DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA INSTITUCIÓN EDUTEC DE LOS ANDES PITALITO, ARGUMENTADA EN LA NORMA ISO/IEC 27001

JASMIN EMILSE CUELLAR CASTRILLÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO, HUILA
2020

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA INSTITUCIÓN EDUTEC DE LOS ANDES PITALITO, ARGUMENTADA EN LA NORMA ISO/IEC 27001

JASMIN EMILSE CUELLAR CASTRILLÓN

Trabajo de grado presentado como requisito parcial para optar al título de especialista en Seguridad Informática

Director
Anívar Chaves Torres
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO, HUILA
2020

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Pitalito, 29 de mayo de 2020

Dedico este logro a Dios por su infinita misericordia y a mi familia por todo su amor, comprensión y apoyo para alcanzar las metas que me he propuesto.

Jasmin Emilse Cuellar Castrillón

AGRADECIMIENTOS

A mi amado esposo, hijos y familia por todo su amor, comprensión y apoyo.
Al Ingeniero Anivar Chaves Torres, por su apoyo, enseñanzas y paciencia, como asesor del proyecto.
A la Universidad Abierta y a Distancia UNAD por proporcionarme los conocimientos propios de la Especialización en Seguridad Informática.
Al Instituto Edutec de los Andes Pitalito, en cabeza de su Director General, Ing. Diógenes Motta Hernández, por permitirme realizar este trabajo de grado con datos reales que hacen parte de la información sensible y valiosa que maneja la Entidad, con el propósito de elaborar el Diseño de un Sistema de Gestión de Seguridad de la Información.

CONTENIDO

Pág.

LISTA DE CUADROS

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

GLOSARIO

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

AMENAZA: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

BOTNET: o red de *bots* (también conocida como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker. Al tomar el control de cientos o miles de equipos, las *botnets* se suelen utilizar para enviar *spam* o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (*DDoS*).

DATOS: es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo. Los datos son el corazón que permite a una organización prestar sus servicios.

INCIDENTE DE SEGURIDAD: se presenta cuando una amenaza o un conjunto de amenazas suceden y aprovecha una vulnerabilidad.

NO REPUDIO: este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo. Este servicio es muy importante en las transacciones comerciales por Internet, ya que incrementa la confianza entre las partes en las comunicaciones.

ÓBICE: obstáculo o impedimento para algo.

POLITICAS DE SEGURIDAD: son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa.

RED WIFI: red que cumple con el estándar internacional 802.11, que define las características de una red de área local inalámbrica (WLAN). Los dispositivos certificados por la Wi-Fi Alliance, pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso[1].

RIESGO: la noción de riesgo suele utilizarse como sinónimo de peligro. El riesgo, sin embargo, está vinculado a la vulnerabilidad, mientras que el peligro aparece asociado a la factibilidad del perjuicio o daño. Es posible distinguir, por lo tanto, entre

[1] CCM - Introducción a WIFI (802.11 o WiFi). https://es.ccm.net/contents/789-introduccion-a-wifi-802-11-o-wifi.

riesgo (la posibilidad de daño) y peligro (la probabilidad de accidente o patología). En otras palabras, el peligro es una causa del riesgo.

SALVAGUARDA: imperativo, singular, 3ª persona singular del presente de indicativo, Acción utilizada con el fin de proteger la información. Se utiliza como mecanismo de defensa, permitiendo de una manera más segura y organizada determinar cuál es la información de más valor en la empresa y si llegara a presentarse un daño o error permitir recuperar los datos que se creían perdidos.

SEGURIDAD DE LA INFORMACIÓN: la seguridad de la información pasa por la integridad, la disponibilidad, la confidencialidad y la auditoria como pilares básicos para la seguridad de los sistemas informáticos. Para las empresas dicha seguridad es muy importante, por eso en el mercado existen diferentes soluciones para un mantenimiento informático que asegure la preparación de los sistemas ante posibles eventualidades que puedan afectar al crecimiento de una empresa.

SEGURIDAD INFORMÁTICA: permite asegurarse que los recursos del sistema se utilizan de la manera en la que se espera y que quienes puedan acceder a la información que en él se encuentran sean las personas acreditadas para hacerlo.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: conjunto de políticas de administración de la información. Con un SGSI, la institución conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente[2].

[2] DE PABLOS HEREDERO, Carmen. LÓPEZ HERMOSO AGIUS, José Joaquín. Organización y transformación de los sistemas de información en la empresa. https://books.google.com.co/books?id=2pqwKkqxxosC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

SISTEMA DE INFORMACIÓN: sistema es la unión de varios elementos que se relación entre sí, logrando un mismo objetivo[3]. Es un modelo formado por elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y unos objetivos que satisfaga las necesidades de la empresa.

TRAZABILIDAD: serie de procedimientos que permiten seguir el proceso de evolución de un producto en cada una de sus etapas.

VIRUS: es un programa informático diseñado para infectar archivos. Además, algunos podrían ocasionar efectos molestos, destructivos e incluso irreparables en los sistemas sin el consentimiento o conocimiento del usuario.

VULNERABILIDAD: está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

[3] FERNANDEZ ALARCÓN, Vicenc. Desarrollo de sistemas de información. Una metodología basada en el modelado. Ediciones UPC. 2006. https://books.google.com.co/books?id=Sqm7jNZS_L0C&pg=PA86&lpg=PA86&dq=FERNANDEZ+ALARCÓN,+Vicenc.+Desarrollo+de+sistemas+de+información.+Una+metodología+basada+en+el+modelado.

INTRODUCCIÓN

Las empresas tienen información importante y sensible para su uso, que ayudan al correcto funcionamiento y cumplimiento de los objetivos trazados para la actividad y el buen desarrollo de la misma; que sin importar su tamaño o actividad, diariamente se enfrentan a innumerables amenazas y riesgos que proceden de una amplia variedad de incidentes que afectan la información procesada y almacenada en los equipos de información y esta a su vez perjudica la reputación y buen nombre de la organización.

Las organizaciones tienen que enfrentar la realidad no solamente de los ataques externos, sino de los internos ya que no pueden subestimar las amenazas o malware diseñado por ciberdelincuentes para causar daño o perjuicio. Por esto, es necesario que cuenten con un Sistema de Gestión de Seguridad de la Información que contribuya a mitigar los riesgos.

En EDUTEC se presentan eventos de pérdida de información en los equipos de cómputo que se encuentran en las aulas de clase, como en los de las dependencias administrativas y en la información de las memorias USB (Universal Serial Bus) que estudiantes y docentes utilizan para su uso personal y académico, para prevenir esta fuga de información, se requiere de la implementación de un DLP (Data Loss Prevention), sistema de prevención de pérdida de datos[4].

Por tal motivo se propuso diseñar un Sistema de Gestión de Seguridad de la información que permitiera identificar los riesgos y proponer políticas y controles

[4] INBEST.SOLUTIONS. ¿Qué es un DLP? Disponible en: https://content.inbest.solutions/ebook-que-es-un-dlp.

que mejoren la seguridad de la información en la institución, para ello se utilizó la metodología Magerit de análisis y gestión de riesgos de los sistemas de información.

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para el Instituto EDUTEC, permitió conocer los Riesgos a los que está sometida la información, ayudando a manejar, controlar e implementar estrategias para un correcto funcionamiento, todo esto con el apoyo de sus directivas que ayudan a incentivar a los involucrados a un buen manejo y aplicación de los sistemas implementando políticas, procedimientos y métodos con el fin de salvaguardar los principios de la Seguridad, Confidencialidad, Integridad y Disponibilidad.

1. PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN

Actualmente la gran mayoría de empresas utilizan Internet para promocionar sus productos o servicios y algunas de ellas realizan operaciones comerciales a través de sus sitios web. Estas estrategias les permiten difundir información sobre su objeto social y facilitar la comunicación e interacción con sus clientes, al igual que con sus proveedores y con el personal de la empresa. Sin embargo, los beneficios de la era digital acarrean también una serie de riesgos e inconvenientes que pueden afectar el desarrollo de las actividades y generar grandes pérdidas si no se cuenta con los mecanismos de control adecuados, como afirma Giménez[5], mientras los usuarios hacen uso de Internet y sus servicios, otras personas mal intencionadas desarrollan estrategias para acceder de forma ilegal a la información y a los recursos depositados en la red, como un ladrón que diseña planes para entrar ilegalmente a una propiedad ajena, los ciberdelincuentes desarrollan programas maliciosos y virus para aprovechar las vulnerabilidades de los sistemas en la web.

Es por esto que las empresas, entidades o instituciones sin importar su tamaño, su ubicación o sus actividades, necesitan tomar medidas de seguridad para proteger su información y sus activos informáticos, y de esta forma evitar eventos que afecten sus actividades o su economía. Para ello, como lo mencionan Gómez y Álvarez[6], existen normas aplicables a los sistemas de gestión, como la ISO 27001, que ayudan a corregir vulnerabilidades y a mitigar los riesgos.

---

[5] GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3), IC Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184155.

[6] GÓMEZ FERNÁNDEZ, Luis, ÁLVAREZ, Ana Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3205110.

El operador de telefonía móvil en Estados Unidos Verizon[7] público el informe "Mientras los hackers mejoran en ofensiva, las empresas desmejoran en defensa", dónde evidencia la problemática diaria que viven miles de empresas en cuanto a seguridad informática, algunos de los hallazgos del estudio, son que hubo 63.437 incidentes los cuales los hackers rompieron los sistemas de seguridad de las empresas, de esos incidentes 1.367 hicieron levantamiento de datos de usuarios.

Los hackers cada vez se organizan mejor, "grupos de delincuencia organizada" y cada vez más rápido logran entrar a los sistemas de las organizaciones, en cuestión de días y horas, en cambio las empresas no se observa el mismo panorama, y se les dificulta identificar cuando sus sistemas están comprometidos.

El 92% de todas las infracciones están relacionadas con nueve tipos de ataques, por ejemplo, los ataques dirigidos a minoristas tienen como objetivo el sistema de punto de venta.

Las empresas que identifican que tipo de ataques les afecta, les permite hacer un plan de juego eficiente, así como identificar qué tipo de hackers pueden estar interesados en la información que maneja la empresa. Es difícil tener una estrategia sino se está seguro de lo que se está tratando de proteger.

Este informe concluye que el año 2013 fue el año de "Una violación Menor" respecto a los años anteriores, sin embargo, fue un año de transición hacia ataques geopolíticos a gran escala a los ataques de sistemas de pago de tarjetas bancarias, y muestran como en años anteriores se relacionaron diferentes informes de ataques quienes sus actores eran patrocinados por el mismo Estado. Colombia no fue ajeno

[7] DERECHO INFORMÁTICO - SEGURIDAD INFORMÁTICA: Mientras los hackers mejoran en ofensiva, las empresas desmejoran en defensa. Disponible en: https://derechoinformatico.co/seguridad-informatica-mientras-los-hackers-mejoran-en-ofensiva-las-empresas-desmejoran-en-defensa/.

a esta tendencia, con las interceptaciones al grupo negociador del acuerdo de paz en la Habana, así como significativas cadenas minoristas sufrieron ataques en sus puntos de pago, y como empresas importantes de la industria TIC sufrieron la violación de datos personales de directivos importantes de esas organizaciones.

Los principales ataques informáticos según este estudio, son la clonación de tarjetas de crédito, intrusiones en el punto de venta, ataques en aplicaciones web, uso indebido de información privilegiada y ciberespionaje. Por todo esto es que todo el personal de la empresa debe trabajar en conjunto para mejorar en defender la seguridad y continuidad del negocio.

Por tal razón este trabajo se enfoca en la necesidad de seguridad de la información evidenciada en EDUTEC, Institución que no es ajena a la realidad que viven las empresas hoy en día, frente a la gran cantidad de amenazas y riesgos informáticos que pueden afectar su buen nombre y su funcionamiento.

En EDUTEC se han presentado eventos de pérdida de información en los equipos informáticos que se encuentran en las aulas, como en los de las dependencias administrativas. En algunos equipos se ha evidenciado la presencia de virus informáticos y se han reportado casos de daño irreversible en medios de almacenamiento externos usados en los equipos.

Para contrarrestar dichos daños se propone adquirir un DLP (*Data Loss Prevention*), que es un conjunto de tecnologías que previenen la fuga o robo de información en las organizaciones, esta herramienta alerta al usuario antes de que se produzcan eventos que atenten contra la confidencialidad o las políticas de seguridad que tiene la Institución, concientizando a los empleados que deben tener buenas prácticas en su puesto de trabajo, insertadas en los controles de seguridad de la norma ISO/IEC 27002.

Dentro de los problemas que actualmente se presentan más en las empresas están las fugas accidentales, empleados maliciosos, entre otros; por lo que deben contar con una solución adecuada que ayude a proteger y respaldar sus datos.

Los DLP previenen la perdida de datos, monitorizan redes y dispositivos móviles Android e IOS, comprueban a que correos se ha accedido, deteniendo la transmisión de datos confidenciales de la organización a aplicaciones de almacenamiento en la nube o redes sociales, incorpora plantillas pre configuradas según normas o estándares como RGPD (Reglamento general de protección de datos), LPI (Ley de propiedad intelectual), LSSI-ICE (Ley 34 del 11-07-2002 servicios de la sociedad de la información y del comercio electrónico), PCI-DSS (*Payment Card Industry Data Security Standard*- Estándar de seguridad de datos para la industria de tarjeta de pago).

Funciona como un antivirus en busca de patrones y firmas de la información que la empresa considera fundamental, distribuyéndose en la infraestructura informática de la empresa (equipos de cómputo, dispositivos de red), cubriendo así todos los puntos desde los que se pueden perder los datos.

La ventaja de tener tecnología DLP es que se puede elegir los archivos y datos que se van a analizar, para que en caso de presentarse alerta por robo de información, bloquee automáticamente la reproducción o el intento de querer compartirla.

Realiza búsquedas para detectar si la información ha sido duplicada o compartida, para saber la cantidad de veces que esto sucedió.

Controla quien tiene acceso a los datos, define el nivel de acceso del usuario mediante tecnología de gestión de derechos digitales.

Los beneficios de contar con un DLP en las empresas, sin importar si es pequeña o grande, van desde asegurar que los usuarios finales no envíen, ni impriman información sensible o critica fuera de la empresa.

Centralizar, gestionar y crear políticas que refuerzan los flujos de trabajo dedicados a la protección del contenido y los datos.

Auditar en tiempo real la distribución de la información corporativa por parte de los usuarios.

Proteger la información confidencial para que no pueda salir de los dispositivos ni a manera de transferencia, impresiones de pantalla, USB, correo electrónico, etc…

En el mercado existen empresas que ofrecen servicios profesiones de consultoría y productos especializados para la prevención de perdida de datos, creando soluciones a la medida de las políticas y regulaciones de cada organización.

Al indagar sobre el uso de los equipos se encontró que un mismo equipo puede ser utilizado por varios usuarios, quienes utilizan memorias USB para transportar sus archivos. Es común que los usuarios hagan uso de dispositivos de almacenamiento externo en distintos computadores para editar sus archivos y luego hagan uso de otro para imprimir. Esta forma de uso de los equipos y los dispositivos genera un riesgo de seguridad por cuanto en el evento de que un equipo se infecte con un virus, éste se replicará rápidamente a los demás equipos afectando a toda la institución.

Por tal razón se sugiere la implementación de un Active Directory (AD) o Directorio activo, ideal para gestionar el control de usuarios y un (GPO) control de acceso, que se encarga de vigilar las memorias USB.

