información contable y financiera del Centro de Estudios.

Fuente: Esta investigación

Tabla 3. Datos / Información [D]

Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a la entidad**	**Nombre activo de acuerdo a la entidad**
[files]	Archivos	4. [Arc_Prog_Academicos_d]	Archivos con información de los programas académicos que ofrece el Centro de Estudios.
[files]	Archivos	5. [Arc_Calificaciones_d]	Archivos con información académica de los alumnos de las diferentes promociones.
[files]	Archivos	6. [Arc_Proyectos_alumnos_d]	Archivos con información contable y financiera institucional.
[files]	Archivos	7. [Arc_Reportes_e_informes_d]	Archivos con reportes e informes institucionales.
[password]	Credenciales	8. [Passwords_d]	Claves de acceso a equipos de oficina y recursos tecnológicos
[backup]	Copias de respaldo	9. [ImageSO_Bk_d]	Copia de respaldo de los sistemas operativos tanto de las oficinas como de las aulas de informática.

Fuente: Esta investigación

Tabla 4. Claves criptográficas [K]

Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a la entidad**	**Nombre activo de acuerdo a la entidad**
[vr]	Datos vitales	10. [Firma_digital_docs_k]	Utilizada para firmar los documentos institucionales.

[per]	Datos de Carácter Personal	11. [Clave_Bancaria_k]	Utilizada para realizar los pagos y transacciones bancarias.

Tabla 5. Inventario de servicios [S]

Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a la entidad**	**Nombre activo de acuerdo a la entidad**
[www]	World wide web	12. [Internet_S]	Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.

Fuente: Esta investigación

Tabla 6. Software - Aplicaciones informáticas [Sw]

Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a la entidad**	**Nombre activo de acuerdo a la entidad**
[prp]	Desarrollo propio	13. [SED_Sw]	Sistema evaluación docente
[prp]	Desarrollo propio	14. [SCAA_Sw]	Sistema de Control de Asistencia Administrativos
[sub]	Desarrollo a medida (subcontratado)	15. [SE_Suite_Sw]	SE Suite
[sub]	Desarrollo a medida (subcontratado)	16. [Q10_Academico_Sw]	Q10 Académico
[sub]	Desarrollo a medida (subcontratado)	17. [Superportsoft_Sw]	Sistema de inventario de equipos
[sub]	Desarrollo a medida (subcontratado)	18. [SIGE_sw]	Sistema de Información de Gestión Documental
[browser]	Navegador web	19. [Browser_sw]	Navegador Web
[Oficce]	Ofimática	20. [Microsoft_Oficce_sw]	Microsoft Office, 2007, 2013, 2016
[av]	Antivirus	21. [ESET_Antivirus_sw]	ESET ENDPOINT ANTIVIRUS 5 con

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
			actualizaciones automáticas.
[os]	Sistema operativo	22. [Windows_OS_aulas__sw]	Sistema operativo Windows XP, 7 y 8 para docentes y estudiantes, en su versión professional con actualizaciones automáticas activadas.
[os]	Sistema operativo	23. [Windows_OS_oficinas_sw]	Sistema operativo Windows 7 y 8 para administrativos, en su versión professional con actualizaciones automáticas activadas.

Fuente: Esta investigación

Tabla 7. Equipos informáticos [Hw]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[mid]	Equipos medios	24. [Evaluacion_mid_hw]	Servidor de evaluación Docente
[mid]	Equipos medios	25. [Asistencia_mid_hw]	Servidor de Control de Asistencia Administrativos
[pc]	Informática personal	26. [oficina_PC_hw]	Equipos de Oficina
[pc]	Informática personal	27. [Aulas_PC_hw]	Equipos de Aulas de clase
[mobile]	Equipos que son fácilmente transportados	28. [Equipos_Movile_hw]	Laptops y celulares de Administrativos, docentes, estudiantes y visitantes.
[print]	Equipos de impresion	29. [local_print_hw]	Impresoras

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[hub] concentradores	Hub	30. [Hub_hw]	Hub
[switch] conmutadores	Switch	31. [Switch_hw]	Switch
[router]	Enrutador	32. [Router_ISP_hw]	Router de Internet Proveedor de Servicios de Internet.
[wap]	Punto de acceso inalámbrico	33. [wifi_Ap_hw]	Red Inalámbrica

Fuente: Esta investigación

Tabla 8. Redes de comunicaciones [COM]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[LAN]	Red local	34. [Intranet_com]	Intranet
[LAN]	Red local	35. [Extranet_com]	Comunicación a los sistemas externos a través de internet

Fuente: Esta investigación

Tabla 9. Equipos Auxiliares [Aux]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[wire]	Cableado	36. [CAB_RED_aux]	Cableado de Red
[ups]	Sistemas de Alimentación ininterrumpida	37. [Computadores_ups_aux]	UPS computadores
[suplly]	Suministros Esenciales	38. [Esenciales_aux]	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.
[Furniture]	Mobiliario	39. [M_Mobiliario_aux]	Mobiliario: Estantes,

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
			armarios, escritorios, archivadores, etc.
[safe]	Cajas fuertes	40. [caja_fuerte]	Cajas fuertes

Fuente: Esta investigación

Tabla 10. Instalaciones [L]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[building]	Edificio	41. [E_entidad-l]	Instalación física del Centro de Estudios EMSSANAR CETEM
[GAB]	Gabinete de Red	42. [Gabinete-l]	Gabinete de Red

Fuente: Esta investigación

Tabla 11. Personal [P]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[ue]	usuarios externos	43. [Usuarios_externos_p]	Visitantes
[ui]	Usuarios internos	44. [Usuarios_int_Adm_p]	Administrativos,
		45. [Usuarios_int-Doc_p]	Docentes
		46. [Usuarios_int_Est_p]	Estudiantes.
[op]	Operadores	47. [Auxiliar_op_p]	Auxiliar de Soporte y mantenimiento
[op]	Operadores	48. [Soporte_op_p]	Ingeniero de soporte EMSSANAR

Fuente: Esta investigación

Tabla 12. Soportes de Información _almacenamiento electrónico y no electrónico [MEDIA]

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[printed]	Material impreso	49. [Doc_Prog_Academicos]	Carpetas con información de los programas académicos que ofrece el Centro de Estudios.
		50. [Doc_Academica_Alumnos]	Carpetas con información académica de los alumnos de las diferentes promociones.
		51. [Doc_Proyectos_alumnos]	Documentos en físico de los proyectos de los alumnos graduados
		52. [Doc_Hv_Docente]	Hojas de vida en físico de los docentes que han trabajado en la institución hasta la fecha.
		53. [Doc_Reportes_e_informes]	Reportes e informes contables y financieros institucionales en físico.
[NO_printed]	Material en digital	54. [Dig_Reportes_e_informes]	Reportes e informes contables y financieros institucionales en físico.
		55. [Dig_calif_alumnos]	Archivos de Excel de las calificaciones promociones antiguas.

Fuente: Esta investigación

Tabla 13. Resumen de activos de información

TIPO	NOMBRE DEL ACTIVO
ACTIVOS ESENCIALES [ESSENTIAL]	1. [Inf_Prog_Academicos_ESS] - Información de los programas académicos que ofrece el Centro de Estudios. 2. [Inf_Academica_Alumnos_ESS] - Información

TIPO	NOMBRE DEL ACTIVO
	académica de los alumnos de las diferentes promociones. 3. [Inf_ContableYfinanciera_ESS] - Información contable y financiera del Centro de Estudios.
DATOS / INFORMACIÓN [D]	4. [Arc_Prog_Academicos_d] - Archivos con información de los programas académicos que ofrece el Centro de Estudios. 5. [Arc_Calificaciones_d] - Archivos con información académica de los alumnos de las diferentes promociones. 6. [Arc_Proyectos_alumnos_d] - Archivos con información contable y financiera institucional. 7. [Arc_Reportes_e_informes_d] - Archivos con reportes e informes institucionales. 8. [Passwords_d] - Claves de acceso a equipos de oficina y recursos tecnológicos 9. [ImageSO_Bk_d] - Copia de respaldo de los sistemas operativos tanto de las oficinas como de las aulas de informática.
CLAVES CRIPTOGRÁFICAS [K]	10. [Firma_digital_docs_k] - Utilizada para firmar los documentos institucionales. 11. [Clave_Bancaria_k] - Utilizada para realizar los pagos y transacciones bancarias.
SERVICIOS [S]	12. [Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.
SOFTWARE - APLICACIONES INFORMATICAS [SW]	13. [SED_Sw] - Sistema evaluación docente 14. [SCAA_Sw] - Sistema de Control de Asistencia Administrativo 15. [SE_Suite_Sw] - SoftExpert Excellence (Suite SE Suite) 16. [Q10_Academico_Sw] - Gestión educativa de los procesos académicos y administrativos. 17. [Superportsoft_Sw] - Sistema de inventario de equipos 18. [SIGE_Sw] - Sistema de Información de Gestión

TIPO	NOMBRE DEL ACTIVO
	Documental 19. [Browser_sw] - Navegador Web 20. [Microsoft_Oficce_sw] – Microsoft Office, 2007, 2013, 2016 21. [ESET_Antivirus_sw] - ESET ENDPOINT ANTIVIRUS 5 con actualizaciones automaticas. 22. [Windows_OS_aulas_sw] - Sistema operativo Windows XP, 7 y 8 para docentes y estudiantes, en su versión professional con actualizaciones automáticas activadas. 23. [Windows_OS_oficinas_sw] - Sistema operativo Windows 7 y 8 para administrativos, en su versión professional con actualizaciones automáticas activadas.
EQUIPAMIENTO INFORMÁTICO [HW]	24. [Evaluacion_mid_hw] - Servidor de evaluación 25. [Asistencia_ mid_hw] - Servidor de Control de Asistencia Administrativos 26. [Oficina_PC_hw] - Equipos de Oficina 27. [Aulas_PC_hw] - Equipos de Aulas de clase 28. [Equipos_Movile_hw] - Laptops y celulares de Administrativos, docentes, estudiantes y visitantes. 29. [local_print_hw] - Impresoras 30. [Hub_hw] - Hub 31. [Switch_hw] - Switch 32. [Router_ISP_hw] - Router de Internet Proveedor de Servicios de Internet. 33. [Wifi_Ap_hw] - Red Inalámbrica
REDES DE COMUNICACIONES [COM]	34. [Intranet_com] – Intranet 35. [Extranet_com] – Comunicación a los sistemas externos a través de internet
EQUIPAMIENTO AUXILIAR [AUX]	36. [CAB_RED_aux] - Cableado de Red 37. [Computadores_ups_aux] - Sistemas de Alimentación ininterrumpida. 38. [Esenciales_aux] - Suministros Esenciales . 39. [M_Mobiliario_aux] - Mobiliario

TIPO	NOMBRE DEL ACTIVO
	40. [caja_fuerte_aux] - Cajas fuertes
INSTALACIONES [L]	41. [E_entidad_l] - Instalación física del Centro de Estudios EMSSANAR CETEM 42. [Gabinete_l] – Gabinete de Red
PERSONAL [P]	43. [Usuarios_externos_p] - Visitantes 44. [Usuarios_int_Adm_p]– Administrativos 45. [Usuarios_int-Doc_p] – Docentes 46. [Usuarios_int_Est_p]– Estudiantes. 47. [Auxiliar_op_p] - Auxiliar de Soporte y mantenimiento 48. [Soporte_op_p] – Ingeniero de soporte EMSSANAR
SOPORTES DE INFORMACIÓN ELECTRONICOS Y NO ELECTRONICOS [MEDIA]	49. [Doc_Prog_Academicos] - Carpetas con información de los programas académicos que ofrece el Centro de Estudios. 50. [Doc_Academica_Alumnos] - Carpetas con información académica de los alumnos de las diferentes promociones. 51. [Doc_Proyectos_alumnos] - Documentos en físico de los proyectos de los alumnos graduados 52. [Doc_Hv_Docente] - Hojas de vida en físico de los docentes que han trabajado en la institución hasta la fecha. 53. [Doc_Reportes_e_informes] - Reportes e informes contables y financieros institucionales en físico. 54. [Dig_Reportes_e_informes] - Reportes e informes contables y financieros institucionales en físico. 55. [Dig_calif_alumnos] - Archivos de Excel de las calificaciones promociones antiguas.

Fuente: Esta investigación

3.2.2.2. **Actividad 3: Valoración cualitativa de los Activos y selección de activos más relevantes.**

Teniendo en cuenta que todos los activos no tienen la misma relevancia e importancia para la entidad, y que cada uno de estos en caso de ser atacado o sufrir un incidente genera un impacto diferente en la entidad, se procede a realizar

una valoración cualitativa teniendo en cuenta la escala de valoración de activos propuesta en MAGERIT V3 (Ver Tabla 4) basada en dimensiones de seguridad como lo son:

- [C] confidencialidad de la Información.
- [I] integridad de los datos
- [D] disponibilidad
- [A] Autenticidad
- [T] trazabilidad

Tabla 14. Escala de Valoración de activos

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

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro 3

Tabla 15. Valoración de Activos esenciales

ID	ACTIVOS ESENCIALES [ESSENTIAL]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
1	[Inf_Prog_Academicos_ESS] - Información de los programas académicos que ofrece el Centro de Estudios.	1	C	S	A	A	4	Auxiliar Soporte y mantenimiento
2	[Inf_Academica_Alumnos_ESS] - Información académica de los alumnos de las diferentes	1	C	S	A	A	4	Auxiliar Administrativo Académico

	promociones.							
3	[Inf_ContableYfinanciera_ESS] - Información contable y financiera del Centro de Estudios.	1	C	S	MA	MA	5	Auxiliar Administrativo Financiero

Fuente: Esta investigación

Tabla 16. Valoración de Datos e Información

ID	DATOS / INFORMACIÓN [D]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
4	[Arc_Prog_Academicos_d] - Archivos con información de los programas académicos que ofrece el Centro de Estudios.	1	I	S	B	M	3	Auxiliar Administrativo Académico
5	[Arc_Calificaciones_d] - Archivos con información académica de los alumnos de las diferentes promociones.	1	I	S	B	M	3	Auxiliar Administrativo Académico
6	[Arc_Proyectos_alumnos_d] - Archivos con información contable y financiera institucional.	1	I	B	B	B	2	Auxiliar Administrativo Académico
7	[Arc_Reportes_e_informes_d] - Archivos con reportes e informes institucionales.	1	I	N	B	B	2	Auxiliar Administrativo Financiero
8	[Passwords_d] - Claves de acceso a equipos de oficina y recursos tecnológicos	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento
9	[ImageSO_Bk_d] - Copia de respaldo de los sistemas operativos tanto de las oficinas como de las aulas de informática.	1	I	B	A	M	3	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 17. Valoración de Claves Criptográficas

ID	CLAVES CRIPTOGRÁFICAS [K]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
10	[Firma_digital_docs_k] - Utilizada para firmar los documentos institucionales.	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento
11	[Clave_Bancaria_k] - Utilizada para realizar los pagos y transacciones bancarias.	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 18. Valoración de Servicios

ID	SERVICIOS [S]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
12	[Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.	1	I	N	MA	A	4	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 19. Valoración de Aplicaciones Informáticas

ID	SOFTWARE - APLICACIONES INFORMATICAS [SW]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
13	[SED_Sw] - Sistema evaluación docente	1	P	N	MB	B	2	Auxiliar Soporte y mantenimiento
14	[SCAA_Sw] - Sistema de Control de Asistencia Administrativo	1	I	N	A	M	3	Auxiliar Soporte y mantenimiento

ID	SOFTWARE - APLICACIONES INFORMATICAS [SW]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
15	[SE_Suite_Sw] - SoftExpert Excellence (Suite SE Suite)	1	C	S	MA	MA	5	Empresa Prestadora del Servicio
16	[Q10_Academico_Sw] - Gestión educativa de los procesos académicos y administrativos.	1	C	S	MA	MA	5	Empresa Prestadora del Servicio
17	[Superportsoft_Sw] - Sistema de inventario de equipos	1	I	B	MB	B	2	Empresa Prestadora del Servicio
18	[SIGE_Sw] - Sistema de Información de Gestión Documental	1	I	S	A	M	3	Empresa Externa
19	[Navegadores_web_sw] - Navegadores Web	2	P	B	B	MB	1	Auxiliar Soporte y mantenimiento
20	[Microsoft_Oficce_sw] – Microsoft Office, 2007, 2013, 2016	1	P	B	B	MB	1	Auxiliar Soporte y mantenimiento
21	[ESET_Antivirus_sw] - ESET ENDPOINT ANTIVIRUS 5 con actualizaciones automaticas.	1	P	B	MA	B	2	Auxiliar Soporte y mantenimiento
22	[Windows_OS_aulas_sw]- Sistema operativo Windows XP, 7 y 8 para docentes y estudiantes, en su versión professional con actualizaciones automáticas activadas.	3	P	B	MA	B	2	Auxiliar Soporte y mantenimiento