El Active Directory (AD) es un servicio de directorio para su uso en un entorno Windows Server[8]. Se trata de una estructura de base de datos distribuida y jerárquica que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.

Active Directory es el servicio de directorio propietario de Microsoft para su uso en redes de dominio de Windows, cuenta con funciones de autenticación y autorización y proporciona un (framework) marco de referencia para otros servicios similares. Básicamente, el directorio consiste en una base de datos LDAP o Protocolo Ligero de Acceso a Directorio, que se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en la red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

El control de acceso dinámico basado en el dominio permite a los administradores aplicar permisos de control de acceso y restricciones de acuerdo a reglas bien definidas que pueden contemplar la confidencialidad de los recursos, el trabajo o el rol del usuario y la configuración del dispositivo que se usa para acceder a tales recursos.

[8] PAESSLER. ¿En qué consiste Active Directory? Disponible en: https://www.es.paessler.com/it-explained/active-directory.

Vanguardia[9] escribe un artículo sobre antivirus informático, que sirve de información para averiguar sobre las medidas de seguridad que se deben implementar en EDUTEC, donde se encontró que no se cuenta con un sistema de antivirus licenciado, ni gratuito, que cubra todas las necesidades de seguridad, siendo conscientes de que ningún sistema puede garantizar una completa seguridad a la información, pero si protege y evita daños. Los antivirus son programas informáticos creados para la prevención, bloqueo, detección y eliminación de ciertos archivos o ejecutables dañinos que se descargan en el ordenador, sin previo aviso, al navegar por internet.

En los equipos de las aulas de informática se utiliza el programa congelador *Deed Frezer* que conserva la configuración de los equipos, cualquier cambio, ya sea malicioso o accidental se revertirá, al ser reiniciado “Reiniciar para restaurar”, con este procedimientos se eliminan todos los archivos en el momento de apagar el equipo; no obstante, durante el tiempo que el computador está encendido puede almacenar y difundir archivos dañinos.

Por otra parte, se encontró que la institución no cuenta con una política de auditoría o evaluación de la seguridad informática; no se ha llevado a cabo un programa de capacitación y sensibilización sobre seguridad informática con los usuarios de los equipos para que hagan uso más seguro de los mismos y no se cuenta con un manual de buenas prácticas o con políticas y controles de seguridad de la información.

[9] VANGUARDIA. ¿Qué es un antivirus informático? TECH 29 dic 2018. https://vanguardia.com.mx/articulo/que-es-un-antivirus-y-para-que-sirve.

Ante las amenazas de virus, pérdida de información importante y sensible como es el caso de matrículas, notas de los estudiantes, informes para Secretaría de Educación y todos los procesos que se llevan a cabo por todos los actores, es una necesidad apremiante para la institución contar con un Sistema de Gestión de Seguridad de la Información (SGSI), que contribuya a disminuir los riesgos de pérdida o daño de los activos informáticos y de información. Las directivas y el encargado de esta área no contemplan la posibilidad de comprar o adquirir un antivirus para la Institución porque, según el encargado de mantenimiento es perder el tiempo porque para eso está instalado el congelador.

La Institución EDUTEC de los Andes Pitalito, no es ajena a la realidad que viven las empresas hoy en día, frente a la gran cantidad de amenazas y riesgos informáticos que pueden afectar su buen nombre y su funcionamiento. En la Institución se han presentado eventos de pérdida de información en los equipos informáticos que se encuentran tanto en los equipos que se encuentran en las aulas, como en los de las dependencias administrativas. En algunos equipos se ha evidenciado la presencia de virus informáticos y se han reportado casos de daño irreversible en medios de almacenamiento externos usados en los equipos. Al indagar sobre el uso de los equipos se encontró que un mismo equipo puede ser utilizado por varios usuarios, quienes utilizan memorias USB para transportar sus archivos. Es común que los usuarios hagan uso de dispositivos de almacenamiento externo en distintos computadores para editar sus archivos y luego hagan uso de otro para imprimir. Esta forma de uso de los equipos y los dispositivos genera un riesgo de seguridad por cuanto en el evento de que un equipo se infecte con un virus, éste se replicará rápidamente a los demás equipos afectando a toda la institución.

1.2 FORMULACIÓN

¿Cómo contribuir a mejorar la Seguridad de la información en el Instituto Edutec de los Andes Pitalito, mediante un Sistema de Gestión de Seguridad de la Información (SGSI) diseñado bajo la norma ISO/IEC 27001?

1.3. OBJETIVOS

1.3.1 Objetivo general

Diseñar un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001, para la Institución Edutec de los Andes Pitalito.

1.3.2 Objetivos específicos

- ✓ Elaborar un inventario de activos informáticos y de información de la Institución.
- ✓ Realizar un análisis de riesgo informático para EDUTEC.
- ✓ Proponer las políticas y controles de seguridad de la información y los activos informáticos.
- ✓ Diseñar un plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad contempladas en el SGSI

1.4. JUSTIFICACIÓN

Para EDUTEC, sede Pitalito, es necesario y muy importante implementar un sistema de gestión de seguridad de la información (SGSI) para contrarrestar las amenazas y vulnerabilidades que presenta el sistema y poder así tener un inventario actualizado de los Activos informáticos y de la información, para poder analizar los riesgo y proponer políticas y controles de seguridad de la información y de los activos informáticos.

Las mejoras en la seguridad de la información y de los activos informáticos tendrá un impacto importante en toda la institución, tanto en su rendimiento y su economía como en el bienestar de las personas que forman parte de ella, ya que la pérdida de información, el daño de un archivo o de un dispositivo de almacenamiento implica trabajo para recuperar la información o costo en la reposición del recurso, a la vez inconformidad por la falta de control en la seguridad de la información.

2. MARCO REFERENCIAL

2.1 ANTECEDENTES TEMÁTICOS

En el ámbito Internacional se han desarrollado investigaciones, utilizando como base la norma ISO/IEC 27001, con el fin de implementar un SGSI.

Luis Mora[10] presentó el proyecto Tratamiento de la gestión de riesgos de seguridad de información para el proceso de desarrollo de sistemas de empresa de soluciones informáticas, identificando los activos de información relevantes al proceso de desarrollo de software aplicando la norma ISO/IEC 27001, realizando un análisis de riesgos en función de las amenazas, vulnerabilidades y principios de seguridad.

De forma similar Yáñez[11] realizó la implementación de un sistema de gestión de seguridad de la información (SGSI) en la subsecretaría de economía y empresas de menor tamaño utilizando herramientas *open source* y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO27001:2013.

En el contexto Colombiano también se han adelantado investigaciones en diferentes empresas con el fin de incluir medidas de seguridad, mediante un sistema de

[10] Mora Torres, Luis Manuel. Tratamiento de la gestión de riesgos de seguridad de información para el proceso de desarrollo de sistemas de empresa de soluciones informáticas. Tesis Facultad de Ingeniería en Electricidad y Computación. Guayaquil-Ecuador: Escuela Superior Politécnica del Litoral (ESPOL). Facultad de Ingeniería en Electricidad y Computación. Disponible en: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/45960.

[11] Yáñez Cáceres, Nelson Alejandro. Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño. Tesis Magister en Tecnologías de la Información. Facultad de Ciencias Físicas y Matemáticas. Santiago de Chile: Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y.

gestión de seguridad informática (SGSI) y la metodología práctica para gestionar riesgos (Magerit).

García y Ortiz[12] realizaron una investigación descriptiva con el propósito de determinar y analizar los riesgos de seguridad de las aulas virtuales de la Universidad Santo Tomás en la modalidad presencial, según la norma ISO 27001:2013. Debido al alto grado de importancia que tiene en la Institución las aulas virtuales es necesario evaluar la seguridad y realizar controles para el acceso a dicha información sensible puesto que en esta se registran notas y trabajos de los estudiantes, como también se almacena todo el material de producción intelectual de los docentes, por lo que la perdida de este bien provocaría graves problemas a la universidad. Lo que se pretende con este diagnóstico del sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados. Se recomendó realizar acciones para reducir los riesgos y elaborar un plan de acción para mitigar los riesgos y el proceso de mejora continua. El aporte que esta investigación da al presente proyecto tiene que ver sobre el análisis que se debe realizar a los riesgos que puede tener o presentarse con la información importante que se maneja en las instituciones, según la norma ISO 27001:2013.

En la ciudad de Popayán, Restrepo[13] Jenny, ejecutó el diagnóstico del estado actual de la seguridad de la información, de la Institución Educativa Técnico Industrial, Sede Mercedes Pardo de la ciudad de Popayán, basado en la norma ISO

[12] GARCIA BALAGUERA, Vivian Andrea, ORTIZ GONZALEZ, Jhon Jarby. Análisis de Riesgos según la Norma ISO 27001:2013 para las Aulas Virtuales de la Universidad Santo Tomás, Modalidad Presencial. Cundinamarca: Tesis Especialización en Seguridad Informática. Bogotá: Escuela de Ciencias Básicas, Tecnologías e Ingenierías. Disponible en: http://hdl.handle.net/10596/12028.

[13] RESTREPO, Jenny Fernanda. Diagnóstico del estado actual de la Seguridad de la Información basado en la Norma ISO 27001:2013, de la Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds de la Ciudad de Popayán. Tesis Especialización en Seguridad Informática. Popayán-Cauca: Escuela de Ciencias Básicas, Tecnología e Ingenierías, Disponible en: http://hdl.handle.net/10596/17381.

27001:2013. Donde recomendó medidas de seguridad para proteger y mantener la confidencialidad, integridad y disponibilidad de la información, cuyo objetivo principal fue realizar un diagnóstico del estado actual de la seguridad de la información, donde se podrá identificar el impacto y la probabilidad de ocurrencia de vulnerabilidades, amenazas y riesgos a los que está expuesta la institución en relación a la seguridad de la información y en el proceso de gestión académica. Durante el análisis realizado se identificaron inconformidades de tipo mayor y de tipo menor, permitiendo identificar diferentes criterios esenciales en la seguridad de la información y el conocimiento detallado de la norma ISO 2700; 2013 y la importancia de la aplicación de los controles en una organización. Este estudio aporta al proyecto presente mucha información necesaria sobre seguridad de la información y pasos a seguir al momento de diagnosticar el estado actual de la seguridad que tiene la institución y poder realizar un manual de buenas prácticas para evitar amenazas y vulnerabilidades que se puedan presentar.

Por otra parte, Nieves[14], elaboró su tesis de grado sobre diseño de un sistema de gestión de la seguridad de la información que permitió evaluar la integridad, confidencialidad y disponibilidad de los activos (hardware y software) del centro de educación técnica y tecnológica del departamento del Cesar, con el fin de analizar e implementar un SGSI, usando la norma ISO 27001:2013 y la metodología Magerit para la gestión del riesgo. Como resultado final, la valoración de los riesgos de los activos de información de la oficina de ingreso del centro de educación técnica y tecnológica del departamento del Cesar permitió identificar que el desconocimiento del tema pone en riesgo los procesos que se desarrollan en cuanto a disponibilidad, integridad y confidencialidad. Este antecedente se relaciona con el presente

[14] NIEVES, Arlenys Carolina. Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) basados en la Norma ISO/IEC 27001:2013. Tesis Especialización en Seguridad de la Información. Cesar: Institución Universitaria Politécnico Gran Colombiano. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y.

proyecto porque se enfoca a la seguridad de la información de una Empresa proponiendo el diseño de un sistema de gestión de seguridad de la información (SGSI) que permite identificar las amenazas, vulnerabilidades y la elaboración de un plan con la finalidad de mitigar los riesgos, capacitando y sensibilizando sobre seguridad de la información a los funcionarios.

En Antioquia Berrio[15], construyó un proyecto cuyo objetivo fue proponer una metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001, utilizando el método Delphi que permite evaluar y seleccionar controles de seguridad.

Es indispensable contar con varios expertos en el tema que den conceptos que ayuden a efectuar una auténtica implementación de gestión de seguridad y permita evaluar los riesgos establecidos.

El estudio permitió concluir que si bien es necesario que todas las personas involucradas en la implementación deben saber del tema para poder elaborar una valoración y calificación de los controles de seguridad de la información, también es necesario que en todas las áreas el personal de la empresa debe tener conocimientos sobre los riesgos a que diariamente se exponen y poder detectar una posible amenaza o vulnerabilidad que atente con la seguridad de la información.
Se recomienda que para llevar con éxito la metodología, los auditores que están implementando el sistema de gestión de seguridad de la información (SGSI) no deben realizar las consultas o encuestas para que su opinión no influya en la decisión, se sugiere también implementar un módulo de alertas tempranas para el monitoreo de los controles.

---

[15] BERRÍO LOPEZ, Juan Pablo. Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la Norma ISO/IEC 27001. Tesis Magister en Ingeniería, Ingeniería de Sistemas. Antioquia: Disponible en: http://www.bdigital.unal.edu.co/56173/1/1128401087.2017.pdf.

Este estudio aporta valiosa información al presente proyecto porque se basa en la norma ISO/IEC 27001 explicando cada una de sus fases y además propone metodologías para evaluar el desempeño de los controles, como lo es el método Delphi.

Núñez y Chacón[16] desarrollaron un diseño del sistema de gestión de seguridad de la información para la empresa "Serexcel" servicios funerarios, con el fin de implementar un nuevo mecanismo, que ayude a la empresa, creando políticas de seguridad que permita contribuir en el resguardo y protección de la información y a tener un mayor control. Con la aparición de los sistemas informáticos y de comunicación se permite la sistematización de la información facilitando su rápido acceso, procesamiento, almacenamiento y transferencia de datos; estos sistemas no garantizan que la información esté protegida ya que esta sigue expuesta a diferentes ataques donde se puede ver afectada la integridad, confidencialidad y disponibilidad de la empresa; es por eso que se diseñó el sistema de gestión de seguridad de la información para la empresa "Serexcel" servicios funerarios, y dentro de las recomendaciones realizadas esta capacitar e involucrar a los funcionarios en el tema de seguridad, manejo de riesgos, vulnerabilidades, revisar y actualizar cada año el documento de políticas de seguridad de la información para así poder evaluar incidentes de seguridad y saber qué cambios afectan la estructura de la organización. Este antecedente se relaciona con el presente proyecto porque orienta sobre los cuidados que se deben implementar sobre seguridad de la información en una empresa; a través del sistema de gestión de seguridad de la información (SGSI).

[16] NUÑEZ, William Andrés y VERGARA, Édison Andrés. Diseño del Sistema de Gestión de Seguridad de la Información para la Empresa "Serexcel" Servicios Funerarios. Bogotá D.C: Tesis Ingeniero en Telemática, disponible en: Universidad Distrital Francisco José de Caldas. Facultad Tecnológica. http://hdl.handle.net/11349/8323.

Al interior de la Universidad abierta y a distancia UNAD, se evidencian documentos con investigación referente al tema de seguridad.

Moreno y Palacios[17] Proyecto cuyo objetivo fue diseñar un sistema de gestión de seguridad de la información para UNISANAR IPS, bajo la norma ISO 27001:2013, que le permita implementar la seguridad de la información y establecer las medidas preventivas y correctivas necesarias; para garantizar la confidencialidad, integridad y disponibilidad de la información administrada por la IPS. Como resultado del estudio encontraron que UNISANAR IPS presenta falencias en cuanto a la aplicación de controles de seguridad establecidos en la norma ISO 27001:2013, esta situación fue considerada para el diseño del SGSI y entre las recomendaciones que hicieron se destaca la sensibilización a la gerencia y a los funcionarios sobre el valor de la información como activo de la empresa y la necesidad de implementar el SGSI para disminuir los riesgos a que está expuesta. Este estudio aporta al proyecto presente elementos metodológicos y conceptuales por presentar un tema de estudio y objetivo común, el diseño de un SGSI.