ID	SOFTWARE - APLICACIONES INFORMATICAS [SW]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
23	[Windows_OS_oficinas_sw] - Sistema operativo Windows 7 y 8 para administrativos, en su versión professional con actualizaciones automáticas activadas.	1	I	N	MA	A	4	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 20. Valoración de Equipamiento Informático

ID	EQUIPAMIENTO INFORMÁTICO [HW]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
24	[Evaluacion_mid_hw] - Servidor de evaluación	1	I	N	A	M	3	Auxiliar Soporte y mantenimiento
25	[Asistencia_ mid_hw] - Servidor de Control de Asistencia Administrativos	1	I	N	MA	A	4	Auxiliar Soporte y mantenimiento
26	[Oficina_PC_hw] - Equipos de Oficina	5	I	N	MA	A	4	Auxiliar Soporte y mantenimiento
27	[Aulas_PC_hw] - Equipos de Aulas de clase	80	P	B	MB	B	2	Auxiliar Soporte y mantenimiento
28	[Equipos_Movile_hw] - Laptops y celulares de Administrativos, docentes, estudiantes y visitantes.	20	P	N	MB	B	2	Propios Usuarios
29	[local_print_hw] - Impresoras	2	I	N	A	M	3	Auxiliar Soporte y mantenimiento

ID	EQUIPAMIENTO INFORMÁTICO [HW]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
30	[Hub_hw] - Hub	3	I	N	MA	A	4	Auxiliar Soporte y mantenimiento
31	[Switch_hw] - Switch	4	I	N	MA	A	4	Auxiliar Soporte y mantenimiento
32	[Router_ISP_hw] - Router de Internet Proveedor de Servicios de Internet.	1	I	N	MA	A	4	Empresa Prestadora del Servicio
33	[Wifi_Ap_hw] - Red Inalámbrica	5	I	N	MA	A	4	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 21. Valoración de Redes de Comunicaciones

ID	REDES DE COMUNICACIONES [COM]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
34	[Intranet_com] – Intranet	1	I	S	MA	MA	5	Auxiliar Soporte y mantenimiento
35	[Extranet_com] – Comunicación a los sistemas externos a través de internet	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 22. Evaluación de equipamiento auxiliar

ID	EQUIPAMIENTO AUXILIAR [AUX]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	

ID	EQUIPAMIENTO AUXILIAR [AUX]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
36	[CAB_RED_aux] - Cableado de Red	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento
37	[Computadores_ups_aux] - Sistemas de Alimentación ininterrumpida.	1	C	N	A	M	3	Auxiliar Soporte y mantenimiento
38	[Esenciales_aux] - Suministros Esenciales	1	I	B	MB	B	2	Auxiliar Servicios Generales
39	[M_Mobiliario_aux] - Mobiliario	1	I	B	MB	B	2	Auxiliar Servicios Generales
40	[caja_fuerte_aux] - Cajas fuertes	1	C	S	A	A	4	Directora Ejecutiva

Fuente: Esta investigación

Tabla 23. . Valoración de Instalaciones

ID	INSTALACIONES [L]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
41	[E_entidad_l] - Instalación física del Centro de Estudios EMSSANAR CETEM	1	P	N	A	B	2	Auxiliar Soporte y mantenimiento
42	[Gabinete_l] – Gabinete de Red	1	C	S	MA	MA	5	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

Tabla 24. Valoración de personal

ID	PERSONAL [P]	Cant	Dimensión	Activo	Custodio

			C	I	D	Nivel	Valor	
43	[Usuarios_externos_p] - Visitantes	30	P	B	MB	B	2	Auxiliar Servicios Generales
44	[Usuarios_int_Adm_p]– Administrativos	5	I	N	MA	A	4	Directora Ejecutiva
45	[Usuarios_int-Doc_p] – Docentes	40	I	N	MB	B	2	Directora Ejecutiva
46	[Usuarios_int_Est_p]– Estudiantes.	400	I	N	MB	B	2	Directora Ejecutiva
47	[Auxiliar_op_p] - Auxiliar de Soporte y mantenimiento	1	I	N	MA	A	4	Directora Ejecutiva
48	[Soporte_op_p] – Ingeniero de soporte EMSSANAR	1	I	N	B	B	2	Directora Ejecutiva

Fuente: Esta investigación

Tabla 25. Valoración de Información Electrónica

ID	SOPORTES DE INFORMACIÓN ELECTRONICA [MEDIA]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
49	[Arc_Prog_Academicos] - Carpetas con información de los programas académicos que ofrece el Centro de Estudios.	1	I	N	B	B	2	Auxiliar Administrativo Académico
50	[Arc_Academica_Alumnos] - Carpetas con información académica de los alumnos de las diferentes promociones.	1	I	S	B	M	3	Auxiliar Administrativo Académico
51	[Arc_Proyectos_alumnos] - Documentos en físico de los proyectos de los alumnos graduados	1	I	B	B	B	2	Auxiliar Administrativo Académico

ID	SOPORTES DE INFORMACIÓN ELECTRONICA [MEDIA]	Cant	Dimensión			Activo		Custodio
			C	I	D	Nivel	Valor	
52	[Arc_Hv_Docente] - Hojas de vida en físico de los docentes que han traBdo en la institución hasta la fecha.	1	P	B	B	MB	1	Auxiliar Administrativo Financiero
53	[Arc_Reportes_e_informes] - Reportes e informes contables y financieros institucionales en físico.	1	I	S	B	M	3	Auxiliar Administrativo Financiero

Fuente: Esta investigación

En esta valoración de activos se puede observar el valor que tiene cada activo para el Centro de Estudios EMSSANAR. Teniendo en cuenta que el objetivo es diseñar un sistema de gestión de seguridad informática bajo la norma ISO27001:2013 para mejorar la seguridad de la red de datos se han seleccionado los activos que tienen mayor valor y están directamente relacionados con esta investigación como se observa en la tabla 26.

Tabla 26. Activos más relevantes para esta investigación

TIPO DE ACTIVO	Nombre del Activo	Activo		Custodio
		Nivel	Valor	
SERVICIOS [S]	[Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.	A	4	Auxiliar Soporte y mantenimiento
EQUIPAMIENTO INFORMÁTICO [HW]	[Wifi_Ap_hw] - Red Inalámbrica	A	4	Auxiliar Soporte y mantenimiento
REDES DE COMUNICACIONES [COM]	[Intranet_com] – Intranet	MA	5	Auxiliar Soporte y mantenimiento

TIPO DE ACTIVO	Nombre del Activo	Activo		Custodio
		Nivel	Valor	
REDES DE COMUNICACIONES [COM]	[Extranet_com] – Comunicación a los sistemas externos a través de internet	MA	5	Auxiliar Soporte y mantenimiento
EQUIPAMIENTO AUXILIAR [AUX]	[CAB_RED_aux] - Cableado de Red	MA	5	Auxiliar Soporte y mantenimiento
INSTALACIONES [L]	[Gabinete_l] – Gabinete de Red	MA	5	Auxiliar Soporte y mantenimiento

Fuente: Esta investigación

3.2.3. Proceso P3: Identificación de amenazas y vulnerabilidades

3.2.3.1. **Actividad 4: Identificación de amenazas.**

Una vez seleccionados en la Actividad A2.1.1 los activos más relevantes para esta investigación, procedemos a determinar la degradación del activo; proceso que consiste en evaluar el valor que pierde el activo (en porcentaje) en caso que se materialice una amenaza.

Estas Amenazas se han tomado del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0.

Para el desarrollo de esta actividad es necesario tener presente los rangos dados en los siguientes cuadros tanto de frecuencia como de degradación.

Tabla 27. Probabilidad de ocurrencia

Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro 3

Tabla 28. Degradación del valor

Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% – 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro 3

Tabla 29. Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.

Activo TI	[Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	SERVICIOS [S]

ID	**Amenaza**
[E.19]	Fugas de información
[E.24]	Caída del sistema por agotamiento de recursos
[A.5]	Suplantación de la identidad del usuario
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.15]	Modificación deliberada de la información
[A.18]	Destrucción de información
[A.19]	Revelación de información
[A.24]	Denegación de servicio

Fuente: Esta investigación

Tabla 30. Red Inalámbrica

Activo TI	33. [Wifi_Ap_hw] - Red Inalámbrica

Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	EQUIPAMIENTO INFORMÁTICO [HW]
ID	**Amenaza**
[I.4]	Contaminación electromagnética.
[I.5]	Avería de origen físico o lógico.
[I.6]	Corte del suministro eléctrico
[I.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador
[E.24]	Caída del sistema por agotamiento de recursos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.24]	Denegación de servicio

Fuente: Esta investigación

Tabla 31. Intranet

Activo TI	34. [Intranet_com] – Intranet
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	REDES DE COMUNICACIONES [COM]
ID	**Amenaza**
[I.8]	Fallo de servicios de comunicaciones
[E.2]	Errores del administrador
[E.9]	Errores de [re-]encaminamiento
[E.19]	Fugas de información
[E.24]	Caída del sistema por agotamiento de recursos
[A.5]	Suplantación de la identidad del usuario
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.10]	Alteración de secuencia
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.14]	Interceptación de información (escucha)
[A.15]	Modificación deliberada de la información
[A.18]	Destrucción de información
[A.19]	Revelación de información
[A.24]	Denegación de servicio

Fuente: Esta investigación

Tabla 32. Comunicación a los sistemas externos a través de internet

Activo TI	35. [Extranet_com] – Comunicación a los sistemas externos a través de internet
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	REDES DE COMUNICACIONES [COM]
ID	**Amenaza**
[I.8]	Fallo de servicios de comunicaciones
[E.2]	Errores del administrador
[E.9]	Errores de [re-]encaminamiento
[E.15]	Alteración accidental de la información
[E.18]	Destrucción de información
[E.19]	Fugas de información
[E.24]	Caída del sistema por agotamiento de recursos
[A.5]	Suplantación de la identidad del usuario
[A.6]	Abuso de privilegios de acceso
[A.9]	Manipulación de los registros de actividad (log)
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.14]	Interceptación de información (escucha)
[A.15]	Modificación deliberada de la información
[A.18]	Destrucción de información
[A.19]	Revelación de información
[A.24]	Denegación de servicio

Fuente: Esta investigación

Tabla 33. Cableado de Red

Activo TI	36. [CAB_RED_aux] - Cableado de Red
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	EQUIPAMIENTO AUXILIAR [AUX]
ID	**Amenaza**
[I.4]	Contaminación electromagnética.
[I.5]	Avería de origen físico o lógico.
[I.6]	Corte del suministro eléctrico
[I.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador

Activo TI	36. [CAB_RED_aux] - Cableado de Red
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	EQUIPAMIENTO AUXILIAR [AUX]
ID	**Amenaza**
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)
[A.11]	Acceso no autorizado

Fuente: Esta investigación

Tabla 34. Gabinete de Red

Activo TI	42. [Gabinete_l] – Gabinete de Red
Administrador	Auxiliar de Soporte y mantenimiento
Tipo de Activo	INSTALACIONES [L]
ID	**Amenaza**
[E.15]	Alteración accidental de la información
[E.18]	Destrucción de información
[E.19]	Fugas de información
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.15]	Modificación deliberada de la información
[A.18]	Destrucción de información
[A.19]	Revelación de información
[A.27]	Ocupación enemiga

Fuente: Esta investigación

3.2.3.2. **Actividad 5: Identificación de vulnerabilidades.**

Se realizó principalmente a través de inspección visual a los activos de información y hacking ético.

- **Inspección visual de los activos de información.**

El acompañamiento del Auxiliar de Soporte y mantenimiento enriqueció en gran medida la inspección visual, ya que a medida se recorría las instalaciones el realizaba una descripción de todos los dispositivos y situaciones encontradas.
Se lograron identificar varios lugares y activos críticos, como lo son.

Sala de Servidores

Figura 8. Servidor de evaluación Docente

Fuente: Esta investigación

Como se observa en la figura 8 el Servidor de Evaluación Docente, se encuentra en una mesa de madera, en caso de incendio este se puede destruir fácilmente. Cuenta con un extintor Solkaflam (especializado para equipos de cómputo en caso de incendio) en la parte de afuera de la oficina del Auxiliar de Soporte y Mantenimiento donde se encuentra ubicado, como se observa en la figura 9.

Figura 9. Oficina Auxiliar de Soporte y mantenimiento

Fuente: Esta investigación

La puerta de acceso al Servidor de Evaluación Docente, no cuenta con chapas que suficientemente seguras como se observa en la figura 10.

Figura 10. Puerta acceso Servidor de Evaluación Docente

Fuente: Esta investigación

El Servidor de Control de Asistencia Administrativos se encuentra en el cuarto de aseo como se observa en la Figura 10.

Figura 11. Servidor de Control de Asistencia Administrativos

Fuente: Esta investigación

La puerta de acceso al Servidor de Control de Asistencia Administrativos, no cuenta con chapas que suficientemente seguras como se observa en la figura 10.

Figura 12. Puerta acceso Servidor de Control de Asistencia Administrativos

Fuente: Esta investigación

Se puede concluir que:

- Los dos servidores se encuentran ubicados en diferentes plantas del edificio.
- Los dos sitios no cuentan con un sistema de cámaras de seguridad.
- Los dos sitios poseen en la puerta principal o de acceso cerraduras normales.
- Las llaves de acceso son custodiadas por la Auxiliar de Servicios Generales y el Auxiliar de Soporte y mantenimiento respectivamente.
- Las llaves de acceso son fácilmente transferibles a personal interno y externo sin autorización.

Sistema de Alimentación Ininterrumpida

En la actualidad todo el edificio se encuentra conectado a sistema de alimentación ininterrumpida (ver Figura 12), es decir, en el momento que se presente un apagón eléctrico el sistema proporcionara energía eléctrica tanto a un servidor como a un equipo del aula de informática sin distinguir el nivel de importancia.

Figura 13. Sistema de Alimentación Ininterrumpida

Fuente: Esta investigación

Como se puede observar en la figura 13 el servidor se encuentra en la parte inferior de las gradas al segundo piso.

Figura 14. Ubicación UPS

Fuente: Esta investigación

Armario de comunicaciones

Actualmente el armario de comunicaciones cuenta con sistemas de control ambientales al interior del salón y un extintor Solkaflam (especializado para equipos de cómputo en caso de incendio) en la entrada. La cerradura del armario de comunicaciones se encuentra en mal estado lo que posibilita que cualquier persona pueda manipular el cableado o cualquier dispositivo de red que este en su interior como se observa en la Figura 14.

Figura 15. Ubicación armario de telecomunicaciones

Fuente: Esta investigación

En la Figura 15 se puede observar que:

- El cableado de red que interconecta los dispositivos de red no presenta ningún tipo de etiquetado aunque se muestra organizado.
- Los dispositivos están conectados al Sistema de Alimentación Ininterrumpida y no presenta un panel de control eléctrico externo.
- El armario de telecomunicaciones aunque tiene cerradura esta forzado y permite ser abierto con cualquier llave.

Figura 16. Armario de telecomunicaciones

Fuente: Esta investigación

Figura 17. Condiciones del área de ubicación de Servidores

Elemento con los que debe contar	**Si**	**No**
Altura de 2,50 metros en el cuarto de servidores se cumple.	X	
Ubicado lejos de fuentes electromagnéticas (Antenas, máquinas eléctricas, radar, iluminación, microondas, aparatos electrónicos).	X	
Esta cerca de Fuentes de inundación.		X
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	X	
Las puertas tienen retardante para el fuego.		X
Iluminación adecuada.		X
Polvo en el medio ambiente.	X	
Cuenta con un equipo contra incendios al entrar a la sala.		X
La sala es resistente al fuego.		X
Normas comunes de conservación y limpieza.		X
Se utilizan paneles de obturación para los cables.		X

Existe cableado bajo el piso elevado que no se utiliza y puede eliminarse.		X
Cuenta con aisladores (Ejemplo espuma) los racks.		X
Cuenta con un sistema de marquillas en los equipo dentro del cuarto.		X
Equipos de respaldo para todos los elementos que interviene en el funcionamiento.		X
Accesibilidad para el suministro de equipos.	X	
Seguridad en el área	**Si**	**No**
Al Ingresar al Área de Ubicación de Servidores tiene un sistema de seguridad que le permita saber quién ingreso.		X
Cuenta con un sistema de seguridad de cámara de vigilancia.		X
Tiene sistema de alarma contra incendios.	X	
Tienen el sistema de alarmas de control de temperatura y humedad.		X
Aire acondicionado	**Si**	**No**
Ventiladores en la parte superior de los racks de los servidores.		X
Existen fugas en el piso elevado o en el sistema de suministro de aire.		X
Los puntos de referencia de los aires acondicionados son apropiados.		X
Climatización para la sala de servidores y UPS.		X
Controles de temperatura.		X
Cuenta con des humidificación y ventilación.		X
La configuración del sistema de retorno de aire es apropiada.		X
Tuberías de suministro y retorno invertidas.		X
Válvulas defectuosas.		X
Hay sistemas de enfriamiento que no fueron puestos en marcha.		X

Fuente: Esta investigación

- **Ethical hacking y análisis de vulnerabilidades.**

El propósito de esta fase es encontrar vulnerabilidades en cuanto a configuración y administración de los activos de información relacionadas con la parte lógica de la red de datos del Centro de estudios EMSSANAR CETEM a través de un test de penetración utilizando herramientas incorporadas en el sistema operativo Windows y otras integradas en sistema operativo Kali Linux (Versión 2016.2). .