Por otra parte, Bojaca[18], elaboró para el área administrativa y de historias clínicas del Hospital san francisco de Gachetá, el diseño de un sistema de gestión de seguridad informática, basado en la norma ISO/IEC 27001- 27002, luego de haber detectado el principal problema que aqueja la empresa como lo es la falta de parámetros y políticas que mejoren el nivel de confiabilidad en el área administrativa y de historias clínicas del hospital san francisco de Gachetá, se requiere analizar las posibles vulnerabilidades y posibles amenazas informáticas a las que se ve

[17] MORENO, Letty y PALACIOS, Yaciry. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2013 para la empresa Unisanar IPS de Quibdó. Tesis Especialización en Seguridad Informática, Chocó: Universidad abierta y a distancia UNAD. Escuela de ciencias básicas e Ingeniería. Disponible en: http://hdl.handle.net/10596/15028.

[18] BOJACA, Edgar Alonso. Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco De Gacheta. Tesis, Especialización en seguridad informática. Gacheta Cundinamarca: Universidad nacional abierta y a distancia. Disponible en: http://hdl.handle.net/10596/12685.

expuesta la información digital aplicando la metodología Magerit (Metodología práctica para gestionar riesgos). Esta tesis es de importancia para el desarrollo del proyecto a desarrollar porque se apoya en el diseño de un sistema de gestión de la seguridad de la información (SGSI), basado en la norma ISO/IEC 27001- 27002 aportando metodologías que ayuda a realizar una evaluación detallada de los riesgos que actualmente hay o los que a futuro se pueden presentar debido a las vulnerabilidades del sistema.

2.2 MARCO TEORICO CONCEPTUAL

2.2.1. Seguridad de la información

Los datos pueden ser una letra, palabra o descripción, ellos no contiene ninguna información, en cambio la información es el conjunto organizado de datos que construye un mensaje.

Por ser la información el activo más valioso que posee cualquier organización, su protección es una prioridad. Por tal razón, la seguridad de la información es definida por Escrivá, Romero y Ramada[19], como “el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información”. La confidencialidad garantiza que sólo los usuarios autorizados pueden acceder a la información para consulta o actualización; mientras que en la disponibilidad aseguran que la información está asequible en el momento en que sea requerida por los usuarios.

La seguridad de la información por ser la disciplina que nos habla de riesgos, amenazas, análisis de escenarios de las buenas prácticas y esquemas normativas, exige niveles de aseguramiento en los procesos que se llevan, su objetivo principal

[19] ESCRIVÁ, Gema; ROMERO, Rosa y RAMADA, David. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A. Retrieved from http://www.ebrary.com

es la de proteger la información contenida en páginas web, correo electrónico, documentos impresos, cd, USB, información confidencial, propiedad intelectual, secretos comerciales, ideas generadas al interior de la empresa, entre otros, la estructura computacional como hardware, sistema operativo, programas de aplicaciones y los usuarios que pueden ser los internos y externos.

Actualmente, las empresas dependen de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad del negocio, a esto se le suma la falta de medidas de seguridad en las redes, siendo un problema que está en crecimiento, lo que genera un mayor número de atacantes que se organizan mejor cada día, por lo que van adquiriendo a diario habilidades más especializadas que les permiten obtener mejores resultados en sus ataques. Al igual que las fallas de seguridad provenientes al interior de las organizaciones ocasionando vulnerabilidades que son aprovechadas por los delincuentes informáticos. También se debe tener en cuenta los usuarios internos empleados activos y los que se han retirado de la organización quienes en su debido momento se encargaron del manejo de información vital de la empresa.

En este contexto, la seguridad de la información es un proceso y no un producto. Se estructura sobre tres elementos claves como son las operaciones realizadas, las personas que las realizan y la tecnología que las soporta, tal como lo mencionan Álvarez, García y Pérez[20]. Si alguno de estos elementos no funcionan bien, la seguridad del sistema en su conjunto estará comprometida, porque la seguridad global es tan robusta como la seguridad del elemento menos protegido.

[20] ÁLVAREZ MARAÑÓN, Gonzalo, GARCÍA PEDRO, Pablo Pérez. Seguridad informática para empresas y particulares, McGraw-Hill España, 2004. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3195263.

2.2.2 Seguridad informática

Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además de otras propiedades, que también pueden estar involucradas como la autenticación, registro de responsabilidad, el no repudio y la confiabilidad[21]. Proceso permanente de monitoreo de los sistemas para identificar las vulnerabilidades y realizar las acciones necesarias para eliminarlas, y de esta manera salvaguardar la información y los activos informáticos de las organizaciones. Con base en Perpiñán[22], se puede afirmar que la seguridad informática consiste en hacer uso de los medios necesarios para reducir las vulnerabilidades de los sistemas a su mínima expresión. Asencio[23], por su parte propone que la seguridad informática es la "capacidad de mantener intacta y protegida la información de sistemas informáticos".

La seguridad informática es una rama de la seguridad de la información que busca proteger la información almacenada o transmitida mediante una infraestructura informática o de comunicaciones de una organización. Tal como lo describen Escrivá, Romero y Ramada[24,] la seguridad informática, según lo que protege y el momento en que lo hace, puede clasificarse como: seguridad física que se encarga de la protección física de los activos y la información frente a amenazas como robos y desastres naturales. En cuanto a la seguridad lógica, busca brindar protección a los datos, las aplicaciones, los sistemas operativos y demás información del sistema.

---

[21] UTN.BA – Universidad Tecnológica Nacional. Seminario ISO 27001 - 09 Septiembre 2014 en UTN BA. https://es.slideshare.net/cgcutn/seminario-iso-27001-09-septiembre-2014.
[22] PERPIÑAN, Antonio. (2011). Seguridad de sistemas GNU/Linux. Fundación código libre dominicano. Recuperado de: http://highsec.es/wp-content/uploads/2013/10/LibroSeguridad-GNU-Linux-Antonio-Perpinan-2011.pdf
[23] ASENCIO, Gonzalo. (2006). Seguridad en Internet. Madrid: Ediciones Nowtilus.
[24] ESCRIVÁ, Gema; ROMERO, Rosa y RAMADA, David. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A. Retrieved from http://www.ebrary.com.

Una de las técnicas utilizadas para este tipo de protección son las claves de seguridad y la encriptación. La seguridad activa como el conjunto de medidas preventivas que se despliegan para detectar y evitar los incidentes que pueden afectar los sistemas informáticos. Son acciones que se llevan a cabo antes de que se produzcan los incidentes, como el manejo de contraseñas. Seguridad pasiva corresponde a las técnicas y procedimientos correctivos que tienen como fin minimizar las consecuencias de un incidente, como la recuperación de una copia de seguridad. Como afirma Galdámez(s.f.)[25], el objetivo de la seguridad informática es proteger los recursos informáticos importantes para el funcionamiento de una organización, como es la información, los equipos, los programas y la infraestructura de tecnología de la información, y de esta forma proteger también la reputación y los recursos financieros.

"Mientras los hackers mejoran en ofensiva, las empresas desmejoran en defensa".[26] El operador de telefonía móvil en Estados Unidos Verizon ha publicado un informe donde evidencia la problemática diaria que viven miles de empresas en cuanto a seguridad informática. Las cifras no son nada alentadoras, pues demuestra que cada vez más, los hackers están mejor preparados y además organizados para realizar ataques, mientras que las organizaciones escasamente logran ponerse al día en medidas de seguridad informática.

2.2.3.1 Norma ISO 27000: gestión de la seguridad de la información (fundamentos y vocabulario). Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA (del

[25] GADALMEZ, Pablo. (2003). Seguridad informática. Actualidad TIC, Revista del Instituto Tecnológico de Informática, 1. Recuperado de: http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf.
[26] Derecho Informático. Disponible en: http://derechoinformatico.co/seguridad-informatica-mientras-los-hackers-mejoran-en-ofensiva-las-empresas-desmejoran-en-defensa/

inglés *plan-do-check-act*, esto es, planificar-hacer-verificar-actuar), al igual que las definiciones de los términos que se emplean en toda la serie 27000, esta norma tiene una similitud con las normas de gestión de calidad ISO 9000, son una serie de estándares con un rango que va de la 27000 a 27019 y de 27030 a 27044. Cada una de las normas de la familia 27000, precisa y concentra todos los aspectos trascendentales de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como pública y privada.

Esta familia de normas que tiene como objetivo definir requisitos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados y proporcionales, protegiendo así la información, es recomendable para cualquier empresa grande o pequeña de cualquier parte del mundo y más especialmente para aquellos sectores que tengan información crítica o gestionen la información de otras empresas.

2.2.3.2 ISO/IEC 27001: es la Norma más importante de la familia 27000 porque abarca todos los requisitos pertinentes que se deben tener en cuenta en el sistema de gestión de seguridad de la información. Cuenta con el anexo A, que detalla de manera resumida los objetivos de los dominios con sus respectivos controles que explica la ISO 27001:2005, con la finalidad de que en las organizaciones se implemente en el desarrollo de los SGSI.

Fue publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013, y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Se puede implementar en cualquier tipo de empresa, con o sin fines de lucro, privada o pública, pequeña o grande, fue escrita por especialistas en el tema y suministra una técnica para implementar el sistema de gestión de la seguridad de la información en una organización, permitiendo que la empresa sea certificada por

la implementación y cumplimiento de los requisitos legales. La mejor opción es la norma ISO 27001, ya que esta se encuentra en la actualidad con la mejor metodología, garantizando mayor cumplimiento y mejores respuestas.

Al conseguir una certificación comercial, se convierte de gran utilidad ante los ojos de los clientes, toda vez que una empresa certificada genera mayor confiabilidad a la hora de preservar la información, dando mejores ventajas ante las otras organizaciones; menos costos, contrarresta incidentes de seguridad; lo que evita costos y ahorra gastos en la organización y claridad en los procesos y procedimientos de la empresa, dejando claro las funciones, responsables y acciones a tomar, con miras a aumentar la motivación de sus empleados por tener directrices claras y coherentes.

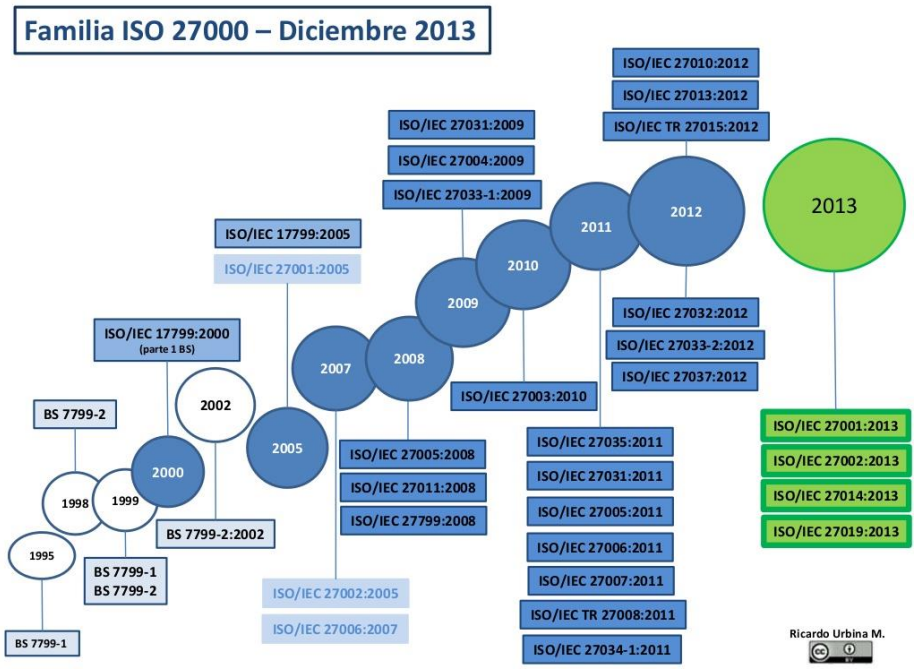
Funciona mediante la evaluación de riesgos, analizando los potenciales problemas que pueden llegar a afectar la información, posteriormente se definen las acciones a tomar para minimizar los riesgos de manera sistemática.

Los controles que se deben implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica teniendo en cuenta por ejemplo el software y los equipos de cómputo. Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero lo utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales, empezando por la redacción de los documentos necesarios para prevenir violaciones de la seguridad, es por ello que la seguridad de la información no se limita a lo relacionado con las TI (tecnologías de la información) solamente, sino que además va de la mano con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

2.2.3.3 ISO/IEC 27002: esta norma es una enseñanza de los pasos a seguir, explica los objetivos de los dominios y controles que son convenientes cuando se habla de seguridad de la información. Posee 14 dominios, 35 objetivos de control y 114 controles. Publicada desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición.

Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información. Esta norma se encuentra publicada en español a través de la empresa AENOR y en Colombia NTC -ISO IEC 27002, así mismo se pueden encontrar en Perú, chile, entre otros países latinoamericanos.

Ilustración 1Evolución de la Familia ISO27000



Fuente: Ricardo Urbina Miranda, Grupo Elecmetal.

2.2.3.4 Correcciones de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013:

Actualmente, se trabaja constantemente tanto en la implementación como en la auditoría, capacitación y consultoría sobre las nuevas versiones de la ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Hace unos días se publicó la corrección técnica 1, tanto para ISO 27001 como para ISO 27002.

ISO/IEC 27001:2013/ corrección 1:2014

ISO/IEC 27002:2013/ corrección 1:2014

Estas correcciones se traducen en cambios que no afectan a la norma, simplemente son cambios en el control de éstas. A pesar de que no tenga mucha repercusión en su implantación, los desarrolladores del material si tendrían que realizar actualizaciones.

Estas variaciones están en las normas ISO/IEC 27001:2013/corrección1:2014 en el control A 8.1.1 inventario de activos y en la ISO/IEC 27002:2013/corrección1:2014 en las sub cláusulas:

7.1.2 Términos y condiciones de contratación,

8.1.1 Inventario de activos,

8.1.3 Uso aceptable de los activos.

El control A 8.1.1, realiza una mejora en la redacción anterior para un mejor entendimiento y comprensión del objetivo de control. Este cambio se aprecia en la 27002, donde se modificó el texto de la sub cláusula 8.1.3 para ayudar al entendimiento de su finalidad[27].

[27] GTDI – Tecnologías de la Información y Consultoría. Publicadas correcciones (Cor1:2014) a la ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Disponible en: https://www.gtdi.pe/correccion_a_27001_27002.

Cuadro 1 ISO27000_estado_diciembre_2013.

NORMA	AÑO	OBJETIVO
ISO/IEC 27001	2005 2013	☞ Establece los requerimientos necesarios para cumplir con un sistema de gestión de la seguridad (SGSI). ☞ Es certificable. ☞ Norma actualizada en el año 2013, aumentando de 102 a 130 requisitos y con cláusulas hasta la 10, se elimina el modelo P-D-C-A argumentando que existen otros que también permiten la mejora continua.
ISO/IEC 27002	2005 2013	☞ Código o guía de buenas prácticas para la seguridad de la información, detalla los 133 controles reunidos en 11 grupos, más 39 “objetivos de control”. ☞ Norma actualizada en el año 2013 disminuyendo a 114 controles pero aumentando a 13 dominios.