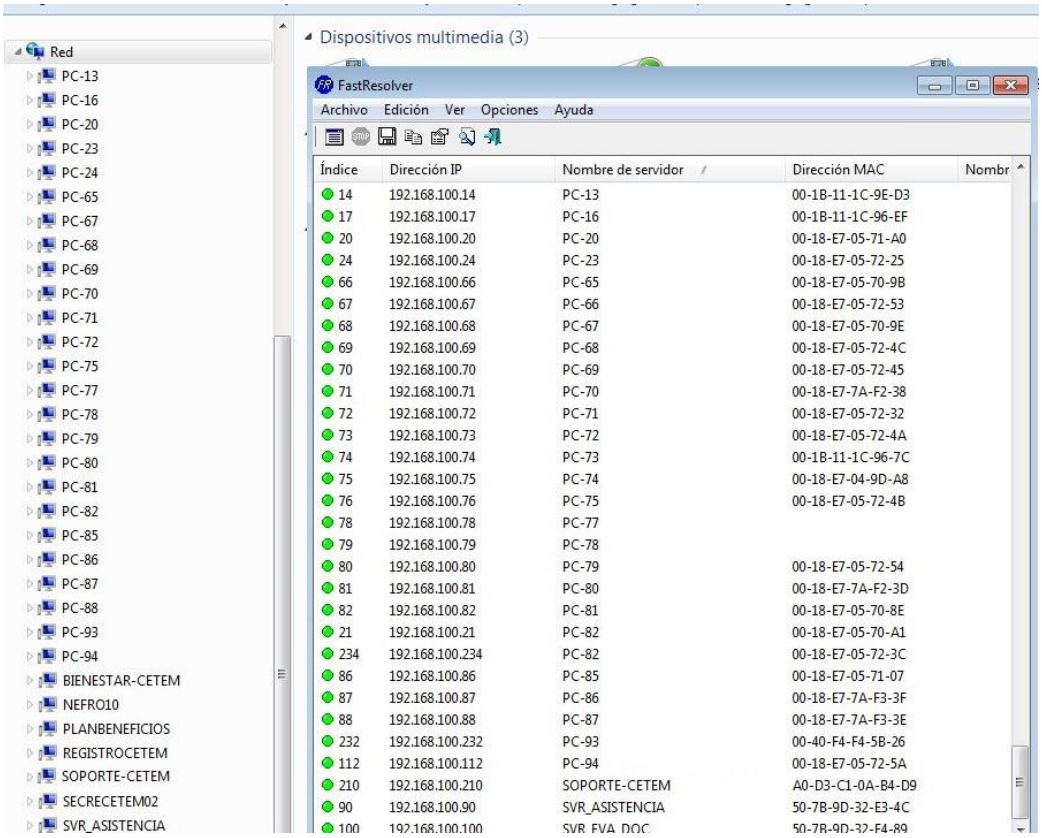
Se hace hincapié que la prueba de penetración descrita en este documento es interna de tipo Blue Teaming, es decir que se realiza con el conocimiento del personal del AREA DE REDES Y SISTEMAS, para evitar que los posibles incidentes generen pánico o fallas en la continuidad del servicio.

Teniendo en cuenta que todo proceso de Hacking Ético se divide en 5 pasos que son, reconocimiento, escaneo, obtener acceso, mantener el acceso, cubrir las huellas, se realizaran los 3 primeros que para el caso servirán como evidencia de vulnerabilidades encontrados.

Paso 1. Reconocimiento

En la figura 17 se puede observar como al realizar una simple verificación de máquinas activas sobre el rango de red 192.168.100.1 a 192.168.100.255 podemos encontrar que los equipos de las aulas de informatica se encuentran en la misma red que la de los Funcionarios.

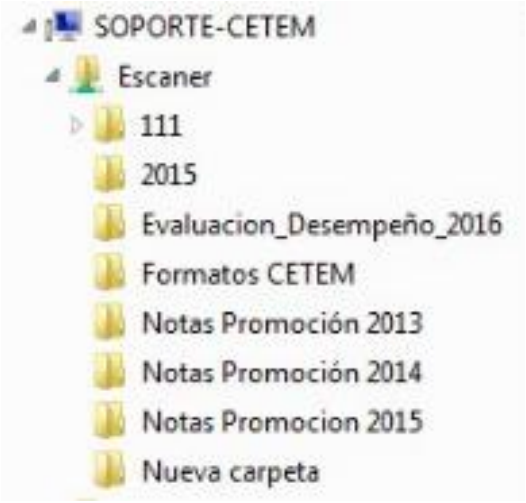
Figura 18. Equipos del Aula de Informática y de Funcionarios



Fuente: Esta investigación

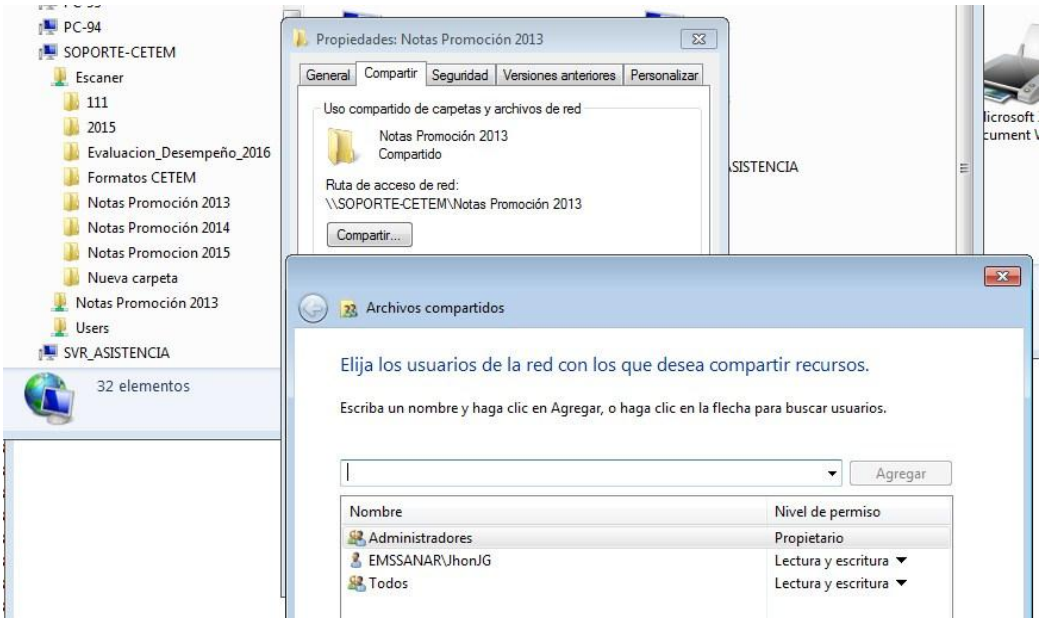
Se puede apreciar en figura 18 que al acceder a la red de datos se puede tener privilegio de acceso a directorios e impresoras compartidos de los funcionarios del CETEM y en la figura 19 que existe mucha informacion que solo le concierne a la institucion y no cuenta con los devidos permisos de acceso, modificacion, eliminacion, ejecucion.

Figura 19. Directorios e impresoras compartidas



Fuente: Esta investigación

Figura 20. Permisos de los directorios compartidos

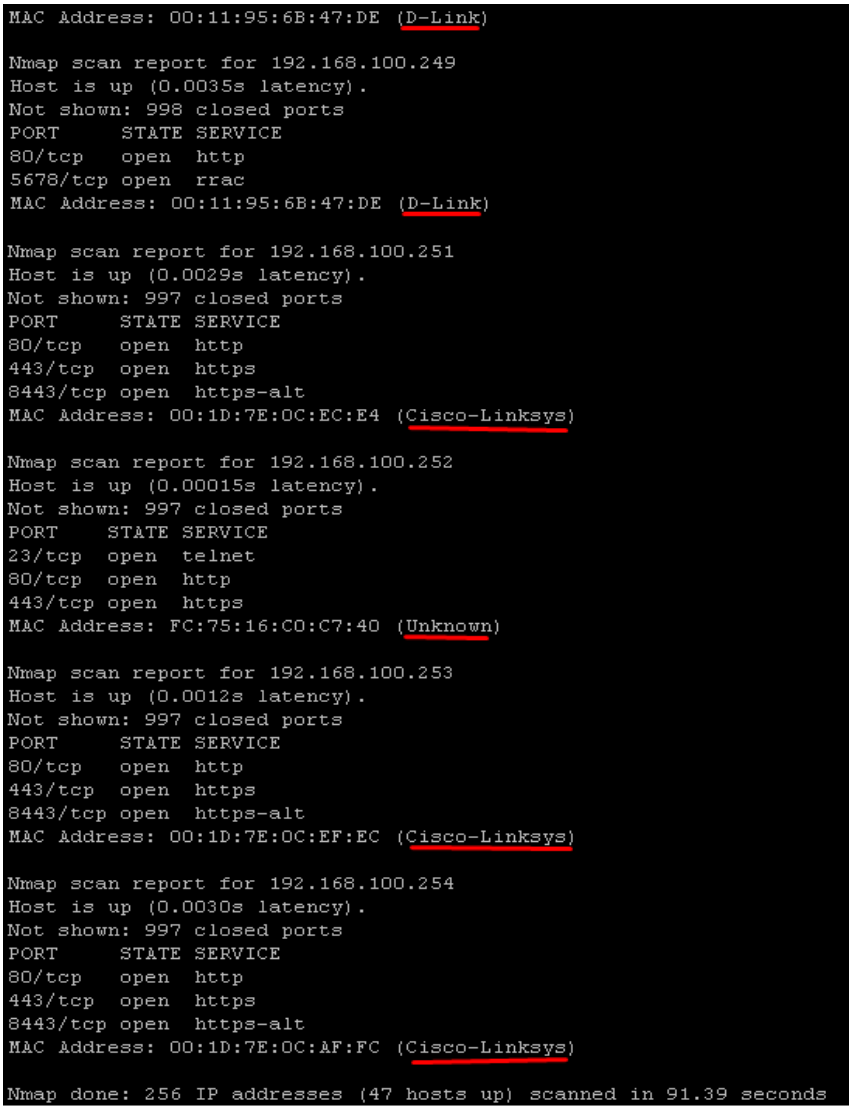


Fuente: Esta investigación

Paso 2. Escaneo

Al realizar un escaneo a toda la red con nmap (namp –T5 192.168.100.0-255) se puede apreciar en la figura 4 que hay 47 equipos activos y que las direcciones 192.168.100.249, 192.168.100.251, 192.168.252, 192.168.168.253.192.168.254 no tiene nombre de equipo y tiene varios puertos abiertos entre ellos el 80 y muestran en su descripcion CISCO lo que nos permite deducir que probablente sea un punto de acceso inalamrbrico del CETEM.

Figura 21. Lista de Access point desde NMAP

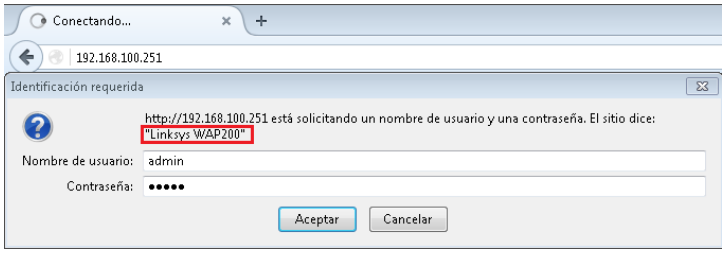


Fuente: Esta investigación

Paso 3. Ganar acceso

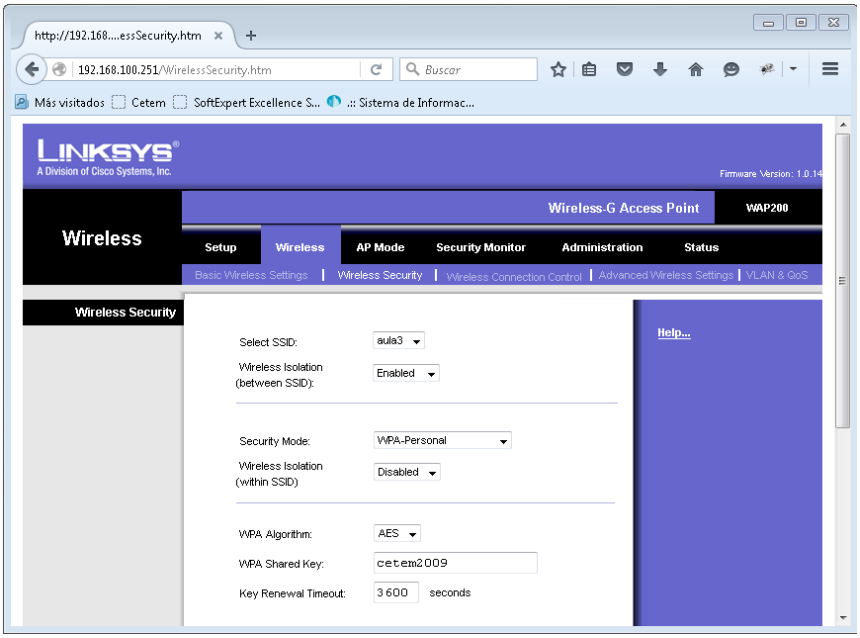
Como se puede observar en la figura 21, al acceder a la direccion 192.168.100.251 utilzando un navegador web aparece una pagina de logueo que en su ventana de identificacion muestra Linksys WAP200. Al ingresar un usuario y contraseña por defecto, logramos ingresar a su sistema de configuración, en la figura 22 se muestra los parametro de configuracion Wifi del punto de acceso. Podemos corroborar los datos de Wifi accediendo desde un cliente como se muestra en la figura 23.

Figura 22. Logueo al punto de Acceso Linksys WAP200



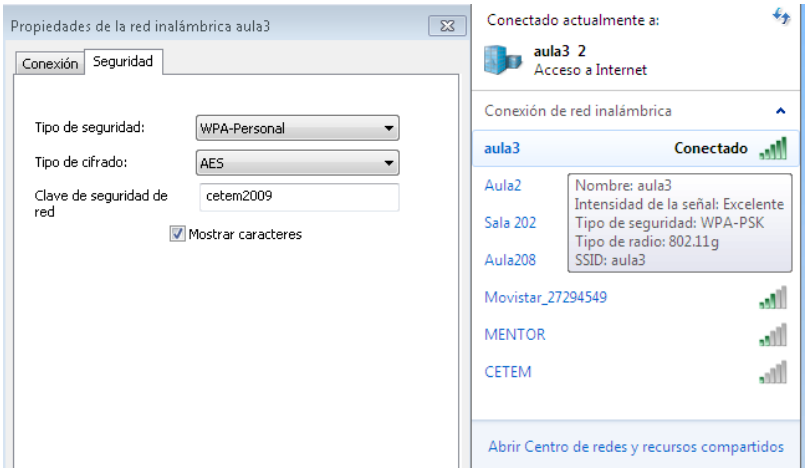
Fuente: Esta investigación

Figura 23. Parámetros de Configuración de Acceso Linksys WAP200



Fuente: Esta investigación

Figura 24. Acceso Wifi Red aula3



Fuente: Esta investigación

En la tabla 35 se puede observar los punto de acceso encontrados y su correspondiente dirección IP y ubicación.

Tabla 35. Lista de Puntos de Acceso inalámbrico

Modelo	**DIRECCIÓN IP**	**UBICACIÓN**
Link Sys WAP200	192.168.100.251	Aula 201
D-Link DAP 2690	192.168.100.252	Aula 202
Link Sys WAP200	192.168.100.253	Aula 203
Link Sys WAP200	192.168.100.254	Aula 204
Airplus XtremeG	192.168.100.249	Aula 208

Fuente: Esta investigación

En el documento ANEXO D – ETHICAL HACKING CETEM, se pueden observar todas las pruebas realizadas de Ethical Hacking y análisis de vulnerabilidades.

Utilizando la escala de probabilidad de la tabla 36, se registran por cada activo las amenazas, las vulnerabilidades y la probabilidad de que materialicen como se muestra en la tabla 37.

Tabla 36. Escala probabilidad

Escala Probabilidad			
Valor			Criterio
5	MA	Muy Frecuente	A diario
4	A	Frecuente	Semanalmente
3	M	Normal	Mensualmente
2	B	Poco Frecuente	Una vez al Año
1	MB	Muy poco Frecuente	Cada varios años

Fuente: Metodología Magerit

Tabla 37. Intranet

Activo TI		34. [Intranet_com] – Intranet					
Administrador		Auxiliar de Soporte y mantenimiento					
Tipo de Activo		REDES DE COMUNICACIONES [COM]					
ID	**Amenaza**	**Exposición / Vulnerabilidad**	**Probabilidad**	**Dimensión**			
				C	**I**	**A**	**D**
[I.8]	Fallo de servicios de comunicaciones	El armario de telecomunicaciones no está debidamente asegurado ni en un sitio privado	A				90
[E.2]	Errores del administrador	Gran parte de los dispositivos de la intranet están configurados por defecto	MA	90	90	90	90
[E.9]	Errores de [re-]encaminamiento	Permite realizar un ataque de hombre en el medio (MITM)	A	30			
[E.19]	Fugas de información	Acceso libre y sin restricciones a información institucional	MA	20			
[E.24]	Caída del sistema por agotamiento de recursos	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	MA				90

Activo TI		34. [Intranet_com] – Intranet					
Administrador		Auxiliar de Soporte y mantenimiento					
Tipo de Activo		REDES DE COMUNICACIONES [COM]					
ID	Amenaza	Exposición / Vulnerabilidad	Probabilidad	Dimensión			
				C	I	A	D
[A.5]	Suplantación de la identidad del usuario	Falta de autentificación y restricciones a información institucional	M	30	30		30
[A.6]	Abuso de privilegios de acceso	Falta de autentificación y restricciones a información institucional	M	90	90		90
[A.7]	Uso no previsto	No existe una restricción de ancho de banda por usuario	MA	90	90		90
[A.10]	Alteración de secuencia	Permite realizar un ataque de hombre en el medio (MITM)	MA	30	30		
[A.11]	Acceso no autorizado	Falta de autentificación y restricciones a información institucional	MA	90	90		
[A.12]	Análisis de tráfico	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	MA	90	90		
[A.14]	Interceptación de información (escucha)	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	MA	70			
[A.15]	Modificación deliberada de la información	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	MA		70		
[A.18]	Destrucción de información	Falta de autentificación y restricciones a información institucional	MA				70
[A.19]	Revelación de información	Falta de autentificación y restricciones a información institucional	MA	90			
[A.24]	Denegación de servicio	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	MA				90

Fuente: Esta investigación

A. **Justificación de Amenazas - Redes de comunicaciones**

[I.8]. Fallo de servicios de comunicaciones:

- Si se materializara esta amenaza se afectaría el 90 % de Disponibilidad de la **Intranet**, ya que el armario de telecomunicaciones no está debidamente asegurado ni en un sito privado. Esta amenaza tiene una probabilidad de ocurrencia **Frecuente**.

[E.2]. Errores del administrador:

- Si se materializara esta amenaza se afectaría el 90 % de Confidencialidad, 90 % de Integridad, 90 % de Autenticidad, 90 % de Disponibilidad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[E.9]. Errores de [re-]encaminamiento:

- Si se materializara esta amenaza se afectaría el 30 % de Confidencialidad de la **Intranet**, ya que permite realizar un ataque de hombre en el medio (MITM) en conexiones inseguras. Esta amenaza tiene una probabilidad de ocurrencia **Frecuente**.

[E.19]. Fugas de información:

- Si se materializara esta amenaza se afectaría el 20 % de Confidencialidad de la **Intranet**, ya que es posible acceder libremente a algunos archivos privados sin restricciones de lectura y escritura. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[E.24]. Caída del sistema por agotamiento de recursos:

- Si se materializara esta amenaza se afectaría el 90 % de Disponibilidad de la **Intranet**, ya que es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o

en el peor de los casos sea provocado por un usuario. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.5]. Suplantación de la identidad del usuario:

- Si se materializara esta amenaza se afectaría el 30 % de Confidencialidad, 30 % de Integridad, 30 % de Disponibilidad de la **Intranet**, ya que es posible ya que, no hay roles de usuario para el acceso a la red. Esta amenaza tiene una probabilidad de ocurrencia **Normal**.

[A.6]. Abuso de privilegios de acceso:

- Si se materializara esta amenaza se afectaría el 90 % de Confidencialidad, 90 % de Integridad, 90 % de Disponibilidad de la **Intranet**, ya que es posible acceder libremente a algunos archivos privados sin restricciones de lectura y escritura. Esta amenaza tiene una probabilidad de ocurrencia **Normal**.

[A.7]. Uso no previsto:

- Si se materializara esta amenaza se afectaría el 90 % de Confidencialidad, 90 % de Integridad, 90 % de Disponibilidad de la **Intranet**, ya que es posible ya que no existe una restricción de ancho de banda por usuario. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.10]. Alteración de secuencia:

- Si se materializara esta amenaza se afectaría el 30 % de Confidencialidad, 30 % de Integridad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.11]. Acceso no autorizado:

- Si se materializara esta amenaza se afectaría el 90 % de Confidencialidad, 90 % de Integridad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por

defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.12]. Análisis de tráfico:

- Si se materializara esta amenaza se afectaría el 90 % de Confidencialidad, 90 % de Integridad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.14]. Interceptación de información (escucha):

- Si se materializara esta amenaza se afectaría el 70 % de Confidencialidad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.15]. Modificación deliberada de la información:

- Si se materializara esta amenaza se afectaría el 70 % de Integridad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.18]. Destrucción de información:

- Si se materializara esta amenaza se afectaría el 70 % de Disponibilidad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.19]. Revelación de información:

- Si se materializara esta amenaza se afectaría el 70 % de Confidencialidad de la **Intranet**, ya que gran parte de los dispositivos de la intranet están configurados por defecto. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

[A.24]. Denegación de servicio:

- Si se materializara esta amenaza se afectaría el 90 % de Disponibilidad de la **Intranet**, ya que es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario. Esta amenaza tiene una probabilidad de ocurrencia **Muy frecuente**.

El mismo análisis se realiza por cada uno de los activos seleccionados previamente. Los documentos completos del registro de vulnerabilidades se pueden revisar en la carpeta ANEXO E – VULNERABILIDADES POTENCIALES POR ACTIVO DE INFORMACIÓN

3.2.4. Proceso P4: Evaluación del Riesgo

3.2.4.1. **Actividad 6: Estimación del impacto.**

El objetivo de esta actividad es determinar el alcance del daño producido sobre los activos de información en caso de llegarse a materializar una amenaza.

Se evalúa el grado de repercusión que pueda presentar cada activo, dentro de las dimensiones de valoración analizadas anteriormente como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de las tablas 38, 39, 40 propuestas por Magerit v.3.

Tabla 38. Degradación del valor

Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% – 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Fuente: Metodología Magerit

Tabla 39. Impacto potencial

Impacto		Degradacion		
		0% - 24%	25%-89%	90% - 100%
Valor	MA (9-10)	M	A	MA
	A (7-8)	M	A	A
	M (4-6)	B	M	M
	B (2-3)	MB	B	B
	MB (0-1)	MB	MB	MB

Fuente: Metodología Magerit

Tabla 40. Escala de Impacto

Escala Impacto		
Valor		Criterio
5	MA	Muy Alto
4	A	Alto
3	M	Medio
2	B	Bajo
1	MB	Muy Bajo

Fuente: Metodología Magerit

Tabla 41. Impacto potencial por activo seleccionado

ID	SERVICIOS [S]	Activo		Degradación	Impacto
		Nivel	Valor		
12	[Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.	A	4	70	Alto
ID	**EQUIPAMIENTO INFORMÁTICO [HW]**	**Activo**		**Degradación**	**Impacto**
		Nivel	**Valor**		
33	[Wifi_Ap_hw] - Red Inalámbrica	A	4	100	Alto
ID	**REDES DE COMUNICACIONES [COM]**	**Activo**		**Degradación**	**Impacto**
		Nivel	**Valor**		
34	[Intranet_com] – Intranet	MA	5	100	Muy Alto
35	[Extranet_com] – Comunicación a los sistemas externos a través de internet	MA	5	100	Muy Alto
ID	**EQUIPAMIENTO AUXILIAR [AUX]**	**Activo**		**Degradación**	**Impacto**
		Nivel	**Valor**		

ID	SERVICIOS [S]	Activo		Degradación	Impacto
		Nivel	Valor		
36	[CAB_RED_aux] - Cableado de Red	MA	5	100	Muy Alto
ID	**INSTALACIONES [L]**	**Activo**		**Degradación**	**Impacto**
		Nivel	**Valor**		
42	[Gabinete_l] – Gabinete de Red	MA	5	100	Muy Alto

Fuente: Esta investigación

3.2.4.2. **Actividad 7: Estimación del Riesgo.**

Para realizar la estimación del riesgo se hace uso de las siguiente escalas cualitativas y cuantitativas. Este valor se obtiene como resultado de la siguiente fórmula:

Riesgo (R)= Probabilidad (F) x Impacto tomando como entradas impacto acumulado y frecuencia.

Tabla 42. Escala de Probabilidad

Escala Probabilidad			
Valor			Criterio
5	MF	Muy Frecuente	A diario
4	F	Frecuente	Semanalmente
3	N	Normal	Mensualmente
2	PF	Poco Frecuente	Una vez al Año
1	MPF	Muy poco Frecuente	Cada varios años

Fuente: Metodología Magerit

Tabla 43. Riesgo

Riesgo		Impacto				
		MB	B	M	A	MA
Probabilidad	MF	5	10	15	20	25
	F	4	8	12	16	20
	N	3	6	9	12	15
	PF	2	4	6	8	10
	MPF	1	2	3	4	5

Fuente: Metodología Magerit

Tabla 44. Escala de riesgo

Escala Riesgo		
Valor		Rango
E	Extremo	De 1 a 4
I	Intolerable	De 5 a 9
T	Tolerable	De 10 a 14
A	Aceptable	De 15 a 25

Fuente: Metodología Magerit

Tabla 45. Valoración de Riesgo en el activo de información Intranet

Activo TI		34. [Intranet_com] – Intranet			
Administrador		Auxiliar de Soporte y mantenimiento			
Tipo de Activo		Redes de Comunica [COM]	**Impacto**	**Valor**	5
Degradación		100		**Nivel**	Muy Alto
ID	**Amenaza**	**Exposición / Vulnerabilidad**	**Probabilidad**		**Riesgo**
			Valor	**Ocurrencia**	**Valor**
[I.8]	Fallo de servicios de comunicaciones	El armario de telecomunicaciones no está debidamente asegurado ni en un sitio privado	4	F	**Extremo**
[E.2]	Errores del administrador	Gran parte de los dispositivos de la intranet están configurados por defecto	3	N	**Intolerable**
[E.9]	Errores de [re-]encaminamiento	Permite realizar un ataque de hombre en el medio (MITM)	3	N	**Intolerable**
[E.19]	Fugas de información	Acceso libre y sin restricciones a información institucional	4	F	**Extremo**
[E.24]	Caída del sistema por agotamiento de recursos	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	4	F	**Extremo**
[A.5]	Suplantación de la identidad del usuario	Falta de autentificación y restricciones a información institucional	3	N	**Intolerable**
[A.6]	Abuso de privilegios de acceso	Falta de autentificación y restricciones a información institucional	4	F	**Extremo**
[A.7]	Uso no previsto	No existe una restricción de ancho de banda por usuario	5	MF	**Extremo**
[A.10]	Alteración de secuencia	Permite realizar un ataque de hombre en el medio (MITM)	3	N	**Intolerable**

Activo TI		34. [Intranet_com] – Intranet			
Administrador		Auxiliar de Soporte y mantenimiento			
Tipo de Activo		Redes de Comunica [COM]	Impacto	Valor	5
Degradación		100		Nivel	Muy Alto
ID	Amenaza	Exposición / Vulnerabilidad	Probabilidad		Riesgo
			Valor	Ocurrencia	Valor
[A.11]	Acceso no autorizado	Falta de autentificación y restricciones a información institucional	5	MF	Extremo
[A.12]	Análisis de tráfico	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	4	F	Extremo
[A.14]	Interceptación de información (escucha)	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	4	F	Extremo
[A.15]	Modificación deliberada de la información	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	3	N	Intolerable
[A.18]	Destrucción de información	Falta de autentificación y restricciones a información institucional	3	N	Intolerable
[A.19]	Revelación de información	Falta de autentificación y restricciones a información institucional	4	F	Extremo
[A.24]	Denegación de servicio	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	5	MF	Extremo
		RIESGO ACTUAL	3,8	N	Extremo

Fuente: Esta Investigación.

Este mismo análisis se realizó sobre cada uno de los activos de información que están directamente relacionados con esta investigación Ver ANEXO F. ESTIMACION DEL ESTADO DEL RIESGO

3.2.4.3. **Actividad 8: Calificación del Riesgo.**

Teniendo en cuenta el análisis de riesgos se puede observar que existen activos del Centro de Estudios EMSSANAR CETEM que presentan valores de riesgo actual catalogados como intolerables y Extremos. En la tabla 46 se observa el resumen de estimación del estado del riesgo.

Tabla 46. Estimación del estado del riesgo.

Tipo de Activo	Activo TI	RIESGO ACTUAL
Servicios [S]	12. [Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.	Intolerable
Equi. Informático [HW]	33. [Wifi_Ap_hw] - Red Inalámbrica	Tolerable
Redes de Comunica [COM]	34. [Intranet_com] – Intranet	Extremo
Redes de Comunica [COM]	35. [Extranet_com] – Comunicación a los sistemas externos a través de internet	Tolerable
Equipamento Auxiliar [AUX]	36. [CAB_RED_aux] - Cableado de Red	Intolerable
Instalaciones [L]	42. [Gabinete_l] – Gabinete de Red	Extremo

Fuente: Esta investigación

12. [Internet_S] - Servicio de internet al que pueden acceder los administrativos, docentes estudiantes y visitantes.

Entre las amenazas que se expone este activo están:

- ✓ Fugas de información
- ✓ Caída del sistema por agotamiento de recursos
- ✓ Suplantación de la identidad del usuario
- ✓ Abuso de privilegios de acceso
- ✓ Uso no previsto
- ✓ Acceso no autorizado
- ✓ Modificación deliberada de la información
- ✓ Destrucción de información
- ✓ Revelación de información

- ✓ Denegación de servicio

Estas amenazas tienen un nivel de riesgo intolerable debido a:

- ✓ Los usuarios que se conectan a internet necesariamente tienen que hacerlo por medio de la intranet, razón por la cual pueden acceder fácilmente a información institucional tales como formatos, copias de seguridad de calificaciones de estudiantes.
- ✓ No existe un control de acceso a páginas Web, ni de ancho de banda.

33. [Wifi_Ap_hw] - Red Inalámbrica

Entre las amenazas que se expone este activo están:

- ✓ Contaminación electromagnética.
- ✓ Avería de origen físico o lógico.
- ✓ Corte del suministro eléctrico
- ✓ Emanaciones electromagnéticas
- ✓ Errores del administrador
- ✓ Caída del sistema por agotamiento de recursos
- ✓ Abuso de privilegios de acceso
- ✓ Uso no previsto
- ✓ Acceso no autorizado
- ✓ Denegación de servicio

Estas amenazas tienen un nivel de riesgo tolerable debido a:

- ✓ El Wifi aunque no es de libre acceso no existen restricciones para acceder a este servicio una vez te proporcionen la contraseña.
- ✓ Los Access Point poseen una configuración por defecto.

34. [Intranet_com] – Intranet

Entre las amenazas que se expone este activo están:

- ✓ Fallo de servicios de comunicaciones
- ✓ Errores del administrador
- ✓ Errores de [re-]encaminamiento
- ✓ Fugas de información

- ✓ Caída del sistema por agotamiento de recursos
- ✓ Suplantación de la identidad del usuario
- ✓ Abuso de privilegios de acceso
- ✓ Uso no previsto
- ✓ Alteración de secuencia
- ✓ Acceso no autorizado
- ✓ Análisis de tráfico
- ✓ Interceptación de información (escucha)
- ✓ Modificación deliberada de la información
- ✓ Destrucción de información
- ✓ Revelación de información
- ✓ Denegación de servicio

Estas amenazas tienen un nivel de riesgo Extremo debido a:

- ✓ El armario de telecomunicaciones no se encuentra resguardado y permite conectar cualquier dispositivo de forma física directamente.
- ✓ Los administrados no usan VLANs para acceder a los sistemas y servicios por lo tanto es posible realizar un ataque MIT.
- ✓ Los dispositivos de comunicaciones poseen claves de acceso por defecto.
- ✓ Es posible saturar el ancho de banda de la intranet.
- ✓ Es posible acceder a directorios e impresoras compartidas.
- ✓ Es posible realizar un DoS.
- ✓ La intranet no está soneteada.