Fuente: Ricardo Urbina Miranda, oficial de seguridad de la información grupo Elecmetal, Presidente CSA Capítulo Chileno

2.2.3.5 Norma Técnica Peruana NTP-ISO/IEC 27001:2014

El comité de normalización de codificación e intercambio electrónico de datos presentó a la comisión de normalización y de fiscalización de barreras comerciales no arancelarias, el PNTP-ISO/IEC 27001:2014, con fecha 2014-08-19, para su revisión y aprobación; siendo oficializada como norma técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2ª Edición, el 01 de diciembre de 2014[28].

[28] INDECOPI 2014. https://canvas.utp.edu.pe/courses/8870/files/42244/download?download_frd=1.

2.2.4 Riesgo

El riesgo es la posibilidad de que una amenaza pueda explotar una vulnerabilidad en particular. Hoy en día la mayoría de los ordenadores con sistemas operativos de escritorio, permanecen conectados a internet, lo que los hace mucho más vulnerable por todas las amenazas que se presentan.

Según Jiménez[29] riesgo es toda proximidad o posibilidad de un daño, peligro, etc. Es cada uno de los imprevistos, hechos desafortunados, etc. que puede cubrir un seguro. Como sinónimo de riesgo se encuentra amenazas, contingencia, emergencia, urgencia y apuro y seguridad es la cualidad o estado de seguro, garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Por ser el riesgo una condición que afecta a diario y por estar expuestos a circunstancias del entorno donde hay posibilidad de pérdidas, como en el caso de los riesgos informáticos que se exponen directamente los sistemas de información a toda clase de atentados y amenazas provocando que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus, etc… el riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores es el que representa el riesgo[30].
El riesgo es la combinación de la probabilidad de un evento y su consecuencia, por tanto:
Riesgo = (probabilidad de ocurrencia de la amenaza) x (impacto o daño).

---

[29] JIMÉNEZ, José Alfredo. Evaluación: seguridad de un sistema de información, El Cid Editor apuntes, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3181540.
[30] SME Instituto Nacional de Ciberseguridad de España MP, S.A. [ES] – INCIBE: Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

Riesgo informático es la incertidumbre que existe por la posible realización de un suceso, relacionado con una amenaza de daño, respecto a los bienes o servicios informáticos. Las clases de riesgos informáticos que existen son: riesgos de integridad, de relación, de acceso, de utilidad, de infraestructura, de seguridad general, mecánico y de radiaciones.

Pero también existen otras clases de riesgo como:

- ✓ Riesgo por fraude electrónico,
- ✓ Persona interna o externa,
- ✓ Desastres naturales,
- ✓ Por servicios, suministros y trabajos no confiables.
- ✓ Abuso de manejo de sistemas informáticos por la incompetencia.
- ✓ Desastre a causa de la intromisión, robo, fraude y sabotaje.

2.2.5. Análisis de riesgo

Para Gómez y Álvarez[31], el análisis de riesgo es el que establece que tipo de amenazas y vulnerabilidades tienen los activos de la información, los cuales previamente han sido inventariados. Dicho procedimiento es crucial para el correcto diseño del SGSI, puesto que de su resultado depende que se escojan los controles útiles y necesarios; que serán los que conformen el sistema.

Para Giménez[32] el gran reto de los métodos de análisis de riesgo, es la complejidad del problema al que se enfrentan, ya que hay muchos elementos que considerar y

[31] GÓMEZ FERNÁNDEZ, Luis y ÁLVAREZ, Ana Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3205110.

[32] GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3), IC Editorial, 2014. ProQuest Ebook Central, https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=4184155.

si no es riguroso, las conclusiones serán poco fiables y no habrá un producto final que supla las necesidades de la empresa o institución.

En el capítulo 2 requisitos de la norma UNE 27001, del libro Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, Gómez y Rivero[33] expresan que dentro de la planificación y las acciones para tratar los riesgos y oportunidades se encuentra el análisis de riesgos y es en esta fase donde se valoran las consecuencias y probabilidades de la materialización de los riesgos identificados en el contexto de la organización, obteniendo así los niveles de riesgo.

2.2.6 Sistema de Gestión de Seguridad de la Información

El sistema de gestión de seguridad de la información (SGSI) es el principal concepto sobre el que se conforma la norma ISO 27001 en donde se establecen políticas, procedimientos y controles, este se debe realizar mediante un proceso integral, documentado y conocido por todos los funcionarios de la empresa, donde se debe tener en cuenta la seguridad física, la seguridad en los recursos humanos que son los trabajadores, los incidentes de seguridad y la continuidad del negocio. En materia de seguridad, los beneficios que debe tener un SGSI, se refleja en que mejora la competitividad en el mercado y disminuyen los costos mediante la prevención.

Un sistema de gestión de la seguridad de la información (SGSI) permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la

[33] GÓMEZ FERNÁNDEZ, Luis y RIVERO PEDRO, Pablo Fernández. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2018. ProQuest Ebook Central, http://ebookcentral.proquest.

información de las empresas ISO[34] y la seguridad informática es la encargada de la protección de la infraestructura de las tecnologías de la información y comunicación que soportan el negocio y la seguridad de la Información, siendo la encargada de proteger los activos de información fundamentales para el éxito de las empresas.

Los correos electrónicos, las páginas web, las imágenes, los logos, las bases de datos, los fax, los contratos, las presentaciones, los documentos, las unidades extraíbles, entre otros, hacen parte de la información importante y sensible a proteger que se encuentra en las organizaciones. Es por eso que diseñar un SGSI en EDUTEC, permitirá analizar y ordenar la estructura de los sistemas de información, facilitando la definición de procedimientos de trabajo para mantener su seguridad y disponer de controles que permitan medir la eficacia de las medidas tomadas.

Todas estas acciones protegen de amenazas y riesgos que pueden poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos del negocio. Para esto se debe distinguir dos tipos de procesos, como el proceso de gestión que es el encargado de controlar el funcionamiento correcto del sistema de gestión, su mejora continua y el proceso de seguridad, centrándose en los aspectos relativos a la seguridad de la información.

Gómez y Rivero[35] destacan que en la versión del 2014 el anexo SL en toda su estructura, fue adoptado y asumido por otras normas internacionales como UNE-

[34] ISO. Sistema de Gestión de Seguridad de la Información. S.P.I. Disponible en: www.ISO27000.ES.

[35] GÓMEZ FERNÁNDEZ, Luis y RIVERO PEDRO, Pablo Fernández. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2018. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=5486388.

EN ISO 9001:2015 y UNE-EN ISO 14001:2015, permitiendo una mejor integración de sistemas de gestión por poseer una estructura y requisitos comunes

Un sistema de gestión de la seguridad de la información (SGSI) es la parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información, tal como lo expresan Gómez y Álvarez[36].

En el diseño de un SGSI no solo se analizan las vulnerabilidades, amenazas y riesgos en hardware o software, también es indispensable realizar un análisis de brechas de seguridad (GAP ANALYSIS)[37], estudio preliminar[38] que permite realizar una comparación del programa de seguridad que actualmente tiene la empresa, con relación a las mejores prácticas reconocidas en la industria. Al confrontar estas mejores prácticas con las prácticas reales, podemos arrojar luz sobre las áreas donde las vulnerabilidades y los riesgos están latentes. Utilizando criterios establecidos en normas o estándares.

Se deben seguir 4 pasos que son críticos para cada análisis de brechas de seguridad de la información:

PASO 1: Seleccionar un marco de seguridad estándar: Uno de los marcos más comunes es el estándar ISO / IEC 27002: 2013 que proporciona recomendaciones de mejores prácticas en la gestión de la seguridad de la información. Esta norma

---

[36] GÓMEZ FERNÁNDEZ, Luis y ÁLVAREZ, Ana Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012. ProQuest Ebook Central, https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3205110.

[37] IFIXED. Como conducir un Análisis de Brechas de Seguridad (*GAP Analysis*). Disponible en: https://www.ifixed.cl/2018/10/22/como-conducir-un-analisis-de-brechas-de-seguridad-gap-analysis/.

[38] MENDOZA, Miguel Ángel. 6 consideraciones previas a la implementación del SGSI. Disponible en: https://www.welivesecurity.com/la-es/2017/11/06/consideraciones-implementacion-del-sgsi/

cubre las mejores prácticas para áreas de seguridad clave como la evaluación de riesgos, el control de acceso, la gestión de cambios, la seguridad física y otros.

PASO 2: Evaluar personas y procesos: El objetivo principal es entender y analizar los objetivos clave de la organización así como también su dirección estratégica. Definitivamente significa aprender qué políticas de seguridad ya existen y en qué dirección los líderes de su organización estarán llevando a su empresa durante los próximos tres a cinco años, esto implica identificar los riesgos de seguridad que estarán asociados con ella. En las buenas prácticas de seguridad deben estar involucrados todos en la empresa, debido a que muchos de los riesgos que enfrentan las redes de la empresa son causados por la intervención humana. Se debe abordar el comportamiento humano, para disminuir las amenazas a los datos. Los miembros clave del personal pueden proporcionar detalles sobre cómo se implementan los diversos controles., cuanto más sepamos

PASO 3: Recopilación de datos / tecnología: El objetivo es comprender qué tan bien funciona el programa de seguridad actual dentro de la arquitectura técnica. Como parte de este paso, es necesario comparar los controles de mejores prácticas (ISO 27002:2013) o los requisitos relevantes con los controles de la organización; es importante tomar, por ejemplo una muestra de dispositivos de red, servidores y aplicaciones para validar brechas y debilidades; revisar los controles de seguridad automatizados; y revisar los procesos de respuesta a incidentes, protocolos de comunicaciones y archivos de registro. Con una recopilación de datos y análisis, se obtiene una imagen clara del entorno técnico, las protecciones implementadas y eficacia de seguridad general.

PASO 4: Análisis: Es el paso final una vez terminadas las fases anteriores, se realizar un análisis profundo del programa de seguridad, tomando los hallazgos y los resultados en todos los factores para crear una imagen clara y concisa del perfil

de seguridad de las tecnologías de la información que incluye áreas de fortaleza y áreas donde es más necesario mejorar. Con esa información en la mano, podemos hacer recomendaciones para crear y avanzar con un plan de seguridad adecuado para la empresa. Esa hoja de ruta de seguridad debe considerar los requisitos de riesgos, personal y presupuesto, así como los plazos para completar las diversas mejoras de seguridad.

Para concluir podemos decir que realizar un análisis de brechas de seguridad no garantiza un 100% de seguridad, pero es un largo camino para certificar que la red, el personal y los controles de seguridad son robustos, efectivos y rentables.

2.2.7 Políticas y controles de seguridad

Una política es un plan general de acción que guía a los miembros de una Empresa en la conducta de su operación, se puede establecer políticas corporativas como lineamientos que sirven de marco de referencia para la operación del negocio o empresa. Son las reglas del juego, que orientan, estandarizan el comportamiento y ejecución de éstos por los empleados de una organización.

Los elementos básicos que deben de tener las políticas es tener un objetivo claro, que sea y tenga alcance, establecer roles y responsabilidades. Por otra parte los lineamientos son reglas esenciales que se requieren para implementar en la entidad y las autorizaciones son las firmas de aprobación de los niveles jerárquicos establecidos en la organización que debe haber y seguir un conducto regular. Son las soluciones específicas de cómo manejar los asuntos.

Las empresas deciden elaborar las políticas sobre seguridad, a menudo para parar y dar solución a incidentes presentados o por recomendación de auditores “Sin políticas no se puede auditar porque no hay contra qué”[39].

“Si existe alguna figura de administración de seguridad, en principio puede ser la idónea para elaborar las políticas, partiendo de directrices y sometiendo los borradores a directivos de un nivel adecuado, preferentemente constituidos en comité”[40].

La palabra control deriva del francés antiguo controle que se refería a un registro que lleva un duplicado. En administración, control es un mecanismo del proceso administrativo creado para verificar que los protocolos y objetivos de una empresa, departamento o producto cumplen con las normas y las reglas fijadas[41]. El control tiene como objetivo evitar irregularidades y corregir aquello que frena la productividad y eficiencia del sistema.

Entre otros conceptos encontramos, según Harold Koontz y Cyril J. O’Donnell que control es medir y corregir las actividades de subordinados para asegurarse que los eventos se ajustan a los planes y para Theo Haimann[42], es el proceso de verificar para determinar si se están cumpliendo los planes o no, si existe un progreso hacia los objetivos y metas. El control es necesario para corregir cualquier desviación, se debe ejerce control en todos los niveles de las organizaciones; desde los niveles superiores o jerárquicos, hasta los niveles inferiores u operativos.

---

[39] PESO NAVARRO, Emilio del, GONZÁLEZ RAMOS, Miguel Ángel. La seguridad de los datos de carácter personal. 2003. Ediciones Díaz de Santos, 2015.
[40] Ibíd., pág. 44.
[41] Zonaeconomica.com "Concepto de Control" [en línea] Dirección URL: https://www.zonaeconomica.com/control.
[42] Ibíd.

Para tener una correcta gestión de la seguridad de la información en las empresas, es necesario definir en un documento una política de seguridad, la cual proporciona a la Dirección de la empresa, las pautas y ayudas en materia de seguridad de la información, procedentes de requerimientos comerciales, requerimientos legales, nacionales e internacionales, de objetivos de la organización y de otras regulaciones aplicables.

2.3. MARCO CONTEXTUAL

EDUTEC, es una institución de educación técnica, bajo la modalidad de educación para el trabajo y el desarrollo humano, con sede en Pitalito (Huila).
Ofrece carreras técnicas en:

- Gestión contable y financiera - duración tres semestres.
- Salud ocupacional - duración tres semestres.
- Mantenimiento electrónico y comunicaciones - duración tres semestres.
- Técnico en sistemas informáticos - duración tres semestres.
- Asistente en administración empresarial - duración tres semestres.
- Formación integral a la primera infancia - duración tres semestres.

Ilustración 2 Instalaciones EDUTEC.

Fuente: EDUTEC

Aprobado por la secretaría de educación de Pitalito (Huila), según licencia de funcionamiento número 268 del 27 de julio de 2011. Ubicado en la calle 4 # 5 – 19 centro en el municipio de Pitalito, Departamento del Huila.

La función principal de EDUTEC, es ofrecer estudio técnico, capacitado y tecnificado con proyección laboral y empresarial. Cuenta con licencia de aprobación, amparada por la secretaria de educación y supervisada por el Ministerio de educación nacional.

EDUTEC es pionero en el sur de Colombia en la educación para el trabajo y desarrollo humano, porque fomenta la capacitación y fuerza laboral de sus más de 400 alumnos en la jornada de la mañana, noche, sábados y domingos; formados en tres aulas o laboratorios de sistemas, orientados por docentes especializados. Actualmente la planta administrativa se compone de cuatro administrativos y veinticuatro docentes en diferentes áreas del conocimiento.

Entre los principios corporativos que se practica en el desarrollo de las actividades pertinentes del servicio educativo, se asume los principios que hacen posible la

convivencia entre la comunidad y la institución y el de la formación para el desarrollo de las competencias específicas como[43]:

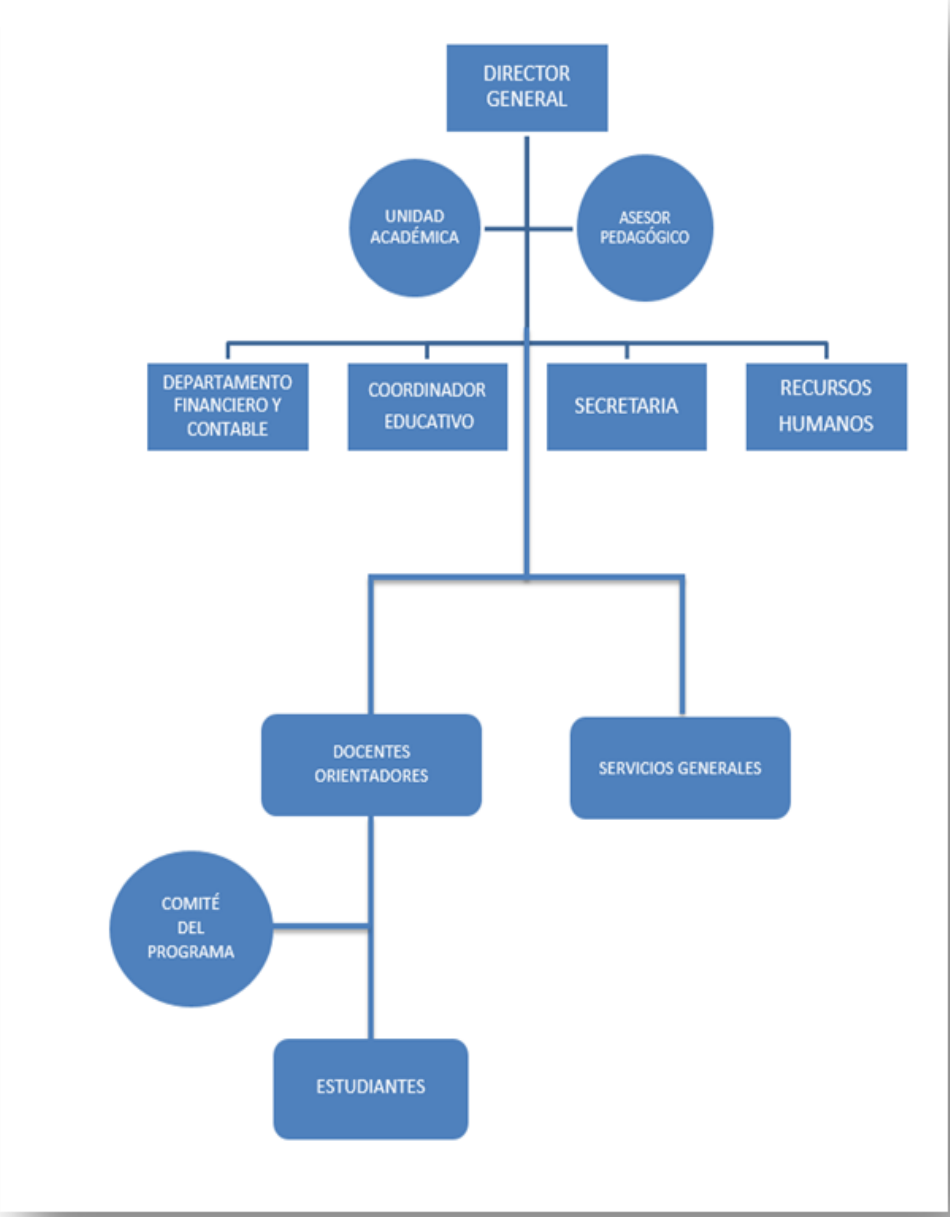
- ✓ Respeto: valoración y cuidado de sí mismo, de los demás y de la naturaleza.
- ✓ Responsabilidad: previsión y compromiso con el actuar.
- ✓ Convivencia: interacción armónica en el encuentro con el otro.
- ✓ Racionalidad: eje vertebral del desarrollo humano.
- ✓ Amistad: interacción de crecimiento y respeto.
- ✓ Solidaridad: acompañamiento a los demás en las diversas circunstancias de la vida.
- ✓ Justicia y equidad: reconocimiento del derecho del otro y de sus méritos.
- ✓ Lealtad: sinceridad y fidelidad consigo mismo y con los demás.
- ✓ Honestidad: integridad en lo público y lo privado.
- ✓ Disciplina: esfuerzo y organización para el logro de las metas.
- ✓ Tolerancia: pensar libremente y expresar sus ideas de palabra y por escrito.
- ✓ Protección al medio ambiente: convivir socialmente con los demás seres en el mundo.

En el organigrama encontramos la representación gráfica de EDUTEC, en donde a través del diagrama jerárquico y funcional se observa que actualmente toda la estructura de la institución, depende del director general; quien es el único responsable en la toma de decisiones en cumplimiento de las metas propuestas y poder así lograr los objetivos trazados.

[43] EDUTEC – Principios corporativos.

ORGANIGRAMA

Ilustración 3 Organigrama EDUTEC



Fuente: EDUTEC.

La misión del Instituto EDUTEC es asegurar la calidad de servicio educativo a través del proceso formativo orientado al desarrollo de las competencias específicas de los estudiantes que accedan al mundo laboral en condiciones de trabajadores o empresarios, como implicados con el desarrollo económico, social, cultural y tecnológico de la región y del país, en un entorno innovador, competitivo y productivo[44].

Como visión EDUTEC se proyecta como una organización reconocida a nivel regional con proyección formativa para el trabajo nacional e internacional; por la pertinencia de sus ofertas y servicios educativos y por el compromiso y aporte de su comunidad académica al desarrollo humano y del ambiente sostenible de las comunidades locales y globales.

[44] EDUTEC – Misión y visión institucional.

2.4. MARCO LEGAL

Según Ojeda[45], el delito informático también conocido como *computer crime,* se sabe que quienes cometen estos delitos son personas expertas y conocedores de la tecnología, con fundamento científico e investigativo de los sistemas y también del comportamiento humano y organizacional.

Los delitos informáticos en Colombia, según la revista cara y sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona al código penal colombiano el título VII BIS denominado «De la Protección de la información y de los datos» que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

2.4.1 Ley 1273 de 2009: El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 por medio del cual se modifica el Código Penal, y 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[46].

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

El capítulo primero adiciona el siguiente articulado:

---

[45] OJEDA-PÉREZ, Jorge Eliécer; RINCÓN RODRÍGUEZ, Fernando; ARIAS FLÓREZ, Miguel Eugenio & DAZA-MARTÍNEZ, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.
[46] DACCACH T, José Camilo. DELTA ASESORES. Ley de Delitos Informáticos en Colombia. https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

– Artículo 269A: acceso abusivo a un sistema informático.
– Artículo 269B: obstaculización ilegítima de sistema informático o red de telecomunicación.
– Artículo 269C: interceptación de datos informáticos.
– Artículo 269D: daño informático.
– Artículo 269E: uso de software malicioso.
– Artículo 269F: violación de datos personales.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

– Artículo 269G: suplantación de sitios web para capturar datos personales.
Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “*phishing*”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

a. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
b. Por servidor público en ejercicio de sus funciones
c. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
d. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
e. Obteniendo provecho para sí o para un tercero.
f. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
g. Utilizando como instrumento a un tercero de buena fe.
h. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.
Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

El capítulo segundo establece:
– Artículo 269I: hurto por medios informáticos y semejantes.
– Artículo 269J: transferencia no consentida de activos.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos.

Dentro de las conductas penalizadas, además se encuentra que quien sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de 36 a 72 meses. Diario Oficial 47223 de 2009[47].

2.4.2 Ley 1581 de 2012: El 17 de octubre de 2012, El Congreso de la República Colombia divulgó la Ley Estatutaria, “Por el cual se dictan disposiciones generales para la protección de datos personales”. Título I Objeto, Ámbito de aplicación y definiciones[48].

Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

---

[47] CONGRESO DE LA REPÚBLICA - Ley 1273 de 2009. NOTINET. https://notinet.com.co/leermas_noticiasinv.php?idinv=237957.
[48] ACTUALÍCESE - Ley Estatutaria 1581 de 17-10-2012. https://actualicese.com/normatividad/2012/10/17/ley-estatutaria-1581-de-17-10-2012.

Artículo 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio Colombiano o cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación Colombiana en virtud de normas y tratados internacionales.

Hábeas data. Los datos personales son todo tipo de información vinculada a una persona y que permite llegar a ella, por lo tanto el acceso indiscriminado y el manejo negligente de dicha información pueden lesionar o poner en riesgo aspectos que lleguen a involucrar derechos fundamentales. Las disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. Esta nueva ley no aplica a los datos financieros, estos continúan regulados por la ley 1266 de 2008, ya que estos son diferentes a los datos personales, tampoco aplica a los datos y archivos regulados por la Ley 79 de 1993, a las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico, entre otros[49].

[49] CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012 - NOTINET. https://notinet.com.co/leermas_noticiasinv.php?idinv=237957.

3. METODOLOGÍA

El presente proyecto se desarrolló en tres fases, como se describe a continuación:
1.Se elaboró un inventario de Activos informáticos y de información: para ello se llevó a cabo un proceso de levantamiento de información que incluyó la observación directa en las salas de informática y en las oficinas, entrevistas a usuarios del sistemas como la secretaria, el coordinador y el encargado de sistemas y salas de informática.

2. Se realizó el análisis de riesgo informático, con la información y los activos informáticos de la institución, para proceder a identificar las vulnerabilidades que presentan y los riesgos a los que están expuestos, luego se procedió a la evaluación de los riesgos y el impacto que tiene en la institución si estos se hacen realidad y con esta información se procede a priorizar los riesgos para ser gestionados mediante el SGSI.

3. Se propuso políticas y controles de seguridad: una vez priorizados los riesgos y con base en la norma ISO 27001, se definen las política de seguridad y los controles que se van a implementar para evitar que sigan sucediendo este tipo de eventos que afecten la confidencialidad, integridad o disponibilidad de la información, para ello es importante tener en cuenta el “Ciclo de vida PHVA” Planear, Hacer, Verificar y actuar. La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se aplicó a todos los procesos que abarca el SGSI, esta metodología es conocida por sus siglas en inglés PDCA*: PlanDo-Check-Act* (Aliaga, 2013) o PHVA en español.

Se realizó el análisis y gestión de riesgos de los sistemas de información del Instituto EDUTEC, donde se escogió también la metodología de Magerit, creada por el Consejo Superior de Administración Electrónica.

MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que las directivas de la Entidad, tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información y puedan asumir, gestionar y minimizar los riesgos.

El objetivo perseguido en sucesivas versiones por la metodología Magerit es la evaluación, homologación y certificación de seguridad de sistemas de información, según ISO 27001 y Giménez[50] expresa en su libro seguridad en equipos informáticos (MF0486_3), que el análisis de riesgos (AR), según se define en el método MAGERIT, es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización y la gestión de riesgos (GR), es la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir, o controlar los riesgos identificados[51]. En un sistema de información las dos cosas esenciales son la información que maneja y los servicios que presenta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Se pueden identificar otros activos relevantes:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas *(Software)* que permiten manejar los datos.
- Los equipos informáticos *(hardware)* que permiten hospedar datos, aplicaciones y servicios.

[50] GIMÉNEZ, ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3), IC Editorial, 2014. ProQuest Ebook Central. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184155.
[51] Ibíd., pág. 83.

- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados[52].

Dentro de la información que se maneja, puede ser interesante considerar algunas características tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos[53] que son esenciales para la supervivencia de la Institución.

Para complementar la información y poder desarrollar de la mejor manera este trabajo, se tuvo en cuenta las opiniones y observaciones realizadas por el personal que labora en la Institución y que hace parte directa de esta investigación, con miras a mejorar en los procesos que se llevan a diario y con el único fin de poder realizar el diseño de un sistema de gestión de seguridad de la información (SGSI) para la institución EDUTEC, argumentado en la norma ISO/IEC 27001.

El plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad contempladas en el SGSI para EDUTEC, nace de la necesidad de contar con medidas preventivas en cuanto a seguridad de la información y de los equipos de cómputo. Dicho plan se creó con el fin de tener un documento que recopiló todas las instrucciones que por directriz del director general y del personal del área de tecnología y mantenimiento, sirva de guía a través de las políticas de seguridad

[52] Método de Análisis de Riesgo – Activos. MAGERIT VERSIÓN 3.O: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I- Método.
[53] MAGERIT VERSIÓN 3.O: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catalogo de Elementos.

informática, a todos los usuarios que gestionan y manipulan información necesaria e importante de la Institución.

4. RESULTADOS

Con el fin de tener un inventario de activos informáticos y de información, como control de bienes u objetos a disposición, por ser lo más recomendable para cualquier entidad, compañía o institución. EDUTEC realizó el inventario de activos informáticos y de información, con el fin de garantizar la seguridad de la información, mediante la implementación, seguimiento y mejoramiento de elementos, donde se tuvo en cuenta los servicios informáticos, los datos, las aplicaciones de software, los equipos informáticos, el personal interno o externo, las redes de comunicación, el soporte de información, los equipos auxiliares, las instalaciones y todo lo intangible, con el objetivo de proteger la información frente a la posible materialización de riesgos que afecten la disponibilidad, confiabilidad e integridad en la Institución.

Uno de los requisitos de la norma ISO 27001, incluido en la lista de controles del anexo A, es la correcta gestión de los activos de información que dan soporte a los diferentes procesos, gestionando la identificación por medio de un inventario, estableciendo el responsable o propietario de cada activo, determinando los usos correctos y adecuados de cada uno de ellos, y recuperando cuando sea necesario para evitar pérdidas o difusiones no controlada.

4.1. INVENTARIO DE ACTIVOS INFORMÁTICOS Y DE INFORMACIÓN

Dada la necesidad de saber que activos informáticos y de información tiene EDUTEC, se procede a realizar el inventario, teniendo en cuenta que:

"Las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio – INCIBE"[54].

Los activos son "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. UNE 71504:2008"[55].

Las Empresas, sin importar su tamaño, todas poseen Activos que son esenciales para el desarrollo de sus actividades, dentro de los tipos de activos se encontraron los siguientes:

- ✓ Servicios informáticos: el Instituto ofrece el servicio de impresión desde un equipo de cómputo que está conectado con la impresora que se ubica en el área de secretariado.
- ✓ Datos/Información: núcleo del sistema.
- ✓ Aplicaciones de Software (aplicaciones y bases de datos).
- ✓ Equipos informáticos: Portátiles, Computadores de mesa, impresoras, etc…
- ✓ Personal Interno o Externo: Activo principal en la organización (estudiantes, docentes, administrativos).

---

[54] Instituto Nacional de Ciberseguridad (INCIBE) Vídeo SGSI - 07 (INTECO) Los activos de Seguridad de la Información. Disponible en: https://www.youtube.com/watch?v=THnQ2FH7NtU.
[55] NORMA UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430.

- ✓ Redes de comunicación: Dan soporte y ayudan a movimiento de la información, pueden ser propias o subcontratadas.
- ✓ Soporte de información: soporte físico que ayuda a almacenar toda la información de la Empresa.
- ✓ Equipo Auxiliar: los que dan soporte a los sistemas de información.
- ✓ Instalaciones: Oficinas, edificios o vehículos.
- ✓ Intangibles: Tiene que ver con la imagen y reputación de la Empresa.

Con el propósito de conocer más a fondo la situación real en cuanto a riesgos y vulnerabilidades que se presentan o pueden presentarse en EDUTEC, se emplea la técnica de investigación cualitativa y cuantitativa, a través del levantamiento de activos, observación y entrevistas a los funcionarios más relevantes de la empresa, para conocer los procesos que realizan y que medidas de seguridad toman.