35. [Extranet_com] – Comunicación a los sistemas externos a través de internet

- ✓ Entre las amenazas que se expone este activo están:
- ✓ Fallo de servicios de comunicaciones
- ✓ Errores del administrador
- ✓ Errores de [re-]encaminamiento
- ✓ Alteración accidental de la información
- ✓ Destrucción de información

- ✓ Fugas de información
- ✓ Caída del sistema por agotamiento de recursos
- ✓ Suplantación de la identidad del usuario
- ✓ Abuso de privilegios de acceso
- ✓ Manipulación de los registros de actividad (log)
- ✓ Acceso no autorizado
- ✓ Análisis de tráfico
- ✓ Interceptación de información (escucha)
- ✓ Modificación deliberada de la información
- ✓ Destrucción de información
- ✓ Revelación de información
- ✓ Denegación de servicio

Estas amenazas tienen un nivel de riesgo Tolerable debido a:

- ✓ Los sistemas de información son administrados por entidades externas, lo cual baja la probabilidad de que se materialicen las amenazas.

36. [CAB_RED_aux] - Cableado de Red

Entre las amenazas que se expone este activo están:

- ✓ Contaminación electromagnética.
- ✓ Avería de origen físico o lógico.
- ✓ Corte del suministro eléctrico
- ✓ Emanaciones electromagnéticas
- ✓ Errores del administrador
- ✓ Errores de mantenimiento / actualización de equipos (hardware)
- ✓ Acceso no autorizado

Estas amenazas tienen un nivel de riesgo Intolerable debido a:

- ✓ El cableado de red comienza en el armario de comunicación y este no se encuentra resguardado.
- ✓ Los dispositivos de interconexión son 100BASE-TX.

42. [Gabinete_l] – Gabinete de Red

Entre las amenazas que se expone este activo están:

- ✓ Alteración accidental de la información
- ✓ Destrucción de información
- ✓ Fugas de información
- ✓ Uso no previsto
- ✓ Acceso no autorizado
- ✓ Modificación deliberada de la información
- ✓ Destrucción de información
- ✓ Revelación de información
- ✓ Ocupación enemiga

Estas amenazas tienen un nivel de riesgo Intolerable Extremo a:

- ✓ El armario de comunicación no se encuentra resguardado.

3.2.5. Proceso P5: Tratamiento de riesgos

3.2.5.1. **Actividad 9: Tratamiento de riesgos.**

El tratamiento de riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la organización. Las posibles acciones de tratamiento de riesgo son:

Reducir: consiste en elegir controles de corrección, eliminación, prevención, mitigación del impacto, detección, recuperación, monitoreo y concienciación con el fin de reducir el nivel de riesgo.

Aceptar: no es necesario implementar controles adicionales, estos riesgos podrán ser aceptados teniendo en cuenta que la organización asume los daños provocados por la materialización del riesgo.

Evitar: o eliminar el riesgo, que no suele ser la mejor opción ya que resulta difícil o demasiado costoso, pues muchas de las veces se basa en eliminación de procesos o incluso del activo involucrado.

Transferir: a un tercero de forma que se asegure el activo o subcontratando el servicio.

En la tabla 47 se muestra el tratamiento adecuado de acuerdo al nivel de riesgo:

Tabla 47. Tratamiento del riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Acepta.
Tolerable	Una de las tres opciones: a. Se transfiere.
Intolerable	b. Se evita.
Extremo	c. Se reduce.

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro 3

Una vez valorado los riesgos para cada uno de los activos más relevantes para esta investigación, se selecciona la opción de tratamiento adecuada de acuerdo a la tabla 47.

Tabla 48. Tratamiento de riesgos del activo "Intranet"

Activo TI		34. [Intranet_com] – Intranet				
Administrador		Auxiliar de Soporte y mantenimiento				
Tipo de Activo		Redes de Comunica [COM]	**Impacto**		**Valor**	5
Degradación		100			**Nivel**	Muy Alto
ID	**Amenaza**	**Exposición / Vulnerabilidad**	**Probabilidad**		**Valor del Riesgo**	**Tratamiento del riesgo**
			Valor	**Ocurrencia**		
[I.8]	Fallo de servicios de comunicaciones	El armario de telecomunicaciones no está debidamente asegurado ni en un sitio privado	4	F	**Extremo**	Evita

Activo TI		34. [Intranet_com] – Intranet				
Administrador		Auxiliar de Soporte y mantenimiento				
Tipo de Activo		Redes de Comunica [COM]	Impacto		Valor	5
Degradación		100			Nivel	Muy Alto
ID	Amenaza	Exposición / Vulnerabilidad	Probabilidad		Valor del Riesgo	Tratamiento del riesgo
			Valor	Ocurrencia		
[E.2]	Errores del administrador	Gran parte de los dispositivos de la intranet están configurados por defecto	3	N	**Intolerable**	Evita
[E.9]	Errores de [re-]encaminamiento	Permite realizar un ataque de hombre en el medio (MITM)	3	N	**Intolerable**	Reduce
[E.19]	Fugas de información	Acceso libre y sin restricciones a información institucional	4	F	**Extremo**	Evita
[E.24]	Caída del sistema por agotamiento de recursos	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	4	F	**Extremo**	Reduce
[A.5]	Suplantación de la identidad del usuario	Falta de autentificación y restricciones a información institucional	3	N	**Intolerable**	Evita
[A.6]	Abuso de privilegios de acceso	Falta de autentificación y restricciones a información institucional	4	F	**Extremo**	Evita
[A.7]	Uso no previsto	No existe una restricción de ancho de banda por usuario	5	MF	**Extremo**	Reduce
[A.10]	Alteración de secuencia	Permite realizar un ataque de hombre en el	3	N	**Intolerable**	Reduce

Activo TI		34. [Intranet_com] – Intranet				
Administrador		Auxiliar de Soporte y mantenimiento				
Tipo de Activo		Redes de Comunica [COM]	Impacto		Valor	5
Degradación		100			Nivel	Muy Alto
ID	Amenaza	Exposición / Vulnerabilidad	Probabilidad		Valor del Riesgo	Tratamiento del riesgo
			Valor	Ocurrencia		
		medio (MITM)				
[A.11]	Acceso no autorizado	Falta de autentificación y restricciones a información institucional	5	MF	**Extremo**	Evita
[A.12]	Análisis de tráfico	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	4	F	**Extremo**	Reduce
[A.14]	Interceptación de información (escucha)	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	4	F	**Extremo**	Reduce
[A.15]	Modificación deliberada de la información	Como el acceso a internet es libre y se hace mediante la intranet, se puede realizar fácilmente.	3	N	**Intolerable**	Evita
[A.18]	Destrucción de información	Falta de autentificación y restricciones a información institucional	3	N	**Intolerable**	Evita
[A.19]	Revelación de información	Falta de autentificación y restricciones a información institucional	4	F	**Extremo**	Evita

Activo TI		34. [Intranet_com] – Intranet				
Administrador		Auxiliar de Soporte y mantenimiento				
Tipo de Activo		Redes de Comunica [COM]	Impacto		Valor	5
Degradación		100			Nivel	Muy Alto
ID	Amenaza	Exposición / Vulnerabilidad	Probabilidad		Valor del Riesgo	Tratamiento del riesgo
			Valor	Ocurrencia		
[A.24]	Denegación de servicio	Es posible que la cantidad de usuarios que acceden causen la denegación de algún servicio o en el peor de los casos sea provocado por un usuario	5	MF	**Extremo**	Reduce

Fuente: Esta investigación

En el ANEXO G. TRATAMIENTO DE RIESGOS se muestra el tratamiento de riesgos para cada uno de los demás activos de información.

3.3. ANÁLISIS DE BRECHA

3.3.1. Actividad 10: Verificación controles establecidos según norma ISO/IEC 27002:2013

Para poder determinar con mayor claridad el tratamiento a seguir para cada uno de los activos, se verifica el cumplimiento de cada uno de los controles establecidos por la norma ISO/IEC 27002:2013 a través del método de observación directa.

El cual consto de varias visitas guiadas y supervisión de todas salas y oficinas pertenecientes al CETEM. Esto se complementó con revisión documental de los manuales de funciones y procedimientos, formatos, etc.

Una vez relevada la información, se procedió a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala de madurez definida por el estándar COBIT.

Figura 25. Escala de madurez COBIT

Escala	%	Descripción
N/A	-	No aplica
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Esta investigación

Las tablas 49 a 62 muestran la verificación controles de seguridad conforme al estándar ISO/IEC 27002:2013:

Tabla 49. Verificación Controles de Políticas De La Seguridad De La Información

<table>
<tr><td>A.5</td><td colspan="4">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="4">Orientación de la dirección para la gestión de la seguridad de la información</td></tr>
<tr><td colspan="5">Objetivo: Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td rowspan="5">A.5.1.1</td><td rowspan="5">Políticas para la seguridad de la información</td><td rowspan="5">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.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas de la seguridad de la información proveen un direccionamiento estratégico acorde a los requerimientos de la organización y cumplimiento con leyes y regulaciones. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No se tiene implementado un SGSI ni existe un documento que contemple las políticas de seguridad de la información</td></tr>
<tr><td rowspan="5">A.5.1.2</td><td rowspan="5">Revisión de las políticas para la seguridad de la información</td><td rowspan="5">Control: seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas de la seguridad de la información deberían ser evaluadas con el fin de responder a los cambios de la organización.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado (ver A.5.1.1).</td></tr>
</table>

Fuente: Esta investigación

Tabla 50. Verificación Controles De Organización De La Seguridad De La Información

<table>
<tr><td>A.6</td><td colspan="4">ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.6.1</td><td colspan="4">Organización Interna</td></tr>
<tr><td colspan="5">Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.</td></tr>
<tr><td rowspan="5">A.6.1.1</td><td rowspan="5">Roles y responsabilidades para la seguridad de la información</td><td rowspan="5">Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los roles y responsabilidades son vitales para la protección de los activos informáticos individuales, así como los procesos específicos para la seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td><td rowspan="3">Inexistente</td></tr>
<tr><td>IMPLEMENTA
SI | NO</td></tr>
<tr><td>Los roles y responsabilidades relativas a la seguridad de la información aún no están definidas, debido a que no se tiene implementado un SGSI.</td></tr>
<tr><td rowspan="5">A.6.1.2</td><td rowspan="5">Separación de deberes</td><td rowspan="5">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.</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Ningún empleado debería tener acceso a modificar los activos informáticos sin autorización previa.</td><td rowspan="3">Inicial</td></tr>
<tr><td>IMPLEMENTA
SI | NO</td></tr>
<tr><td>El personal aunque está separado por áreas, se les otorga acceso a los activos y/o información en general.</td></tr>
<tr><td rowspan="2">A.6.1.3</td><td rowspan="2">Contacto con las</td><td rowspan="2">Control: Se deben mantener contactos</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
</table>

	autoridades	apropiados con las autoridades pertinentes.	Deberían existir procedimientos para contactar a las autoridades pertinentes y reportar las incidencias relativas a la seguridad de la información. **IMPLEMENTA** **SI** / **NO** Las incidencias relativas a la seguridad de la información son resueltas internamente	Inexistente
A.6.1.4	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.	**APLICA** **SI** / **NO** Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información, así como las actualizaciones de los equipos y/o dispositivos. **IMPLEMENTA** **SI** / **NO** No hay contactos con asociaciones profesionales especializadas en seguridad.	**NIVEL DE MADUREZ** Inexistente
A.6.1.5	Seguridad de la información en la gestión de proyectos	**Control:** La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	**APLICA** **SI** / **NO** Una metodología de análisis de riesgos debería ser parte del proceso de implementación de un proyecto de TI con el fin de direccionarlos y controlarlos. **IMPLEMENTA** **SI** / **NO** Los riesgos asociados a la seguridad de la información no son contemplados desde los inicios de los proyectos de TI.	**NIVEL DE MADUREZ** Inexistente
A.6.2	**Dispositivos móviles y teletrabajo**			

<table>
<tr><td colspan="5">Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.</td></tr>
<tr><td rowspan="5">A.6.2.1</td><td rowspan="5">Políticas para dispositivos móviles</td><td rowspan="5">Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los dispositivos móviles son un riesgo potencial para la seguridad de la información.</td><td rowspan="4">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una política de seguridad para los dispositivos móviles.</td></tr>
<tr><td rowspan="5">A.6.2.2</td><td rowspan="5">Teletrabajo</td><td rowspan="5">Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El teletrabajo debería tener una política de seguridad sobre las condiciones y restricciones.</td><td rowspan="4">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Aunque se permite el acceso a algunos dispositivos de forma remota, no se implementa el teletrabajo.</td></tr>
</table>

Fuente: Esta investigación

Tabla 51. Verificación Controles de Seguridad De Los Recursos Humanos

<table>
<tr><td>A.7</td><td colspan="4">SEGURIDAD DE LOS RECURSOS HUMANOS</td></tr>
<tr><td>A.7.1</td><td colspan="4">Antes de asumir el empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.</td></tr>
<tr><td rowspan="5">A.7.1.1</td><td rowspan="5">Selección</td><td rowspan="5">Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.</td><td>APLICA</td><td rowspan="5">Repetible</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensitiva de la organización.</td></tr>
<tr><td>IMPLEMENTA
SI / NO</td></tr>
<tr><td>El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.</td></tr>
<tr><td rowspan="5">A.7.1.2</td><td rowspan="5">Términos y condiciones del empleo</td><td rowspan="5">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.</td><td>APLICA</td><td rowspan="5">Repetible</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Los acuerdos contractuales de los empleados deberían tener cláusulas relativas a la confidencialidad de la información y respecto a las leyes y derechos de propiedad intelectual.</td></tr>
<tr><td>IMPLEMENTA
SI / NO</td></tr>
<tr><td>Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.</td></tr>
<tr><td>A.7.2</td><td colspan="4">Durante la ejecución del empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
</table>

<table>
<tr><td rowspan="5">A.7.2.1</td><td rowspan="5">Responsabilidades de
la dirección</td><td rowspan="5">Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La dirección asegura que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados están comprometidos con las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td><td rowspan="4">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.</td></tr>
<tr><td rowspan="5">A.7.2.2</td><td rowspan="5">Toma de conciencia, educación y formación en la seguridad de la información</td><td rowspan="5">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, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Mediante un programa de entrenamiento relativo a la seguridad de la información, los empleados son conscientes de su importancia y cómo pueden cumplir con las políticas del SGSI.</td><td rowspan="4">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se tiene implementado un SGSI ni un plan de concientización formal relativo a la seguridad de la información.</td></tr>
<tr><td rowspan="2">A.7.2.3</td><td rowspan="2">Proceso disciplinario</td><td rowspan="2">Control: Se debe contar con</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

		un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y el impacto que tiene en la organización. **IMPLEMENTA** **SI** / **NO** Debido a que no se ha implementado un SGSI, no se tiene plan de concientización relativo a la seguridad de la información.	Inexistente
A.7.3	**Terminación y cambio de empleo**			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**APLICA** **SI** / **NO** Los acuerdos contractuales deberían plasmar el compromiso relativo a la confidencialidad de la información aún después de la terminación o cambio de empleo. **IMPLEMENTA** **SI** / **NO** Al terminar o cambiar de empleo no se notifica a al empleado sobre la validez de sus responsabilidades y deberes relativos a la seguridad de la información.	**NIVEL DE MADUREZ** Inicial

Fuente: Esta investigación

Tabla 52. Verificación Controles de Gestión De Activos

<table>
<tr><td>A.8</td><td colspan="4">GESTIÓN DE ACTIVOS</td></tr>
<tr><td>A.8.1</td><td colspan="4">Responsabilidad por los activos</td></tr>
<tr><td colspan="5">Objetivo: Identificar los activos organizacionales y definir las responsabilidades apropiadas.</td></tr>
<tr><td rowspan="5">A.8.1.1</td><td rowspan="5">Inventario de activos</td><td rowspan="5">Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deben elaborar y mantener un inventario de estos activos</td><td>APLICA</td><td rowspan="5">Inicial</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El inventario y clasificación de activos permite identificar la importancia de cada uno de ellos y su impacto en la organización. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td>IMPLEMENTA
SI | NO</td></tr>
<tr><td>Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.</td></tr>
<tr><td rowspan="5">A.8.1.2</td><td rowspan="5">Propiedad de los activos</td><td rowspan="5">Control: Los activos mantenidos en el inventario deben tener un propietario.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los propietarios son responsables del uso de los activos informáticos durante todo su ciclo de vida. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td>IMPLEMENTA
SI | NO</td></tr>
<tr><td>No se especifican los propietarios de los activos informáticos inventariados.</td></tr>
<tr><td rowspan="3">A.8.1.3</td><td rowspan="3">Uso aceptable de los activos</td><td rowspan="3">Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de</td><td>APLICA</td><td rowspan="3">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los empleados o contratistas son responsables del uso que les dan a los activos informáticos de la organización.</td></tr>
</table>

		procesamiento de información.	**IMPLEMENTA** **SI** / **NO** No se especifican las reglas para el uso aceptable de los activos.	
A.8.1.4	Devolución de activos	**Control:** Todos los empleados y usuarios de las partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	**APLICA** **SI** / **NO** La devolución de activos debe ser formalizada y la información almacenada en dispositivos personales transferida a la organización. **IMPLEMENTA** **SI** / **NO** Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.	**NIVEL DE MADUREZ** Repetible
A.8.2	**Clasificación de la información**			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización.				
A.8.2.1	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 autorizada.	**APLICA** **SI** / **NO** La clasificación de la información es vital para determinar el grado y control de seguridad que debería tener. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** / **NO** Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.	**NIVEL DE MADUREZ** Repetible
A.8.2.2	Etiquetado de la	**Control:** Se debe desarrollar e	**APLICA** **SI** / **NO**	**NIVEL DE MADUREZ**

	información	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.	El etiquetado de la información debe reflejar el esquema de clasificación adoptador por la organización (ver A.8.2.1). **IMPLEMENTA** **SI** / **NO** Actualmente no existe procedimiento alguno para el etiquetado y/o clasificación de la información según el nivel de criticidad.	Repetible
A.8.2.3	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.	**APLICA** **SI** / **NO** El acceso a los activos debería restringirse de acuerdo a su esquema de clasificación. **IMPLEMENTA** **SI** / **NO** Actualmente no existen procedimientos para el manejo de la información, ya que ésta no está clasificada según el nivel de criticidad (ver A.8.2.1).	**NIVEL DE MADUREZ** Repetible
A.8.3	**Manejo de medios**			
Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.				
A.8.3.1	Gestión de medios removibles	**Control:** Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de la organización.	**APLICA** **SI** / **NO** Los medios removibles podrían almacenar información confidencial y deberían tener el mismo tratamiento y esquema de clasificación que cualquier otro activo informático. **IMPLEMENTA** **SI** / **NO**	**NIVEL DE MADUREZ** Inicial

			Los medio removibles son protegidos, pero no cuentan con un nivel de clasificación de información (ver A.8.2.1)	
A.8.3.2	Disposición de los medios	**Control:** Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	**APLICA** **SI** / **NO** Los medios removibles podrían almacenar información confidencial y deberían ser removidos almacenando copias de seguridad en lugares seguros y garantizar que su información no sea revocable o legible. **IMPLEMENTA** **SI** / **NO** Los medio removibles son dispuestos en lugares inseguros y su información es almacenada en medios no tan confiables.	**NIVEL DE MADUREZ** Inicial
A.8.3.3	Transferencia de medios físicos	**Control:** Los medios que contienen información se deben proteger contra acceso no autorizados, uso indebido o corrupción durante el transporte.	**APLICA** **SI** / **NO** Los medios transportados podrían tener información sensitiva **IMPLEMENTA** **SI** / **NO** No se transportan activos informáticos.	**NIVEL DE MADUREZ** Inicial

Fuente: Esta investigación

Tabla 53. Verificación Controles De Acceso

<table>
<tr><td>A.9</td><td colspan="4">CONTROL DE ACCESO</td></tr>
<tr><td>A.9.1</td><td colspan="4">Requisitos del negocio para control de acceso</td></tr>
<tr><td colspan="5">Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.</td></tr>
<tr><td rowspan="5">A.9.1.1</td><td rowspan="5">Política de control de acceso</td><td rowspan="5">Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El control de acceso físico y lógico con principios del menor privilegio permite tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existen controles físicos y lógicos que garantizan el acceso con menor privilegio, ni se ha documentado en una política de seguridad de la información.</td></tr>
<tr><td rowspan="5">A.9.1.2</td><td rowspan="5">Acceso a redes y a servicios en red</td><td rowspan="5">Control: Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las redes y servicios de red proveen acceso a diferentes servicios dentro de la organización al personal autorizado.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
La red está sin segmentar y es accedida libremente por estudiantes, docentes y administrativos sin restricciones.</td></tr>
<tr><td>A.9.2</td><td colspan="4">Gestión de acceso de usuarios</td></tr>
<tr><td colspan="5">Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.</td></tr>
<tr><td>A.9.2.1</td><td>Registro y cancelación</td><td>Control: Se debe implementar un</td><td>APLICA
SI | NO</td><td>NIVEL DE MADUREZ</td></tr>
</table>

	de registro de usuarios	proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Los identificadores únicos de los empleados mantienen un registro de las acciones realizadas. **IMPLEMENTA** **SI** / **NO** El acceso a la red no requiere registrarse previamente y no cuenta con ninguna restricción.	Inexistente
A.9.2.2	Suministro de acceso de usuarios	**Control:** Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios	**APLICA** **SI** / **NO** Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal. **IMPLEMENTA** **SI** / **NO** El acceso a la red no requiere registrarse previamente y no cuenta con ninguna restricción. (Ver A.9.2.1).	**NIVEL DE MADUREZ** Inexistente
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	**APLICA** **SI** / **NO** Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso. **IMPLEMENTA** **SI** / **NO** El acceso a la red no requiere registrarse previamente y no cuenta con ninguna restricción. (Ver A.9.2.1).	**NIVEL DE MADUREZ** Inexistente
A.9.2.4	Gestión de información	**Control:** La asignación de	**APLICA** **SI** / **NO**	**NIVEL DE MADUREZ**

	de autenticación secreta de usuarios	información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	La autenticación de los empleados en los sistemas debería mantenerse confidencial y secreta para evitar alteración y/o modificación de la información por parte de personas no autorizadas. **IMPLEMENTA** **SI** / **NO** Aunque los equipos de administrativos tengan clave de acceso no es indispensable para el acceso a la red. La entrega de claves de acceso se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.	Inexistente
A.9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	**APLICA** **SI** / **NO** Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas. **IMPLEMENTA** **SI** / **NO** No se realizan verificaciones regulares de los derechos de acceso a los sistemas.	**NIVEL DE MADUREZ** Inexistente
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben	**APLICA** **SI** / **NO** La remoción de los derechos de acceso permite que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminado el contrato o cambio en el cargo. **IMPLEMENTA**	**NIVEL DE MADUREZ** Inexistente

		ajustar cuando se hagan cambios.	**SI**	**NO**	
			No existe un proceso y/o documentación formal de remoción de los privilegios de acceso de los empleados que cambian el cargo o terminan contrato.		
A.9.3	**Responsabilidades de los usuarios**				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A.9.3.1	Uso de información de autenticación secreta	**Control:** Se debe exigir a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	
			La información confidencial debería ser accedida sólo por las personas autorizadas y para fines de la organización.		Inicial
			IMPLEMENTA		
			SI	**NO**	
			No existe un proceso y/o documentación formal de resguardo de información.		
A.9.4	**Control de acceso a sistemas y aplicaciones**				
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.					
A.9.4.1	Restricción de acceso a la información	**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.	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	
			El acceso a la información debe ser granular en pro de evitar revelación o acceso a personas no autorizadas.		Inicial
			IMPLEMENTA		
			SI	**NO**	
			Los derechos de acceso a los sistemas e información no son controlados de acuerdo a rol y responsabilidad del empleado en la organización.		
A.9.4.2	Procedimiento de	**Control**: Cuando lo requiere la política de	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	

	ingreso seguro	control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	El inicio de sesión seguro permite que una persona no autorizada tenga acceso a información privilegiada **IMPLEMENTA** **SI** / **NO** Aunque los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro no es indispensable para el acceso a la red.	Inicial
A.9.4.3	Sistema de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	**APLICA** **SI** / **NO** Los sistemas de gestión de contraseñas son un mecanismo fuerte de autenticación de usuarios y evita que sean adivinadas por ataques de fuerza bruta y/o diccionario. **IMPLEMENTA** **SI** / **NO** Los sistemas de gestión de contraseñas no son interactivos ya que es otorgada de forma manual.	**NIVEL DE MADUREZ** Inexistente
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.	**APLICA** **SI** / **NO** Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente. **IMPLEMENTA** **SI** / **NO** Los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados.	**NIVEL DE MADUREZ** Inicial
A.9.4.5	Control de acceso	**Control:** Se debe restringir el acceso a	**APLICA** **SI** / **NO**	**NIVEL DE MADUREZ**

	a códigos fuente de programas	los códigos fuentes de los programas.	El código fuente contiene la información de cómo se ha implementado el programa y bajo que lenguaje de programación, así como las librerías empleadas.	Repetible
			IMPLEMENTA	
			SI / **NO**	
			El código fuente sólo es accedido por las personas autorizadas.	

Fuente: Esta investigación

Tabla 54. Verificación Controles de Cifrado

A.10	**CIFRADO**			
A.10.1	**Controles criptográficos**			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.				
A.10.1.1	Política sobre el uso de controles criptográficos	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			La criptografía cifra mediante algoritmos de encriptación los mensajes transmitidos garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas.	Inexistente
			IMPLEMENTA	
			SI / **NO**	
			No existe una política sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida.	
A.10.1.2	Gestión de llaves	**Control:** Se debe desarrollar e	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	

		implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	La gestión de llaves criptográficas vela por su seguridad, mantenimiento, renovación, distribución y destrucción.	Inexistente
			IMPLEMENTA	
			SI / **NO**	
			No existe una política sobre el uso y distribución de llaves criptográficas (ver A.10.1.1).	

Fuente: Esta investigación

Tabla 55. Verificación Controles de Seguridad Física Y Del Entorno

A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**			
A.11.1	**Áreas seguras**			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A.11.1.1	Perímetro de seguridad física	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			El perímetro de seguridad física impide el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.	Inexistente
			IMPLEMENTA	
			SI / **NO**	
			No existe un perímetro físico controlado a los armarios de telecomunicaciones, solo existe personal de seguridad en las noches en la entrada el CETEM.	
A.11.1.2	Controles de acceso físicos	**Control:** Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			Los controles de accesos físicos impiden el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.	Inexistente

			IMPLEMENTA	
			SI / **NO**	
			Se permiten el acceso a todos los usuarios ya que el armario de telecomunicaciones se encuentra en un salón de clases.	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**Control:** Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas así como no ser públicamente visibles.	Inicial
			IMPLEMENTA	
			SI / **NO**	
			Las oficinas y lugares de trabajo cuentan con cerraduras normales.	
A.11.1.4	Protección contra amenazas externas y ambientales	**Control:** Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			Protección física contra los desastres naturales y/o humanos.	Inexistente
			IMPLEMENTA	
			SI / **NO**	
			No existe una protección física contra los desastres naturales y/o humanos.	
A.11.1.5	Trabajo en áreas seguras	**Control:** Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	
			Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente.	Inexistente
			IMPLEMENTA	
			SI / **NO**	
			No se tienen áreas seguras para ser aseguradas físicamente.	
A.11.1.6	Áreas de despacho y	**Control:** Se deben controlar los puntos	**APLICA**	**NIVEL DE MADUREZ**
			SI / **NO**	

	carga	de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Los lugares de entrega de equipos y otros dispositivos están controlados y se restringe el acceso a áreas externas de la organización. **IMPLEMENTA** **SI** / **NO** No se tienen áreas de despacho y de carga.	Inexistente

Fuente: Esta investigación

Tabla 56. Verificación Controles de Seguridad De Las Operaciones

A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	**Procedimientos operacionales y responsabilidades**			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	**Control:** Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	**APLICA** **SI** / **NO** Los procedimientos operacionales deberían estar documentados y disponibles para todos los usuarios. Estos procedimientos incluyen las copias de seguridad, almacenamiento, manejo de errores, encendido/apagado de equipos, instalación/configuración de sistemas, etc. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** / **NO** Los procedimientos operacionales están documentados aunque no se encuentre implementado un SGSI.	**NIVEL DE MADUREZ** Repetible
A.12.1.	Gestión de	**Control:** Se	**APLICA**	**NIVEL DE**

2	cambios	deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	**SI** / **NO** Los cambios en los equipos que afectan la seguridad de la información deberían ser controlados y debidamente planeados y probados. **IMPLEMENTA** **SI** / **NO** No existe una política sobre el control sobre los cambios en los equipos que afectan la seguridad de la información.	**MADUREZ** Inexistente
A.12.1.3	Gestión de capacidad	**Control:** Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.	**APLICA** **SI** / **NO** Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento, así como proyectar que responda a las necesidades de la organización a largo plazo. **IMPLEMENTA** **SI** / **NO** Se les realiza un monitoreo continuo a los recursos y la adquisición de nuevos se proyecta de acuerdo a las necesidades críticas de la organización.	**NIVEL DE MADUREZ** Repetible
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**Control:** Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**APLICA** **SI** / **NO** La separación de ambientes de desarrollo y pruebas reduce el riesgo de operaciones no autorizadas. **IMPLEMENTA** **SI** / **NO** Los ambientes de salones de clase y las oficinas de administrativos están separados.	**NIVEL DE MADUREZ** Repetible
A.12.2	**Protección contra códigos maliciosos**			

<table>
<tr><td colspan="5">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</td></tr>
<tr><td rowspan="5">A.12.2.1</td><td rowspan="5">Controles contra códigos maliciosos</td><td rowspan="5">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</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El malware o software malicioso es un riesgo potencial para los sistemas y equipos, ya que pueden hacer que los sistemas operen de forma ineficiente, captura ilegal de información confidencial y borrado total.
IMPLEMENTA
SI | NO</td><td rowspan="3">Repetible</td></tr>
<tr><td>Aunque no existe una política claramente definida contra el malware, los usuarios son conscientes de los efectos nefastos que éstos podrían tener sobre el sistema y/o información. De igual forma, se mantienen los equipos actualizados y con software antivirus ejecutándose donde son monitoreados continuamente.</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>A.12.3</td><td colspan="4">Copias de respaldo</td></tr>
<tr><td colspan="5">Objetivo: Proteger contra la pérdida de datos.</td></tr>
<tr><td rowspan="4">A.12.3.1</td><td rowspan="4">Respaldo de la información</td><td rowspan="4">Control: Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las copias de seguridad (backups) e imágenes de los sistemas garantizan que la información esencial e instalación de software podría ser recuperada después de fallas o desastres.
IMPLEMENTA
SI | NO</td><td rowspan="2">Repetible</td></tr>
<tr><td></td></tr>
</table>

			Las copias de seguridad se realizan regularmente de forma manual.	
A.12.4	**Registro y seguimiento**			
Objetivo: Registrar eventos y generar evidencia.				
A.12.4.1	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.	**APLICA** **SI** / **NO** Los registros (logs) almacenan información relevante sobre los eventos ocurridos en la operación de un sistema. **IMPLEMENTA** **SI** / **NO** No se revisan ni se mantienen los registros de los eventos ocurridos en los sistemas.	**NIVEL DE MADUREZ** Inexistente
A.12.4.2	Protección de la información de registro	**Control:** Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**APLICA** **SI** / **NO** Los registros de eventos deberían ser custodiados para prevenir modificación no autorizada. **IMPLEMENTA** **SI** / **NO** Los registros de eventos están protegidos contra el acceso no autorizado.	**NIVEL DE MADUREZ** Repetible
A.12.4.3	Registros del administrador y del operador	**Control:** Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	**APLICA** **SI** / **NO** Los administradores tienen accesos privilegiados y podrían modificar información de los registros de eventos. **IMPLEMENTA** **SI** / **NO** Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.	**NIVEL DE MADUREZ** Repetible
A.12.4.4	Sincronización	**Control:** Los	**APLICA**	**NIVEL DE**

	de relojes	relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**SI**	**NO**	**MADUREZ**
			La sincronización de los relojes de los sistemas permite mantener una referencia única de tiempo y zona horaria.		Repetible
			IMPLEMENTA		
			SI	**NO**	
			Aunque no existe una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.		
A.12.5	**Registro y seguimiento**				
Objetivo: Asegurarse de la integridad de los sistemas operacionales.					
A.12.5.1	Instalación de software en los sistemas operativos	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	
			Se debería controlar las instalaciones de software en los sistemas operativos.		Repetible
			IMPLEMENTA		
			SI	**NO**	
			No existe una política documentada o procedimientos sobre la instalación de software en los sistemas operativos.		
A.12.6	**Gestión de la vulnerabilidad técnica**				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.					
A.12.6.1	Gestión de las vulnerabilidades técnicas	**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	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	
			El inventario de los activos se debería mantener actualizado con el fin de identificar a tiempo los riesgos asociados a las vulnerabilidades y amenazas técnicas.		Inexistente
			IMPLEMENTA		
			SI	**NO**	

		estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Aunque existe un inventario de los activos físicos y del software operacional, no se tiene una metodología de riesgos que los evalúe.	
A.12.6.2	Restricciones sobre la instalación de software	**Control:** Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	**APLICA** **SI** / **NO** Cualquier persona con elevados privilegios de acceso podría instalar cualquier software en un equipo y/o dispositivo. El no control podría liderar a la instalación de software malicioso o no permitido. **IMPLEMENTA** **SI** / **NO** Los equipos de las oficinas como los de las aulas de clase tienen todos los privilegios para La instalación de software.	**NIVEL DE MADUREZ** Inexistente
A.12.7	**Consideraciones sobre auditorías de sistemas de información**			
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.				
A.12.7.1	Controles de auditorías de sistemas de información	**Control:** Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	**APLICA** **SI** / **NO** Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos. **IMPLEMENTA** **SI** / **NO** No se tiene un plan de auditoría para la verificación de los sistemas operativos.	**NIVEL DE MADUREZ** Inexistente