4.1.1 Servicios

Con el fin de realizar la investigación en EDUTEC, fue necesario realizar un inventario detallado de los activos informáticos en donde se establece que se brinda el servicio que de impresión y fotocopiado a estudiantes y docentes, desde un equipo de cómputo que está conectado con una impresora ubicada en el área de secretariado, apoyando los procesos formativos orientados al desarrollo de las competencias específicas de los estudiantes que accedan al mundo laboral en condiciones de trabajadores o empresarios. Los datos o información sensible que se maneja es relacionado con los estudiantes, docentes, matriculas, notas y pagos de matrículas.

La función principal del Instituto es ofrecer estudio técnico, capacitado y tecnificado con proyección laboral y empresarial. Cuenta con licencias de aprobación, amparadas por la secretaria de educación y supervisada por el Ministerio de educación nacional.

4.1.2 Datos/Información

Los datos o información son el activo más valioso con el que cuenta EDUTEC, porque hacen parte de su hacer diario, ayudando a cumplir con los objetivos diseñados, brindando prestigio y buena reputación en los servicios que ofrece. Estos datos o información se encuentran en diferentes formas:

- Física, impresa o escrita en papel,
- Digitalizada y almacenada electrónicamente,
- Transmitida vía correo o e-mail,
- Vídeos
- Fotos, etc…

La información más relevante que se gestiona al interior de EDUTEC, tiene que ver con el formulario o registro de datos personales - Hábeas data, de quien diligencia al momento de manifestar querer hacer parte de la Institución como alumno en una de las carreras técnicas que se ofrece, en dónde queda registrada y concretada su vinculación, además de la forma de pago; si va a ser mediante crédito o de contado.

La documentación e información de los profesionales contratados o vinculados como docentes administrativos, denominados contratistas de módulos académicos, mediante contrato de prestación de servicios independiente, bajo la modalidad de hora catedra, de acuerdo a disponibilidad de tiempo.

El manejo de notas o calificaciones parciales y definitivas que llevan los contratistas de módulos académicos, bien sea en papel o digital a través de hojas de cálculo en Excel, como control de asistencia, entrega de trabajos y exámenes normales o Institucionales.

También la información financiera es de gran importancia porque a través de la Base de datos “MORO” se registra y lleva control de todo lo que entra y sale en cuanto a

dinero se trata y es fundamental a la hora de tomar decisiones de pagos, compras y compromisos.

4.1.3 Aplicaciones de software (Programas que maneja)

Dentro de las aplicaciones de software, el Instituto cuenta con una base de datos local, creada en Acces[56] sistema de administración de bases de datos para Microsoft Windows, con el cual pone a su alcance la capacidad de organizar, buscar y presentar información, aprovechando al máximo la potencia gráfica de Windows ofreciendo métodos visuales de acceso a sus datos y proporcionando maneras simples y directas de presentar y trabajar con la información.

La Base de Datos local: Moro - Sistema de información de estudiantes, trae los siguientes módulos.

- Estudiantes,
- Profesores,
- Matriculas,
- Notas,
- Pagos de matrículas.

La Base de datos fue creada en el programa Access o Microsoft Access, que forma parte de Microsoft Office, por uno de los directivos de EDUTEC, que es ingeniero de sistemas y es el encargado de administrarla.

Este software permite gestionar una base de datos y trae un paquete de aplicaciones que permiten realizar tareas de oficina. Posee información detallada en cada uno de los campos creados, con el fin de mantener actualizada la información importante y sensible de la Institución. La aplicación está protegida

[56] Microsoft Access. Disponible en: https://www.ecured.cu/Microsoft_Access.

mediante usuario y contraseña, permitiendo únicamente a los autorizados ingresar, modificar, generar recibo de caja, y borrar datos.

La base de datos local Moro, maneja toda la información digital importante y valiosa de la Entidad, su entorno es amigable, tiene las pestañas archivo, principal, informes, herramientas y vista. Está diseñada para extraer los siguientes datos:
En el bloque programas están las opciones grupos y profesores, en datos académicos matrículas y formulario, en recibos, las opciones pagos a matriculas, pagos por otros conceptos, imprimir recibo e imprimir recibo por otros conceptos, también se encuentran los bloques portapapeles, cerrar y salir.

El módulo profesores se almacena todos los datos personales como ubicación y ocupación, foto del docente; también toda la información académica relacionada con la vinculación de los docentes administrativos y contratistas de módulos académicos, mediante contrato de prestación de servicios independiente, bajo la modalidad de hora catedra, de acuerdo a disponibilidad de tiempo.

El módulo estudiantes reposa toda la información detallada del estudiante, como nombres, apellidos, sexo, el tipo del documento de identificación, estado civil, fecha de nacimiento, régimen de salud, discapacidad, alergias, tipo de sangre, formación, correo electrónico, estrato, teléfono fijo, teléfono móvil, ubicación, ocupación y foto actualizada del estudiante.

El módulo matriculas se registra y encuentra los datos por carrera técnica, periodo, grupo: horario, periodo, horario, semestre, valor, activo, matriculas: número, estudiante, id grupo, grupo, fecha, forma de pago y valor matricula.

El módulo abonos, se encuentra la información del estudiante, foto, documento de identidad, matriculas realizadas, ver solo retiros, recibos, historial de pagos y nuevos pagos.

El módulo notas detalla la información del estudiante, foto, documento de identidad, ficha académica, matriculas realizadas: periodo, número, grupo, carrera, valor neto y notas: código materia, nota, modo y carrera técnica.
En imprimir recibo se genera el recibo de caja como soporte del pago, el cual lleva un número consecutivo, fecha, valor, cédula de ciudadanía, firma y sello.

Por seguridad y periódicamente se hace copias de seguridad y cambios de contraseña en la base de datos Moro, por parte del Ing. encargado, quien accede remotamente desde su equipo desde la ciudad de Neiva.

Únicamente el director general y el administrador tienen acceso a la base de datos y pueden hacer modificaciones. Solo el director es quien puede hacer correcciones en el módulo de notas y autoriza pagos y anticipos.

Dentro de las aplicaciones o programas que manejan o utilizan en los equipos de cómputo de las aulas de clase o en la parte administrativa esta Microsoft office, *suite* ofimática que abarca el mercado completo en Internet e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows, dentro del paquete se encuentra los programas de *Word, Excel, Power Point, Publisher*, etc…
Se deben seguir 4 pasos que son críticos para cada análisis de brechas de seguridad de la información:

PASO 1: Seleccionar un marco de seguridad estándar: Uno de los marcos más comunes es el estándar ISO / IEC 27002: 2013 que proporciona recomendaciones

de mejores prácticas en la gestión de la seguridad de la información. Esta norma cubre las mejores prácticas para áreas de seguridad clave como la evaluación de riesgos, el control de acceso, la gestión de cambios, la seguridad física y otros.

PASO 2: Evaluar personas y procesos: El objetivo principal es entender y analizar los objetivos clave de la organización así como también su dirección estratégica. Definitivamente significa aprender qué políticas de seguridad ya existen y en qué dirección los líderes de su organización estarán llevando a su empresa durante los próximos tres a cinco años, esto implica identificar los riesgos de seguridad que estarán asociados con ella. En las buenas prácticas de seguridad deben estar involucrados todos en la empresa, debido a que muchos de los riesgos que enfrentan las redes de la empresa son causados por la intervención humana. Se debe abordar el comportamiento humano, para disminuir las amenazas a los datos. Los miembros clave del personal pueden proporcionar detalles sobre cómo se implementan los diversos controles., cuanto más sepamos

PASO 3: Recopilación de datos / tecnología: El objetivo es comprender qué tan bien funciona el programa de seguridad actual dentro de la arquitectura técnica. Como parte de este paso, es necesario comparar los controles de mejores prácticas (ISO 27002:2013) o los requisitos relevantes con los controles de la organización; es importante tomar, por ejemplo una muestra de dispositivos de red, servidores y aplicaciones para validar brechas y debilidades; revisar los controles de seguridad automatizados; y revisar los procesos de respuesta a incidentes, protocolos de comunicaciones y archivos de registro. Con una recopilación de datos y análisis, se obtiene una imagen clara del entorno técnico, las protecciones implementadas y eficacia de seguridad general.

PASO 4: Análisis: Es el paso final una vez terminadas las fases anteriores, se realizar un análisis profundo del programa de seguridad, tomando los hallazgos y

los resultados en todos los factores para crear una imagen clara y concisa del perfil de seguridad de las tecnologías de la información que incluye áreas de fortaleza y áreas donde es más necesario mejorar. Con esa información en la mano, podemos hacer recomendaciones para crear y avanzar con un plan de seguridad adecuado para la empresa. Esa hoja de ruta de seguridad debe considerar los requisitos de riesgos, personal y presupuesto, así como los plazos para completar las diversas mejoras de seguridad.

Para concluir podemos decir que realizar un análisis de brechas de seguridad no garantiza un 100% de seguridad, pero es un largo camino para certificar que la red, el personal y los controles de seguridad son robustos, efectivos y rentables.
También se encuentran instalados los programas *Corel draw*, *Dreamweaver*, *Adobe Photoshop*, *Adobe indesign*, *movie maker*, *Adobe flash*, Software contable y administrativo SIIGO, entre otros que forman parte del proceso de formación de los estudiantes.

4.1.4 Equipos Informáticos

Las aulas de sistemas están dotadas con 40 computadores portátiles de la marca *Hewlett Packard, Dell y Lenovo*, que se utilizan para la realización y desarrollo de las clases a estudiantes de la Institución.

EDUTEC cuenta con tres aulas de sistemas identificadas como:

- Aula 2 con 10 portátiles,
- Aula 12 con 16 portátiles y
- Aula 13 con 14 portátiles.

Mediante la herramienta *Dxdiag.exe*, es posible extraer la información de los equipos informáticos que hacen parte de las aulas de sistema y la parte administrativa de la Institución. En este diagnóstico se obtiene información relevante del sistema, pantalla, sonido y entrada del equipo.

Las tres aulas o laboratorios de sistemas, están dotadas con 40 computadores portátiles de la marca Hewlett Packard, Dell y Lenovo respectivamente, la mayoría tienen instalado el sistema operativo Windows 7 *Ultímate* de 32 bits y unos pocos de 64 bits; con procesador Intel ® Core ™ 2 DUO CPU, Intel ® Core ™ i3 CPU y uno que otro con Intel ® Core ™ i5 CPU, con velocidad entre 2.4 y 2.8 GHZ, con memoria de 4 GB, el monitor es de 14 pulgadas genérico, el teclado y el mouse tienen puerto PS/2. Estos equipos están al servicio de sus usuarios internos (estudiantes y docentes) para la realización y desarrollo de las clases. Es importante expresar que como medida de seguridad, el Instituto tomo la decisión de ubicar e instalar los portátiles sobre las mesas con un soporte que impide que sean extraídos o hurtados fácilmente, otra medida es que en las aulas no se puede ingresar a páginas como *Facebook y YouTube*.

La planta administrativa tiene tres equipos de cómputo de escritorio, con sistema operativo Windows 7, uno para secretaría, uno para el auxiliar administrativo y uno para el área de impresión.

El área de secretaría, está dotado con dos computadores de escritorio para el uso de las tareas y funciones diarias de la secretaria y el auxiliar, se identifican con el nombre secretaria2-pc y secretaria3-pc, marca Lenovo y Dell, con procesador Intel ® Core ™ 2 DUO CPU e Intel ® Pentium ® D CPU, poseen memoria ram de 2048 y 2560 MB – DDR3, con sistema operativo Windows 7 *Ultímate* 32 bits, unidad óptica DVD/RW, monitor Dell y Hp de 14 pulgadas, torre Lenovo y Dell, teclado Ps2 marca Dell y Genius, Mouse óptico Ps2 Lenovo y Genius respectivamente. Ambos equipos tienen conectada una una impresora Epson L380 multifuncional para todo lo relacionado con las actividades propias del puesto de trabajo.

En el área de impresión y fotocopiado hay un computador de escritorio, identificado con el nombre secretaria1-pc para el uso de estudiantes y docentes, con las siguientes especificaciones: marca *Dell Inc*, con procesador Intel ® Pentium ® D

CPU, memoria ram de 2560 MB – DDR3, sistema operativo Windows 7 Ultímate 32 bits, unidad óptica DVD/RW, monitor Dell genérico de 14 pulgadas, torre Hp, modelo del sistema L1506, teclado Ps2, marca Dell y mouse óptico Ps2 Lenovo, este equipo tiene configurada y conectada una de las impresoras Epson L380 multifuncional, para el uso de Impresiones y fotocopias.

EDUTEC, posee en sus equipos de cómputo software de Microsoft Windows con arquitectura x86 y x86-64, tipo sistema operativo Windows 7 Ultímate 32 bits, de propiedad de EDUTEC y se encuentra localizado en los computadores portátiles y de escritorio. Servidores no hay, no se cuenta con un antivirus licenciado, ni gratuito, que proteja los equipos de cómputo, sólo en las aulas de sistemas, se instaló el congelador *Deep Freeze* a los equipos portátiles, cuya función es conservar la configuración de los equipos. Cualquier cambio, ya sea malicioso o accidental, se revertirá al ser reiniciado, esto como única medida de protección.

El navegador web utilizado en los equipos de cómputo es *Google Chrome*, es el navegador web creado por la compañía *Google INC*. Considerado como el navegador más rápido del mundo, en poco tiempo que tiene desarrollado *Google Chrome* cumple con sus objetivos principales, rápido, seguro, práctico, estable y con un sentido minimalista único, que le brinda al usuario la mayor comodidad a la hora de navegar por la web. Este navegador, forma parte de los planes de expansión de la gigante Canadiense a otros campos de la web. Puede ser instalado en casi cualquier sistema operativo y está disponible en 50 idiomas. El secreto de la rapidez de *Google Chrome* se basa en la capacidad que tiene el navegador de procesar códigos de *JavaScript*, los cuales son los que se usan en la mayoría de las páginas web[57].

[57] CONCEPTODEFINICIÓN. Definición de Google Chrome. https://conceptodefinicion.de/google-chrome/

El Ingeniero encargado y custodio del área de mantenimiento de los equipos de cómputo y la red es el que tiene que velar que todo funcione perfectamente en la Institución.
EDUTEC es el propietario del inventario de equipos informáticos.

Se utilizó el formato estandarizados de Inventario de Activos de Incibe-cert.es, en donde se detalla el tipo, responsable, criticidad del activo, entro otros. En los anexos se adjunta el inventario de activos.

Dentro del equipamiento auxiliar, EDUTEC cuenta con nueve vídeos *beam* en las aulas de clase que ayudan al desarrollo de las actividades educativas, además de una impresora, un televisor y tres cámaras de vigilancia. En la tabla No. 1, se observa la relacionan de equipos auxiliares que tiene el instituto para el servicio y desarrollo de sus actividades.

Cuadro 2 Equipos auxiliares - EDUTEC.

LUGAR	CANT	ITEM	DESCRIPCIÓN
Aula 1	1	Video Beam	Marca optoma, DLP Projection Display.
Aula 2	1	Cámara de vigilancia	CCTV camera
Pasillo	1	Cámara de vigilancia	CCTV camera
Aula 3	1	Video Beam	Epson Power Lite S10+
Aula 4	1	Video Beam	Optoma, DLP Projection Display
Aula 5	1	Video Beam	Optoma TX612
Aula 6	1	Video Beam	Nec VE282. DLP. Texas instruments.
Aula 7	1	Video Beam	ViewSonic PJD5123
Aula 9	1	Video Beam	ViewSonic PJD5123
Aula 10	1	Video Beam	Epson PowerLite S8+
Aula 11	1	Video Beam	ViewSonic PJD5123
Aula 12	1	Cámara de vigilancia	CCTV camera
Oficina Director	1	Impresora	Epson L1300 Multifuncional.
Oficina Secretaria	1	Televisor	LG 49LH57OT-DJ

Fuente: La Autora.

4.1.5 Personal Interno o Externo

La planta administrativa se compone de cuatro administrativos. El director general, el coordinador académico, la secretaria y el auxiliar.

En el área de los docentes hay 24 profesionales de las diferentes áreas del conocimiento, que orientan los programas técnicos que ofrece el Instituto.

- Técnico en formación integral a la primera infancia (preescolar),
- Técnico en electrónica y comunicaciones,
- Técnico en administración empresarial (secretariado),
- Técnico en sistemas informáticos,
- Técnico en gestión contable financiera,
- Técnico en salud y seguridad en el trabajo.

En el área de sistemas hay seis docentes que tienen conocimiento y habilidades en el uso de tecnologías de la información y comunicaciones (TIC) y dieciocho en áreas diferentes.

Para el año 2018, en los dos periodos académicos se matricularon aproximadamente 750 alumnos para las diferentes carreras técnicas que ofrece EDUTEC.

4.1.6 Redes de Comunicación

Conjunto de elementos con características comunes interconectadas o conectadas a través de un medio físico común, con el objetivo de compartir y optimizar recursos a través de una disposición física en particular.[58]

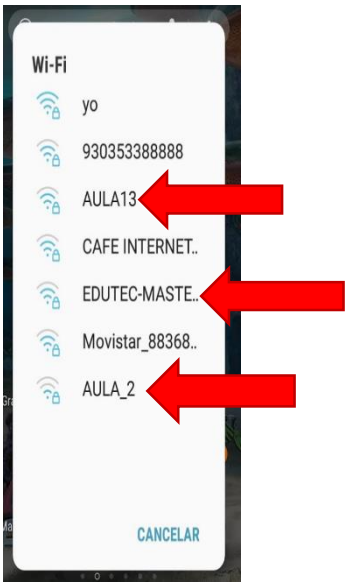
EDUTEC, cuenta con tres redes de topología híbrida, llamadas Aula 2 ubicada en el segundo piso, es una red inalámbrica, EDUTEC-MASTER2015 que está dividida

[58] http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/135_definicin_de_red_de_comunicaciones_y_su_importancia.html

en dos segmentos: uno para el aula 12 red inalámbrica y el otro para la oficina de secretaría por medio de canaleta plástica para cable UTP que conecta tres computadores y dos impresoras multifuncionales, haciendo más eficiente la transmisión y comunicación de datos; es de topología lineal y tiene funciones administrativas y por ultimo está el aula 13. Cabe aclarar que estas dos últimas están ubicadas en el primer piso. Las aulas 2, 12 y 13 son de topología estrella, cada una está conectada independiente a través de un Router.

En la ilustración 4, se observan las tres redes wifi - modo inalámbrico que tiene EDUTEC.

Ilustración 4 Redes Wifi EDUTEC



Fuente: La Autora.

Las topologías híbridas son confiables y versátiles, porque proporcionan un gran número de conexiones y caminos de transmisión de datos para los usuarios. Las redes permiten a los usuarios enviar y recibir información de forma rápida, compartir recursos y reducir costos.

El ingeniero encargado de la red, es el custodio del área de mantenimiento y el director es el representante legal del Instituto EDUTEC. La red de comunicación es de tipo aplicación y se encuentra localizado en los computadores portátiles y de escritorio. Según el encargado, la red está configurada en modo inalámbrico, con un *router* central y un *router* secundario con el SSID (*Service Set IDentifier*) o identificador de paquetes de servicio tiene el nombre oculto, están por una IP fija para conectar un # de equipos, a través de un rango de IP asignadas para los equipos de cada aula. Así tengan la clave se conectan pero no van a poder navegar.

Hay tres líneas de Internet del proveedor Movistar, una para cada aula con velocidades diferentes, el aula 2 es de 5 megas, el aula 12 es de 10 megas y el aula 13 es de 5 megas.

El sitio o portal web se denomina http://www.edutecdelosandes.com, fue diseñado con el fin de brindar información sobre las carreras técnicas que se ofrecen, además de poder realizar la inscripción en línea, donde la persona interesada deja sus datos e indica en que programa técnico está interesado; para que el personal administrativo se comunique con él. El portal web se encuentra alojado en un servidor del hosting https://www.siteground.com, empresa a la que se paga por proveer este servicio.

Se utilizan tres correos institucionales, el del director general director@edutecdelosandes.com, el del coordinador académico coordinador@edutecdelosandes.com y el de la secretaria secretaria@edutecdelosandes.edu.com.

EDUTEC, tiene dos logotipos que identifican y representan la empresa y hacen parte de la hoja membrete de los documentos expedidos y los registros realizados por la Institución. Como se aprecia en la ilustración 5, uno se compone de las letras E y D mayúscula y el otro son las mismas letras pero adicional tiene otras letras y forma la palabra Edutec de los Andes.

Logotipos que caracterizan y ponen el sello de presentación de la entidad.

Ilustración 5 Logotipos de EDUTEC

Fuente: EDUTEC.

La ilustración 6 muestra la página de inicio de Facebook que tiene el instituto, la dirección es https://www.facebook.com/edutecdelosandespitalito, en este perfil se brinda toda la información y se promocionan las carreras técnicas que oferta.

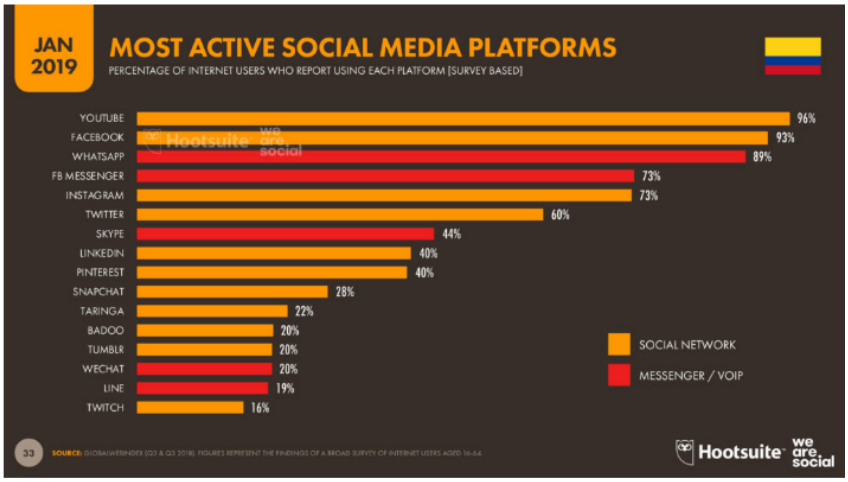
Ilustración 6 Facebook EDUTEC

Fuente: EDUTEC.

Las redes sociales con más usuarios activos en Colombia son YouTube, Facebook, Instagram, Twitter, LinkedIn, Pinterest, Snapchat, Taringa, Tumblr y Twitch.

YouTube sigue siendo una plataforma principal para crear, subir y compartir contenido audiovisual de manera masiva y con gran presencia, tal como se puede observar en la ilustración 7.

Ilustración 7 YouTube



Fuente: yiminshum.com/digital-social-media-colombia-2019/

Las mensajerías instantáneas que tienen más presencia en Colombia son WhatsApp, FB Messenger, Skype, WeChat y Line. El crecimiento en el último trimestre de la publicidad en audiencia de social media en la publicidad, demuestra que Facebook no ha crecido absolutamente en nada, con respecto al año pasado.

En audiencia por medios sociales, Facebook posee unos 32 millones de personas, según Yi Min Shum Xie[59], conferencista de marketing digital, social media y branding, quien escribió un informe de la situación digital de Colombia 2019, realizado por We Are Social y Hootsuite.

[59] SHUM XIE, Yi Min. Situación digital y social media en Colombia 2019. yiminshum.com/digital-social-media-colombia-2019/

4.2. ANALISIS DE RIESGO

El análisis de riesgo es el primer paso a tener en cuenta en la gestión de riesgo, cuyo propósito es determinar los componentes de un sistema que requiere protección, conocer las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

"Es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando"[60] Es necesario e imprescindible que las empresas inicien cuanto antes este proceso y mantenga informado a los empleados sobre el alcance que tiene dicho análisis para mejorar y corregir errores que se vienen presentado o se pueden presentar más adelante.

Para determinar e identificar las amenazas que afectan los activos de EDUTEC, fue necesario realizar un inventario detallado de todos los activos informáticos y de información.
Al realizar un buen inventario, se conoce y entiende mejor la actividad a la que se dedica la empresa, se conocen las amenazas, vulnerabilidades y se puede así calificar el impacto y consecuencias que tendrá.

La metodología Magerit es una guía práctica para analizar y gestionar riesgos en el marco ISO[61], que agrupa y tiene en cuenta los siguientes tipos de activos:

Servicios: los servicios informáticos que ofrece el Instituto (Impresión y fotocopiado)

[60] MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.
[61] Video Lección 11: Análisis y gestión de riesgos (intypedia) https://www.youtube.com/watch?v=EgiYIIJ8WnU.

Datos / Información: todos los datos al ser procesados se vuelven información corriente o sensible de la empresa, es el núcleo del sistema.
Aplicaciones de software: se utiliza la base de datos “MORO”, que almacena gran parte de la información más sensible y relevante de la Institución.
Los equipos informáticos hardware: 43 equipos de cómputo y 2 impresoras.
El personal activo principal: interno o subcontratada, etc...
Las redes de comunicación: topología híbrida.
Los soporte de información: memorias USB, disco duro externo.
Los equipos auxiliares: los que dan soporte.
Las instalaciones: oficina – vehículos.
Los intangibles: imagen – reputación.

Amenazas

Magerit cuenta con un catálogo sobre las posibles amenazas que atentan contra los activos de un sistema de información, a continuación se diligencia el siguiente cuadro, teniendo en cuenta la disponibilidad, la integridad y el grado de confidencialidad. Dentro las categorías de riesgo analizaremos desastres naturales de origen (accidental), industriales (accidental o deliberada), errores y fallos no intencionados de origen humano (accidental) y ataques intencionados de origen humano (deliberado).

Identificación de Amenazas

Los desastres naturales desafortunadamente han llenado de tristeza e impotencia el corazón de los colombianos por la incontenible fuerza de la naturaleza, por aquellos elementos del medio ambiente que son peligrosos para el hombre y que están causados por fuerzas extrañas a él. Las amenazas naturales son todos los fenómenos atmosféricos, hidrológicos, geológicos (especialmente sísmicos y volcánicos), los incendios que por su ubicación, severidad y frecuencia, tienen el

potencial de afectar adversamente al ser humano, a sus estructuras y a sus actividades.

Dentro de los desastres naturales ocurridos en Colombia, que han causado más de 500 víctimas mortales y que, por lo tanto, son considerados como los más representativos en la historia, tenemos:

- La tragedia de Armero,
- El terremoto de Cúcuta,
- El terremoto de Tumaco,
- El terremoto del Eje Cafetero,
- El sismo provocado por el volcán Nevado del Huila y posterior avalancha del Río Páez,
- El deslizamiento de Villatina,
- La tragedia de Quebrada blanca.

En el cuadro 3, desastres naturales, se diligenció la información, según el tipo de activos y amenazas que se presentan o que en el futuro se puedan presentar. De tal manera se pudo concluir que los desastres naturales que no son más que hechos que pueden suceder, sin previo aviso y de origen natural (accidental), podemos observar que el Instituto EDUTEC, no es ajeno a que se pueda presentar una situación o calamidad de origen natural, a través del fuego, agua u otro tipo de desastres naturales (sismos, Inundaciones, rayo eléctrico) que no se pueden prevenir, ni detener, porque “Nadie en el mundo puede decir que está preparado para un desastre”.

Cuadro 3 Desastres Naturales

TIPO DE ACTIVO / AMENAZA		SERVICIOS	DATO	APLICACIONES	EQUIPOS INFORMÁTICOS (Hardware)	SOPORTES DE INFORMACIÓN	EQUIPAMIENTO AUXILIAR	INSTALACIONES	PERSONAL
CÓDIGO	**DESCRIPCIÓN**								
DESASTRES NATURALES									
N.1	Fuego	X	X	X	X	X	X	X	
N.2	Daños por agua.	X	X	X	X	X	X	X	
N.*	Desastres naturales.	X	X	X	X	X	X	X	

Fuente: Metodología Magerit.

Pitalito está ubicado al sur del Departamento del Huila sobre el Valle del Magdalena y en el vértice que forman las cordilleras central y oriental a 1.318 mts sobre el nivel del mar[62] y es surcado por el río Guarapas, que en tiempos de invierno aumenta su caudal y puede provocar una avalancha o inundación. Otro hecho que es de gran preocupación es que el Nevado del Huila se mantiene en alerta amarilla, tal como lo evidencia la periodista de RCN radio DÍAZ PEÑA, Yamileth[63] en su reportaje sobre las características geológicas y geográficas del Huila que lo ubican en el mapa global de riesgo sísmico. Debido a esto está entre los departamentos con altas probabilidades sísmicas; en la zona se presenta eventos sísmicos constantes, algunos más fuertes que otros.

[62]ALCALDIA DE PITALITO. Ubicación Geográfica Pitalito. http://www.alcaldiapitalito.gov.co/web1/index.php/pitalito/informacion-general/item/1303-geografia
[63] DIAZ PEÑA, Yamileth – RCN Radio. https://www.rcnradio.com/colombia/region-central/nevado-del-huila-se-mantiene-en-alerta-amarilla.

Se debe tener en cuenta también que las instalaciones donde se encuentra funcionando EDUTEC es en el municipio de Pitalito, ubicado en el centro de la ciudad y es una casa muy antigua con un segundo piso, con una entrada principal para acceder al primer piso y una escalera en madera para subir al segundo. En el segundo piso se encuentran las aulas de clase y algunas tienen grandes puertas gruesas en madera al igual que el piso.

Por ser una edificación tan antigua es probable que llegue a presentarse eventos de incendio o inundación, como consecuencia de las instalaciones por ser antiguas.

Los eventos de tipo industrial son los que provienen de accidentes o situaciones deliberadas, es decir de acciones desarrolladas a propósito o con intención. Dichos eventos se presentan constantemente y se repite en varios ítems; alterando o afectando el normal funcionamiento de la empresa, tal como se observa en la tabla 4 de origen industrial.

Cuadro 4 De origen industrial

TIPO DE ACTIVO		SERVICIOS	DATO	APLICACIONES	EQUIPOS INFORMÁTICOS (Hardware)	SOPORTES DE INFORMACIÓN	EQUIPAMIENTO AUXILIAR	INSTALACIONES	PERSONAL
AMENAZA									
CÓDIGO	DESCRIPCIÓN								
INDÚSTRIAL									
I.6	Corte del suministro eléctrico.	X	X	X	X	X	X	X	
I.7	Condiciones inadecuadas de temperatura o humedad.	X		X	X	X	X		
I.8	Fallo de servicios de comunicaciones.		X	X	X	X	X		
I.9	Interrupción de otros servicios y suministros esenciales.						X		
I.10	Degradación de los soportes de almacenamiento de la información.	X		X	X	X	X		
I.11	Emanaciones electromagnéticas.	X	X	X	X				

Fuente: Metodología Magerit.