Fuente: Esta investigación

Tabla 57. Verificación Controles de Seguridad De Las Comunicaciones

<table>
<tr><td>A.13</td><td colspan="4">SEGURIDAD DE LAS COMUNICACIONES</td></tr>
<tr><td>A.13.1</td><td colspan="4">Gestión de la seguridad de las redes</td></tr>
<tr><td colspan="5">Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.</td></tr>
<tr><td rowspan="5">A.13.1.1</td><td rowspan="5">Controles de redes</td><td rowspan="5">Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td rowspan="4">Inexistente</td></tr>
<tr><td>Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.</td></tr>
<tr><td rowspan="5">A.13.1.2</td><td rowspan="5">Seguridad de los servicios de red</td><td rowspan="5">Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o contraten externamente.</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td rowspan="4">Inexistente</td></tr>
<tr><td>El acceso a la red de los proveedores de servicios de red debería ser controlado y monitoreado.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
El acceso a la red de los proveedores de servicio de red no es monitoreado y controlado.</td></tr>
<tr><td rowspan="2">A.13.1.3</td><td rowspan="2">Separación en las</td><td rowspan="2">Control: Los grupos de</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td></td></tr>
</table>

	redes	servicios de información, usuarios y sistemas de información se deben separar en las redes.	Los usuarios y servicios deberían estar separados lógicamente en unidades organizacionales o dominios, o a través de VLANS. **IMPLEMENTA** **SI** / **NO** No hay separación de usuarios y servicios a través de dominios y VLANS.	Inexistente
A.13.2	**Transferencia de información**			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y procedimientos de transferencia de información	**Control:** Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	**APLICA** **SI** / **NO** Los procedimientos y controles ayudan a mantener la seguridad de la información cuando es transferida a otra entidad. **IMPLEMENTA** **SI** / **NO** No existe una documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información.	**NIVEL DE MADUREZ** Inexistente
A.13.2.2	Acuerdos sobre transferencia de información	**Control:** Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	**APLICA** **SI** / **NO** Se deberían tener acuerdos sobre los procedimientos para la transferencia segura de la información. **IMPLEMENTA** **SI** / **NO** No se han implementado controles Criptográficos que garanticen la seguridad en la transmisión de la información.	**NIVEL DE MADUREZ** Inexistente
A.13.2.3	Mensajería	**Control:** Se debe	**APLICA**	**NIVEL DE**

	electrónica	proteger adecuadamente la información incluida en la mensajería electrónica.	**SI**	**NO**	**MADUREZ**
			Se deberían proteger los mensajes enviados internamente de los empleados de la organización.		Inexistente
			IMPLEMENTA		
			SI	**NO**	
			No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.		
A.13.2.4	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.	**APLICA**		**NIVEL DE MADUREZ**
			SI	**NO**	
			Los acuerdos con los empleados o con entes externos deberían tener acuerdos de confidencialidad de la información.		Repetible
			IMPLEMENTA		
			SI	**NO**	
			En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información		

Fuente: Esta investigación

Tabla 58. Verificación Controles De Adquisición, Desarrollo Y Mantenimiento De Sistemas

<table>
<tr><td>A.14</td><td colspan="4">ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS</td></tr>
<tr><td>A.14.1</td><td colspan="4">Requisitos de seguridad de los sistemas de información</td></tr>
<tr><td colspan="5">Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas.</td></tr>
<tr><td rowspan="5">A.14.1.1</td><td rowspan="5">Análisis y especificación de requisitos de seguridad de la información</td><td rowspan="5">Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.</td><td>APLICA</td><td rowspan="5">Repetible</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una política de seguridad de información que ayude a determinar la adquisición de los nuevos sistemas de información</td></tr>
<tr><td rowspan="5">A.14.1.2</td><td rowspan="5">Seguridad de servicios de las aplicaciones en redes públicas</td><td rowspan="5">Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.</td></tr>
<tr><td>A.14.1.3</td><td>Protección de</td><td>Control: La</td><td>APLICA</td><td>NIVEL DE</td></tr>
</table>

	las transacciones de los servicios de las aplicaciones	información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	**SI** / **NO** La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.	**MADUREZ** Inexistente
A.14.2	**Seguridad en los procesos de desarrollo y soporte**			
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	**Control:** Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	**APLICA** **SI** / **NO** Las políticas y controles de seguridad deberían ser aplicados en el desarrollo de software. **IMPLEMENTA** **SI** / **NO** No se desarrolla software.	**NIVEL DE MADUREZ** N/A
A.14.2.2	Procedimientos de control de cambios en sistemas	**Control:** Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	**APLICA** **SI** / **NO** El procedimiento formal de los cambios en el desarrollo de software debería ser documentado para garantizar la integridad del sistema o aplicación. **IMPLEMENTA** **SI** / **NO** No se desarrolla	**NIVEL DE MADUREZ** N/A

			software.	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**Control:** Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad de la organización.	**APLICA** **SI** / **NO** Los cambios en las aplicaciones deberían ser revisados y probados antes de implementarlas de manera que se garantice que no comprometa la seguridad. **IMPLEMENTA** **SI** / **NO** Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse por los proveedores de los sistemas de información.	**NIVEL DE MADUREZ** Gestionado
A.14.2.4	Restricciones en los cambios a los paquetes de software	**Control:** Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	**APLICA** **SI** / **NO** Limitar las modificaciones de software sólo a lo estrictamente necesario. **IMPLEMENTA** **SI** / **NO** Las actualizaciones y modificaciones de software son desarrolladas por los proveedores de los sistemas de información.	**NIVEL DE MADUREZ** Gestionado
A.14.2.5	Principios de construcción de los sistemas seguros	**Control:** Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad	**APLICA** **SI** / **NO** Se deberían establecer y documentar los principios de desarrollo de software seguro. **IMPLEMENTA** **SI** / **NO**	**NIVEL DE MADUREZ** N/A

		de implementación de sistemas de información.	No se desarrolla software.	
A.14.2.6	Ambiente de desarrollo seguro	**Control:** Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	**APLICA** **SI** / **NO** Los ambientes de desarrollo de software también deberían estar protegidos de acceso no autorizado o de ejecución de software malicioso. **IMPLEMENTA** **SI** / **NO** No se desarrolla software.	**NIVEL DE MADUREZ** N/A
A.14.2.7	Desarrollo contratado externamente	**Control:** La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	**APLICA** **SI** / **NO** El software desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros. **IMPLEMENTA** **SI** / **NO** Se asegura que el software desarrollado externamente contiene las prácticas de desarrollo y pruebas seguros.	**NIVEL DE MADUREZ** Inexistente
A.14.2.8	Pruebas de seguridad de sistemas	**Control:** Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	**APLICA** **SI** / **NO** Se deberían realizar visitas y pruebas de seguridad al software que se está desarrollando. **IMPLEMENTA** **SI** / **NO** No se realizan pruebas de seguridad al software durante su período de desarrollo.	**NIVEL DE MADUREZ** Inexistente

<table>
<tr><td rowspan="5">A.14.2.9</td><td rowspan="5">Pruebas de aceptación de sistemas</td><td rowspan="5">Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización.</td><td rowspan="3">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se realizan las pruebas de seguridad debido a que aún no existen los lineamientos o políticas de la seguridad de la información.</td></tr>
<tr><td>A.14.3</td><td colspan="5">Datos de prueba</td></tr>
<tr><td colspan="6">Objetivo: Asegurar la protección de los datos usados para pruebas.</td></tr>
<tr><td rowspan="5">A.14.3.1</td><td rowspan="5">Protección de datos de prueba</td><td rowspan="5">Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.</td><td colspan="2">APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial.</td><td rowspan="3">Inexistente</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.</td></tr>
</table>

Fuente: Esta investigación

Tabla 59. Verificación Controles de Relaciones Con Los Proveedores

<table>
<tr><td>A.15</td><td colspan="4">RELACIONES CON LOS PROVEEDORES</td></tr>
<tr><td>A.15.1</td><td colspan="4">Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="5">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</td></tr>
<tr><td rowspan="5">A.15.1.1</td><td rowspan="5">Política de seguridad de la información para las relaciones con proveedores</td><td rowspan="5">Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y se deben documentar.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>La organización debería emplear los controles y procedimientos de seguridad para el acceso a los activos por parte de los proveedores.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI / NO
No se tiene una política de seguridad definida.</td></tr>
<tr><td rowspan="5">A.15.1.2</td><td rowspan="5">Tratamiento de la seguridad dentro de los acuerdos con proveedores</td><td rowspan="5">Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.</td><td>APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI / NO
No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.</td></tr>
<tr><td rowspan="4">A.15.1.3</td><td rowspan="4">Cadena de suministro de tecnología de información y comunicación</td><td rowspan="4">Control: Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la</td><td>APLICA</td><td rowspan="4">Inexistente</td></tr>
<tr><td>SI / NO</td></tr>
<tr><td>Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información de la organización.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
</table>

		cadena de suministro de productos y servicios de tecnología de información y comunicación.	**SI** / **NO** No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.	
A.15.2	**Gestión de la prestación de servicios de proveedores**			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**Control:** Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.	**APLICA** **SI** / **NO** El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos.	**NIVEL DE MADUREZ** Inexistente
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**Control:** Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de	**APLICA** **SI** / **NO** Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos.	**NIVEL DE MADUREZ** Inexistente

		riesgos.		

Fuente: Esta investigación

Tabla 60. Verificación Controles de Gestión De Incidentes De Seguridad De La Información

A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**			
A.16.1	**Gestión de incidentes y mejoras de la seguridad de la información**			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A.16.1.1	Responsabilidades 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.	**APLICA** **SI** / **NO** Los planes y procedimientos para gestionar los incidentes relacionados a la seguridad de la información deberían estar documentados. **IMPLEMENTA** **SI** / **NO** No existen los procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.	**NIVEL DE MADUREZ** Inexistente
A.16.1.2	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.	**APLICA** **SI** / **NO** Todos los empleados deben estar pendientes de los eventos y reportes de seguridad de la información. **IMPLEMENTA** **SI** / **NO** Los empleados no están alertados de los eventos e incidentes correspondientes relativos a la seguridad	**NIVEL DE MADUREZ** Inexistente

			de la información.	
A.16.1.3	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.	**APLICA** **SI** / **NO** Se deberían implementar mecanismos de reportes de incidentes de seguridad de la información en donde todos los empleados deberían reportar las brechas de seguridad con el fin de prevenir incidentes. **IMPLEMENTA** **SI** / **NO** Los empleados saben reconocer adecuadamente las debilidades de seguridad de información por lo tanto lo reportan como caída del sistema.	**NIVEL DE MADUREZ** Inexistente
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Control:** Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	**APLICA** **SI** / **NO** La clasificación y priorización de los incidentes de seguridad ayudan a identificar el impacto en la organización. **IMPLEMENTA** **SI** / **NO** Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos.	**NIVEL DE MADUREZ** Inexistente
A.16.1.5	Respuesta a incidentes de	**Control:** Se debe dar respuesta a los	**APLICA** **SI** / **NO**	**NIVEL DE MADUREZ**

	seguridad de la información	incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Deberían existir procedimientos documentados para dar respuesta a los incidentes restableciendo la operación al nivel de seguridad aceptable lo más pronto posible. **IMPLEMENTA** **SI** / **NO** Los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio.	Inexistente
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**Control:** El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.	**APLICA** **SI** / **NO** Se debería recolectar información de los incidentes ocurridos con el fin de prevenirlos en el futuro. **IMPLEMENTA** **SI** / **NO** No se recolecta la información de los incidentes y en la mayoría de casos no se aplican los controles necesarios para prevenirlos.	**NIVEL DE MADUREZ** Inexistente
A.16.1.7	Recolección de evidencia	**Control:** La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**APLICA** **SI** / **NO** Se deberían recolectar las evidencias y registros para tomar acciones legales. **IMPLEMENTA** **SI** / **NO** No se almacena ninguna evidencia formalmente para emprender las acciones legales.	**NIVEL DE MADUREZ** Inexistente

Fuente: Esta investigación

Tabla 61. Verificación Controles de Aspectos De Seguridad De La Información De La Gestión De La Continuidad Del Negocio

<table>
<tr><td>A.17</td><td colspan="4">ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</td></tr>
<tr><td>A.17.1</td><td colspan="4">Continuidad de seguridad de la información</td></tr>
<tr><td colspan="5">Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.</td></tr>
<tr><td rowspan="5">A.17.1.1</td><td rowspan="5">Planificación de la continuidad de la seguridad de la información</td><td rowspan="5">Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.</td><td colspan="2">APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td rowspan="5">A.17.1.2</td><td rowspan="5">Implementación de la continuidad de la seguridad de la información</td><td rowspan="5">Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.</td><td colspan="2">APLICA</td><td rowspan="5">Inexistente</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

			IMPLEMENTA **SI** / **NO** No existe la documentación o los procedimientos para los BCP y DRP.	
A.17.1.3	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.	**APLICA** **SI** / **NO** Los procedimientos y controles para la restablecer los servicios se deberían revisar en intervalos regulares con cada uno de los responsables para verificar su efectividad. **IMPLEMENTA** **SI** / **NO** No existe la documentación o los procedimientos para los BCP y DRP.	**NIVEL DE MADUREZ** Inexistente
A.17.2	**Redundancias**			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	**Control:** Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	**APLICA** **SI** / **NO** La información debería ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares. **IMPLEMENTA** **SI** / **NO** La organización no dispone de redundancia de la información, que almacena los sistemas de información.	**NIVEL DE MADUREZ** Inexistente

Fuente: Esta investigación

Tabla 62. Verificación Controles de Cumplimiento

<table>
<tr><td>A.18</td><td colspan="4">CUMPLIMIENTO</td></tr>
<tr><td>A.18.1</td><td colspan="4">Cumplimiento de los requisitos legales y contractuales</td></tr>
<tr><td colspan="5">Objetivo: Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.</td></tr>
<tr><td rowspan="6">A.18.1.1</td><td rowspan="6">Identificación de la legislación aplicable a los requisitos contractuales</td><td rowspan="6">Control: Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los administradores deberían identificar toda la información legislativa aplicable a la organización con el fin de cumplir con los requerimientos del negocio.</td><td rowspan="4">Definido</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.</td></tr>
<tr><td rowspan="6">A.18.1.2</td><td rowspan="6">Derechos de propiedad intelectual</td><td rowspan="6">Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.</td><td>APLICA</td><td rowspan="2">NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Se deberían definir las políticas y procedimientos para controlar la propiedad intelectual.</td><td rowspan="4">N/A</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Se permite la instalación, copia y distribución de software sin licencia.</td></tr>
<tr><td>A.18.1.3</td><td>Protección de</td><td>Control: Los</td><td>APLICA</td><td>NIVEL DE</td></tr>
</table>

	registros	registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	**SI** / **NO** Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización de acuerdo al nivel de confidencialidad. **IMPLEMENTA** **SI** / **NO** No existe un nivel de clasificación formal de confidencialidad de los registros.	**MADUREZ** Inexistente
A.18.1.4	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 en la legislación y la reglamentación pertinentes, cuando sea aplicable.	**APLICA** **SI** / **NO** Se debería documentar y definir políticas relativas a la protección de datos personales de acuerdo a las reglamentaciones que la ley exige. **IMPLEMENTA** **SI** / **NO** No existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley.	**NIVEL DE MADUREZ** Inexistente
A.18.1.5	Reglamentación de controles criptográficos	**Control:** Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	**APLICA** **SI** / **NO** Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida y/o almacenada sea segura.	**NIVEL DE MADUREZ** Inexistente

<table>
<tr><td>A.18.2</td><td colspan="4">Revisiones de seguridad de la información</td></tr>
<tr><td colspan="5">Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.</td></tr>
<tr><td rowspan="4">A.18.2.1</td><td rowspan="4">Revisión independiente de la seguridad de la información</td><td rowspan="4">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 información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td rowspan="4">Inexistente</td></tr>
<tr><td>Se deberían realizar auditorías de los procesos, procedimientos y sistemas por medio de entidades externas.
IMPLEMENTA
SI | NO</td></tr>
<tr><td>No se realizan auditorías con entidades externas.</td></tr>
<tr><td rowspan="4">A.18.2.2</td><td rowspan="4">Cumplimiento con las políticas y normas de seguridad</td><td rowspan="4">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.</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td rowspan="4">Inexistente</td></tr>
<tr><td>Se deberían realizar revisiones de las políticas de seguridad con el fin de verificar su cumplimiento.
IMPLEMENTA
SI | NO</td></tr>
<tr><td>No existen políticas de la seguridad de la información con la cual se permitan comparar los resultados.</td></tr>
<tr><td rowspan="2">A.18.2.3</td><td rowspan="2">Revisión del cumplimiento</td><td rowspan="2">Control: Los sistemas de</td><td>APLICA</td><td>NIVEL DE MADUREZ</td></tr>
<tr><td>SI | NO</td><td></td></tr>
</table>

	técnico	información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de información.	Los test de penetración deben ser realizados por con herramientas automáticas, con personal calificado y en intervalos programados y acordados con el fin de verificar las políticas de seguridad así como los requerimientos. **IMPLEMENTA** **SI** / **NO** No se aplica ningún test de penetración, ni mucho menos hay políticas de seguridad o metodología de riesgo que permita comparar los resultados.	Inexistente

Fuente: Esta investigación

3.4. POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.4.1. Actividad 11. Definición de las políticas de seguridad informática.

El objetivo de este documento es establecer las políticas en seguridad de la información del CETEM, con el fin de mejorar la gestión de la seguridad de la información al interior de la entidad.

Las Documento completo de Políticas de Seguridad se describen en el ANEXO H – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE ESTUDIOS EMSSANAR CETEM, proporcionando instrucciones sobre cómo mantener más seguros la plataforma tecnológica del CETEM. La violación de dichas políticas puede conducir medidas disciplinarias dependiendo de la gravedad de los incidentes de seguridad que puedan ocasionar.

Entre las políticas más importantes podemos mencionar:

3.4.1.1. **Política de acceso a redes y recursos de red**

La COMITÉ DE SEGURIDAD DE LA INFORMACION Y AREA DE REDES Y SISTEMAS del CETEM, como responsables de la plataforma tecnológica del CETEM, suministrará los mecanismos necesarios para proteger las redes y recursos de red, a través de mecanismos de control de acceso lógico y físico.

Normas de acceso a redes y recursos de red

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben establecer y verificar periódicamente los procesos de autorización y controles para proteger el acceso a la plataforma tecnológica del CETEM, con el fin de revisar que los usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios para los que fueron autorizados.
- Deben asegurar que las redes inalámbricas del centro de estudios cuenten con métodos de autenticación que evite accesos no autorizados y conceder

el acceso únicamente a los Funcionarios, Docentes, Estudiantes vinculados al CETEM actualmente y denegar en caso contrario.

Normas dirigidas a: TODOS LOS USUARIOS

- Se prohíbe conectar a los perfiles de red del CETEM equipos de cómputo incluyente dispositivos móviles de uso personal, salvo se solicite acceso al AREA DE REDES Y SISTEMAS.

3.4.1.2. **Política de administración de acceso de usuarios**

El CETEM establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a la plataforma tecnológica. Así mismo, velará porque los funcionarios, docente y estudiantes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores.

Normas de administración de acceso de usuarios

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben establecer y otorgar privilegios de administración de usuarios de la plataforma tecnológica del CETEM sólo a aquellos funcionarios designados para dichas funciones, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- Otorgar o revocar privilegios de acceso a las redes de datos, los recursos tecnológicos y los sistemas de información del CETEM de manera oportuna a los Funcionarios, Docente y Estudiantes de acuerdo a los perfiles establecidos.
- Deben definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica del CETEM; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

- Deben verificar periódicamente los privilegios de acceso concedidos tanto a Funcionarios, Docentes, Estudiantes sobre sus recursos tecnológicos y sistemas de información.

3.4.1.3. **Política de responsabilidades de acceso de los usuarios**

Los usuarios de la plataforma tecnológica del CETEM realizarán un uso adecuado y responsable de los recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica del CETEM deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros usuarios o ajenos.

3.4.1.4. **Política de controles criptográficos**

El CETEM velará porque la información del centro de estudios, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

Normas de controles criptográficos

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- Deben desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: FUNCIONARIOS

- Deben almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Normas dirigidas a: DESARROLLADORES EXTERNOS

- Deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por el AREA DE REDES Y SISTEMAS.

3.4.1.5. **Política de registro de eventos y monitoreo de la plataforma tecnológica**

El CETEM realizará monitoreo permanente del uso que dan los Funcionarios, Docentes, Estudiantes a la plataforma tecnológica del centro de estudios.

Normas de registro de eventos y monitoreo de la plataforma tecnológica

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben determinar y revisar periódicamente los registros (logs) de auditoria de la plataforma tecnológica del CETEM con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.
- Deben certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica del CETEM. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
- Deben determinar los periodos de retención de los registros (logs) de auditoria de la plataforma tecnológica del CETEM.

Normas dirigidas a: DESARROLLADORES EXTERNOS

- Deben presentar un informe que muestre los usuarios que han accedido a los sistemas de información de la plataforma tecnológica del CETEM, el horario y si es posible descripción general de las actividades.

3.4.1.6. **Política de gestión de vulnerabilidades**

El CETEM, a través del COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

Normas para la gestión de vulnerabilidades

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- Deben generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
- Deben revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- Deben generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- Deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

3.4.1.7. **Política de gestión y aseguramiento de las redes de datos**

El CETEM establecerá, a través del COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios de la plataforma tecnológica; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida del centro de estudios.

Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del CETEM.
- Deben implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- Deben mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios o cualquier otra tipificación que se considere conveniente para el centro de estudios.
- Deben establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del centro de estudios, acogiendo buenas prácticas de configuración segura.
- Deben identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el centro de estudios en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

- Deben instalar protección entre las redes internas del CETEM y cualquier red externa, que este fuera de la capacidad de control y administración del centro de estudios.
- Deben velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos del CETEM.

3.4.1.8. **Política de uso adecuado de internet**

El CETEM consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en el centro de estudios.

Normas de uso adecuado de internet

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Deben proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- Deben diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- Deben monitorear continuamente el canal del servicio de Internet.
- Deben establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- Deben generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- Deben generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las

precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet del CETEM deben hacer uso del mismo en relación al rol que desempeñen (funcionarios, Docentes y Estudiantes) con el objetivo de cumplir con los propósitos del negocio.
- Los usuarios del servicio de Internet deben evitar la descarga de software, información audiovisual desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles del centro de estudios a menos se para actividades propias del centro de estudios.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, redes sociales, mensajería, descarga de software, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o bien para fines diferentes a las actividades propias del centro de estudios.
- No está permitida la descarga e intercambio no autorizado de información de propiedad del CETEM.

3.4.1.9. **Política de intercambio de información**

El CETEM asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. El centro de estudios propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Normas de intercambio de información

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION Y EL AREA DE REDES Y SISTEMAS

- Junto con el grupo de Contratación, establecer en los contratos que a realizar con terceras partes, los Acuerdos de Confidencialidad y/o de Intercambio de Información incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se Deben incluir la prohibición de divulgar la información entregada por el CETEM a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- Deben definir, establecer y autorizar el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación del CETEM, reciben o envían información de los beneficiarios del centro de estudios, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- Deben ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: FUNCIONARIOS

- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros sea autorizada previamente y deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DEL CETEM

- Los terceros con quienes se intercambia información del CETEM deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad del centro de estudios, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.
- Los terceros con quienes se intercambia información del centro de estudios deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS:

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible del centro de estudios o de sus beneficiarios.
- No está permitido el intercambio de información sensible del centro de estudios por vía telefónica.

4. CONCLUSIONES

El SGSI diseñado incluye en los anexos un inventario de los activos de información, en los que se estipulan el valor de los activos, su clasificación y sus responsables. De igual manera se realizó satisfactoriamente un proceso de análisis y evaluación de riesgos utilizando la metodología de análisis de riesgos MAGERIT, en el cual esta discriminado por cada activo, indicando los tipos de amenazas a los que se encuentran sometidos cada uno de ellos junto con el riesgo actual y las vulnerabilidades presentes en la actualidad como resultado de un test de penetración básico. Sin ser menos importante también permitió conocer de manera más exacta el estado actual de la seguridad informática de la red de datos del CETEM y dar a conocer al AREA DE REDES Y SISTEMAS los riesgos a los que está sometida la información que circula por su Plataforma Tecnológica.

Se realizó de igual manera una verificación de los controles implementados y los que faltan implementar en el CETEM teniendo como referencia la norma ISO/IEC 27002:2013 con el fin de determinar su respectivo nivel de madurez en la escala del COBIT.

Se realizó un documento de políticas de seguridad basado en los controles establecidos en la norma ISO/IEC 27002 y teniendo en cuenta los resultados obtenidos en todo el proceso diagnóstico del CETEM en temas de seguridad de la de la red de dato, logrando así un SGSI acorde a las necesidades y requerimientos propios y así dar el primer paso una posible certificación en ISO/IEC 27001:2013.

La adopción del SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS DEL CENTRO DE ESTUDIOS EMSSANAR CETEM permitirá mejorar la administración de la calidad y la confiabilidad de la infraestructura tecnológica de red y responder a un creciente número de requerimientos regulatorios y

contractuales en un futuro cercano necesarios para alcanzar los objetivos de negocio ya que es dinámico y fácilmente adaptable a los cambios.

5. RECOMENDACIONES

Acondicionar el entorno físico donde está ubicado actualmente el gabinete de red para que brinde un perímetro de seguridad que minimice el riesgo a los que se encuentran sometidos los equipos de la red de datos del CETEM.

Realizar una nueva distribución de direcciones IP por subredes como se muestra en la Tabla 46 preferiblemente asignadas por un servidor DHCP[20] y su respectiva restricción de sitios Web a través de un servidor proxy.

Tabla 63. Distribución de direcciones IP por subredes

Subred	Dirección de Red	Inicio de Host	Fin de Host	Broadcast
Aula 201	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
Aula 202	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
Aula 203	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
Aula 204	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
Aula 208	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
Estudiantes	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
Visitantes	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
Administrativos	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255

Fuente: Esta investigación

La implementación de un firewall físico o de un servidor destinado con este propósito para implementar los controles lógicos frente a ataques dirigidos por parte de personal externo a la institución con el fin de resguardar adecuadamente la información almacenada en los servidores de forma lógica.

En el aspecto lógico se detectaron vulnerabilidades en cuanto al acceso y configuración de dispositivos de red, por lo cual se recomienda de carácter

[20] DHCP (siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres

urgente proteger el acceso a estos dispositivos con contraseñas robustas, con el fin de evitar que el acceso a estos ocasione denegación de algún servicio.

Con respecto a los aplicativos y plataformas web implementadas por el AREA DE REDES Y SISTEMAS, la más preocupante y critica es la de inyección SQL, mediante la cual se puede analizar e identificar la estructura de las bases de datos implementadas en estos aplicativos web, para lo cual se recomienda de carácter urgente analizar e implementar controles en las entradas y salidas que generan los mismos, con el fin de evitar este tipo de ataques junto con los de cross site scripting.

Otra vulnerabilidad encontrada es la transferencia de formularios de inicio de sesión por texto plano, lo que permite obtener las credenciales de usuario y contraseña a través de un ataque de hombre en medio escuchando el tráfico de red, se recomienda para solventar esta vulnerabilidad implementar servicios de navegación con encriptamiento como lo es el HTTPS.

Difundir y poner en práctica las políticas a los empleados que intervienen con los activos de la información, a través de correo electrónico, charlas u otros medios con el fin de concientizarlos de la importancia de los archivos físicos así como la información generada, procesada, almacenada y transmitida a través de su plataforma tecnológica

Una recomendación específica es capacitar al personal del AREA DE REDES Y SISTEMAS en temas de seguridad de la información e incentivar el estar actualizados en temas relacionados con el fin de estar a la vanguardia de las nuevas vulnerabilidades y tipos de ataques utilizados.

Realizar periódicamente análisis de riesgos y monitorear frecuente los activos de información, pues la seguridad que se va a proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo.

Encargar a más personas de la seguridad informática de la institución ya que la actualidad el único encargado es el auxiliar de soporte y mantenimiento, el cual se encargar tiene otras funciones aparte de esta.

Considerar al SGSI propuesto como un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.

BIBLIOGRAFÍA

Administración Nacional de Usinas y Trasmisiones Eléctricas (Uruguay). (45 de 03 de 2016). *Política De Seguridad De La Información.* Obtenido de Política De Seguridad De La Información: http://www.ute.com.uy/compras/normativa/PSeguridad_2014.pdf

Corporación Peruana de Aeropuertos y Aviación Comercial. (15 de 04 de 2016). *Políticas De Seguiridad En El Uso De Dispositivos Móviles.* Obtenido de Políticas De Seguiridad En El Uso De Dispositivos Móviles: http://www.corpac.gob.pe/Docs/Transparencia/OyM/DocNormativos/Politicas/Seguridad_Uso_Dispositivos_Moviles_Ver1_(GG-0620-2011-M_12-12-2011).pdf

Departamento Administrativo de la Función Pública (DAFP). (20 de 03 de 2016). *Guía para la administración del riesgo*. Obtenido de Guía para la administración del riesgo: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

DIRECCIÓN GENERAL MARITIMA. (09 de 07 de 2016). *Política Seguridad En La Informatica Y Fisica.* Obtenido de Política Seguridad En La Informatica Y Fisica: https://www.dimar.mil.co/sites/default/files/atach/politica_seguridad.pdf

Emssanar. (04 de 04 de 2015). *Centro de Estudios EMSSANAR CETEM*. Obtenido de Centro de Estudios EMSSANAR CETEM: http://www.emssanar.org.co/contenidos/cetem/portafolio_de_servicios/portafolio_cetem.pdf

ICETEX. (10 de 9 de 2016). *Manual De Políticas De Seguridad De La Información.* Obtenido de Manual De Políticas De Seguridad De La Información: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

Implementación efectiva de un SGSI ISO 27001. (22 de 05 de 2015). Obtenido de Implementación efectiva de un SGSI ISO 27001:

http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

Incoder. (12 de 09 de 2016). *Política De Seguridad De La Información.* Obtenido de Política De Seguridad De La Información: http://www.incoder.gov.co/documentos/A%C3%91O_2014/Gestion_Incoder/Politicas/Agosto_15/PoliticadeSeguridaddelaInformacion.pdf

ISO/IEC 27002:2013. (04 de 04 de 215). *Information Technology - Security techniques – Code of practice for security management*. Obtenido de Information Technology - Security techniques – Code of practice for security management: http://inicio.ifai.org.mx/DocumentosdeInteres/4-2_ISO-IEC_27002-2013.pdf

Iso27002.Es. (04 de 04 de 2015). *10 6 Gestión de redes*. Obtenido de 10 6 Gestión de redes: http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf

Iso27002.Wiki.Zoho.Com. (04 de 04 de 2015). *10. Gestión de Comunicaciones y Operaciones*. Obtenido de 10. Gestión de Comunicaciones y Operaciones: https://iso27002.wiki.zoho.com/10ComunicacionesyOperaciones.html

Javeriana - Centro de escritura. (04 de 04 de 2015). *Norma ICONTEC*. Obtenido de Norma ICONTEC: http://centrodeescritura.javerianacali.edu.co/index.php?option=com_content&view=article&id=84:norma-icontec&catid=45:referencias-bibliograficas&Itemid=66

Lamilla Rubio, E. A., Patiño Sánchez , J. R., & Martín M. , I. (04 de 04 de 2015). *Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil*. Obtenido de Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil:

https://www.dspace.espol.edu.ec/bitstream/123456789/5247/1/Desarrollo%20de%20Pol%C3%ADticas%20de%20Seguridad%20Inform%C3%A1tica%20e%20Implementaci%C3%B3n.pdf

Redseguridad.Com. (04 de 04 de 2015). *¿Sabes diferenciar la ISO 27001 y la ISO 27002?* Obtenido de ¿Sabes diferenciar la ISO 27001 y la ISO 27002?: http://www.redseguridad.com/opinion/articulos/sabes-diferenciar-la-iso-27001-y-la-iso-27002

UDISTRITAL. (24 de 08 de 2016). *Politica para Seguridad Informacion.* Obtenido de Politica para Seguridad Informacion: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

UNAD. (25 de 05 de 2015). *Proyecto De Seguridad Informática Ii*. Obtenido de Proyecto De Seguridad Informática Ii: ftp://201.236.222.3/publico/Jrivera/Proyecto%20de%20Seguridad%20Informatica%202%20(233013_10)/00%20Protocolo%20y%20Modulo/Anterior/233013_Proyecto%20de%20Seguridad%20Inform%E1tica%20II.pdf

UNAD. (06 de 05 de 2016). *Politicas Marco de Referencia SGSI.* Obtenido de Politicas Marco de Referencia SGSI: https://gidt.unad.edu.co/images/Documentos/20150303%20-%20Resolucin%204256%20-%20Polticas%20Marco%20de%20Referencia%20del%20SGSI.pdf

Universidad Nacional de Cordoba (Argentina). (23 de 04 de 2016). *Politicas de Seguridad de la Información para la UNC.* Obtenido de Politicas de Seguridad de la Información para la UNC: http://www.unc.edu.ar/gestion/unidades/direccion-operativa/concursos/dgti/00003-08.pdf

Wikipedia.Org. (04 de 04 de 2015). *Iso/Iec 27002*. Obtenido de iso/iec 27002: http://es.wikipedia.org/wiki/ISO/IEC_27002