El fuego, los daños provocados por el agua, los desastres industriales, la contaminación mecánica, las avería de origen físico o lógico, son importantes y hacen parte de este selecto grupo; sin embargo se hace énfasis en el corte del suministro eléctrico y el fallo de servicios de comunicaciones.

Debido a los constantes cortes en el suministro eléctrico por parte de la entidad ELECTROHUILA S.A E.S.P., encargada de proporcionar el servicio de energía eléctrica a Pitalito y la región sur del Huila, “El Alcalde de Pitalito, pidió a la electrificadora del Huila, dar solución rápida a deficiencias que generan fallas constantes en servicio de energía eléctrica para Pitalito y la región sur la cual debe dar solución rápida a deficiencias que generan fallas constantes en el servicio de energía eléctrica”[64]. En EDUTEC estos cortes y cambio de voltaje afectan directamente a los equipos informáticos (*Hardware y Software*) porque en las aulas de sistema y en la parte administrativa los equipos no cuentan con UPS (Sistema de Alimentación ininterrumpida SAI), que “en el caso que haya un corte de luz o un problema eléctrico en la infraestructura suministre energía por unos minutos más para que el empleado tenga el tiempo necesario para guardar archivos de importancia y apagar el ordenador de la forma correcta”, tal como lo define Espitia Bernal[65] para evitando dañar partes internas del computador y la perdida de archivos o información valiosa para la empresa, ayudando a preservar la vida útil del computador.

En el área administrativa el equipo de cómputo de la secretaria cuenta con un estabilizador, cuya función básica es proveer de un voltaje estable (220 Volts en alimentación monofásica hogareña) para una computadora o artefacto periférico. Supliendo las posibles deficiencias del nivel de voltaje que provee ELECTROHUILA, como así también cubrirnos de algún aspecto como descargas atmosféricas o picos de tensión.

---

[64] Alcaldía de Pitalito, Huila. http://www.alcaldiapitalito.gov.co/web1/index.php/la-alcaldia/oficina-comunicaciones/boletines-de-prensa/item/606-alcalde-de-pitalito-pidio-a-electrificadora-del-huila-dar-solucion-rapida-a-deficiencias-que-generan-fallas-constantes-en-servicio-de-energia-electrica-para-pitalito-y-la-region-sur.

[65] ESPITIA BERNAL, Iván David. Administración Informática. https:/ SEYMOUR, Joseph. HORSLEY, Terry – APC by Schneider Electric. Revisión 1 - Los siete tipos de problemas en el suministro eléctrico. Informe interno 18./administacioninformatica.wordpress.com/2012/08/31/definicion-de-ups-y-su-funcion/.

“Muchos de los misterios de las fallas en los equipos, el tiempo de inactividad, el daño de software y de los datos, son resultado de una fuente de alimentación problemática[66]. Las perturbaciones en la calidad del suministro definidas por el estándar del IEEE, han sido organizadas en siete categorías: transitorios, interrupciones, bajada de tensión / subtensión, aumento de tensión / sobretensión, distorsión de la forma de onda, fluctuaciones de tensión, y variaciones de frecuencia.

Movistar Colombia[67] que es una filial colombiana de la empresa telefónica que ofrece telefonía fija y servicio de internet en las aulas de sistemas y en la parte administrativa, en donde a pesar de que cada aula tiene una línea independiente y una clave establecida para acceso a Internet, se puede observar que no todos los equipos se conectan al mismo tiempo y que se cae el servicio cuando se está navegando, evidenciando que hay fallo en los servicios de comunicaciones.

Se debe tener en cuenta que las velocidades de navegación por internet pueden disminuir por:

- ✓ Los componentes que tiene la computadora, como la velocidad del procesador, la cantidad de memoria disponible, el sistema operativo y las variables de configuración del equipo.
- ✓ La cantidad de aplicaciones ejecutándose al mismo tiempo.
- ✓ La cantidad de computadoras (u otros dispositivos) que comparten conexión a internet.
- ✓ La calidad y el estado del cableado que conecta el o los computadores a la red.

[66] Ibíd., Pág. 3.
[67] MOVISTAR - http://atencionalcliente.movistar.co/proteccion-al-usuario/pdf/Factores%20de%20la%20velocidad%20de%20Internet.pdf.

Otros factores que afectan la velocidad de acceso a internet son:

- ✓ Congestión de la red,
- ✓ Limitaciones del sitio web/servidor,
- ✓ Congestión de internet,
- ✓ Conectarse con múltiples dispositivos y limitaciones de los mismos, etc…

En Movistar[68] las conexiones vía Wi-Fi usan un espectro de frecuencias limitado (2.4 GHz), utiliza 13 canales para cualquier conexión de cualquier compañía. Estos canales no son puros, cada canal ocupa parte de los cuatro canales adyacentes, además un router emitiendo a doble banda (en Wi-Fi N) ocuparía 8 de los 13 canales disponibles el solo.

Por tal razón la empresa Movistar trabaja para mejorar las conexiones vía Wifi en entornos densamente poblados, lo cual es muy común que se produzcan colisiones o interferencias entre varios routers cercanos que están trabajando en el mismo o cercano canal. Por estas interferencias suelen hacer que la velocidad baje, que existan cortes de navegación etc… cortes y lentitud que se dan a ciertas horas (cuando coinciden en la navegación dos redes por el mismo o cercano canal) y que en otros momentos van bien (cuando trabajan solas o una de las dos no está cursando navegación).

La interrupción de otros servicios y suministros esenciales, degradación de los soportes de almacenamiento de la información y emanaciones electromagnéticas hacen parte de las amenazas industriales que se presentan en la disponibilidad de los activos que posee EDUTEC, afectando condiciones inadecuadas de temperatura, humedad, fallo en los servicios de comunicación.

[68] MOVISTAR - Mejorando el Wifi. https://comunidad.movistar.es/t5/Soporte-Fibra-y-ADSL/Mejorando-el-Wi-Fi/td-p/989996.

Por tal razón los directivos se enfrentan a más riesgos en un mundo tan complejo y digital, donde se deben conocer primero los riesgos tradicionales y emergentes que puede ayudar a crear y priorizar estrategias para capitalizar las oportunidades que también presentan estos desafíos.

Sin embargo Cambronero[69] sugiere que se debe tener en cuenta que el fuego, puede llegar y llevar a situaciones extremas según su magnitud; dependiendo del tipo de empresa y a la actividad que se dedica, también al personal que ahí labora, pues pueden quedar en la calle por la pérdida de trabajo. "Las empresas suelen ser objeto de devastadores incendios que producen grandes pérdidas económicas no solo por los bienes incendiados sino por la actividad económica que se deja de generar"

Los daños por agua también se pueden presentar y materializar en un daño, si alguien por descuido o maldad deja un grifo abierto o rompe un tubo, se presenta daño material por inundación que afecta a la Institución por daños o pérdidas que puedan sufrir los activos.

El Doctor Villaseñor[70], indica que en condiciones inadecuadas de temperatura o humedad, como es el caso en Pitalito, la temperatura generalmente varía de 17 °C a 26 °C y rara vez baja a menos de 16 °C o sube a más de 28 °C, por lo que en tiempo de altas temperaturas se puede generar problemas en las aulas de clase porque se ve la necesidad de usar los ventiladores en alta potencia y puede traer problemas de salud a las personas, como daño a los equipos informáticos. A pesar de que las instalaciones de EDUTEC son adecuadas porque sus aulas son amplias

[69] CAMBRONERO IBAÑEZ, Antonio. Redacción cuadernos de seguridad - 23 marzo, 2018. Disponible en https://cuadernosdeseguridad.com/2018/03/pautas-para-prevenir-incendios-en-la-industria/.
[70] VILLASEÑOR, Benjamín, UHMASALUD. Salud laboral: La temperatura en el trabajo. Disponible en https://www.uhmasalud.com/bid/285662/salud-laboral-la-temperatura-en-el-trabajo.

y ventiladas a excepción de una que otra y cuenta también con corredores amplios “El ambiente climático puede estar condicionado a la temperatura ambiente, los materiales de construcción de las oficinas, la humedad y la ventilación” por lo que una temperatura inadecuada provocará desde estrés, problemas respiratorios, incomodidad hasta lesiones graves.

La Interrupción de otros servicios y suministros esenciales, se da cuando en el municipio o en el área donde se encuentra EDUTEC, se programan o se suspende el servicio de agua, afectando el normal funcionamiento en las baterías sanitarias para el uso de estudiantes, docentes y administrativos.

Degradación de los soportes de almacenamiento de la información**:** los soportes de almacenamiento son los que cumplen un rol fundamental en la Institución para tener respaldo de la información que es guardada en equipos de cómputo, memorias extraíble USB (*Universal Serial Bus*), también llamada lápiz de memoria, lápiz USB, memoria externa, pen *drive o pendrive*; es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información y los discos duros externos.

Para CEPAL[71], “Los dispositivos de almacenamiento son de bajo costo, pero presentan desventajas, tales como su rápida degradación en el tiempo, la velocidad con la que pueden quedar obsoletos, tasas de error relativamente frecuentes, limitado tamaño o riesgos de seguridad a los que puedan estar sujetos debido a su portabilidad. Se recomienda que su uso esté limitado al almacenamiento de copias (nunca archivos de datos maestros) y deberán siempre contar con un respaldo en medios más seguros”

[71] CEPAL Biblioguías – Biblioteca de la CEPAL. Métodos de almacenamiento y respaldo de datos. Disponible en: https://biblioguias.cepal.org/c.php?g=495473&p=4398069.

Emanaciones electromagnéticas: “La emanación es la acción y el efecto de emanar, verbo que procede del latín “*emanare*”, integrado por el prefijo “e” que indica “desde” y por “*manare*” con el significado de manar o brotar”. Para Panda Security[72] las emanaciones electromagnéticas pueden ser un vector de ataque, tal como lo demuestra TEMPEST, “aunque los sistemas de una organización no salgan de espacios físicos aparentemente seguros e incluso no estén conectados, no son completamente invulnerables”.

La mayoría de vulnerabilidades en infraestructuras críticas se deben a ataques más convencionales como el ***ransomware***, software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. El virus actúa lanzando una ventana emergente en la que pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (*bitcoins* por ejemplo).

Según Panda security[73] uno de los *Ransomware* más famosos es el **Virus de la Policía**, que tras bloquear el ordenador infectado lanza un mensaje simulando ser la Policía Nacional y advirtiendo que desde ese equipo se ha detectado actividad ilegal relacionada con la pederastia o la pornografía. Para volver a acceder a toda la información, el malware le pide a la víctima el pago de un rescate en concepto de multa.

[72] PANDA SECURITY - TEMPEST y EMSEC: ¿Son posibles los ciberataques a partir de las emanaciones electromagnéticas? https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberataques-emanaciones-electromagneticas/.

[73] PANDA SECURITY. ¿Qué es un Ransomware? https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/.

Panda Security[74] redacto un informe denominado “Un nuevo modelo de ciberseguridad ha nacido”. En donde explica que este tipo de vulnerabilidades pueden evitarse de manera sencilla con medidas adecuadas y soluciones avanzadas de ciberseguridad (seguridad informática), garantizando la inviolabilidad de los sistemas críticos para el devenir de una organización o incluso un país. La empresa panda *Adaptive Defense* es una *suite* de ciberseguridad que integra soluciones de protección de punto final, con servicios de 100% en atestación y amenaza de caza e investigación, con un control absoluto de todos los procesos en ejecución, y la reducción de la superficie de ataque.

En la tabla 5 errores y fallos no intencionados, se identificaron y diligenciaron las amenazas que afectan los activos de la institución, dónde podemos ver que hay errores, vulnerabilidades, etc. que suceden o acontecen sin intención alguna.

La palabra error[75] proviene del latín “errare” que significa “fallar o equivocarse”. Este es un término que puede estar involucrado a cualquier cosa o circunstancia que pueda existir en el mundo. Los errores y fallos no intencionados son de origen humano (accidental), tienen que ver con el personal interno (empleados actuales o salientes) de la empresa que no hacen bien su trabajo por desconocimiento o por maldad, que no sigue instrucciones o procesos. Se puede presentar también que un empleado insatisfecho que ya no labora en la Institución destruye, esconde o borran información sensible con el fin de hacer daño.

[74] PANDA SECURITY. Un Nuevo Modelo de Ciberseguridad ha nacido. https://www.pandasecurity.com/es/business/adaptive-defense/.
[75] CONCEPTO DEFINICIÓN. Error. https://conceptodefinicion.de/error/

MAGERIT, en su libro II catálogo de elementos[76], especifica que en la correlación de errores y ataques se pueden presentar estas tres combinaciones:

Las amenazas que son solo errores, nunca son ataques deliberados,

Las amenazas que nunca son errores, son siempre ataques deliberados o pensados.

Las amenazas que pueden producirse por error o deliberadamente.

[76] Ministerio de Hacienda y Administraciones Públicas - Secretaría General Técnica - Subdirección General de Información, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid, octubre de 2012. Pág. 48 Disponible en: http://administracionelectronica.gob.es/.

Cuadro 5 Errores y fallos no intencionados

TIPO DE ACTIVO / AMENAZA		SERVICIOS	DATO	APLICACIONES	EQUIPOS INFORMÁTICOS (Hardware)	SOPORTES DE INFORMACIÓN	EQUIPAMIENTO AUXILIAR	INSTALACIONES	PERSONAL
CÓDIGO	**DESCRIPCIÓN**								
ERRORES Y FALLOS NO INTENCIONADOS									
E.1	Errores de los usuarios	X	X	X	X				
E.2	Errores del administrador	X	X	X	X				
E.4	Errores de configuración	X	X	X	X				
E.8	Difusión de software dañino	X	X	X	X	X			
E.14	Escapes de información	X	X	X					
E.15	Alteración accidental de la información	X	X	X					
E.18	Destrucción de información	X	X	X					
E.19	Fugas de información	X	X	X					
E.20	Vulnerabilidades de los programas (Software).	X	X	X	X	X	X		
E.21	Errores de mantenimiento/actualización de programas (Software).	X	X	X	X	X	X		
E.23	Errores de mantenimiento/actualización de programas (Hardware).	X			X	X	X		
E.24	Caída del sistema por agotamiento de recursos.	X	X	X	X				
E.25	Perdida de equipos - Robo.	X	X		X	X	X		
E.28	Indisponibilidad del personal.	X	X						X

Fuente: Metodología Magerit.

En las empresas o a nivel personal estos errores y fallos no intencionados de origen humano (accidental) son los más comunes y los que con más frecuencia se presentan por desconocimiento, engaño o por exceso de confianza. En EDUTEC, se presentan los siguientes:

Errores de los usuarios: como usuarios están los estudiantes, docentes y administrativos que hacen uso de las aulas de sistemas. En las clases se trabaja directamente con los equipos de cómputo y en las horas libres de descanso o cuando no hay actividad académica, se prestan los computadores para realizar trabajos u otras actividades. La empresa Welivesecurity - ESET[77] da a conocer 11 errores de seguridad que a diario se cometen., muchos de los errores se dan por instalar parches, ya que la mayoría de las filtraciones de datos no solo se debe a errores humanos, como hacer clic en un vínculo malicioso, sino también a sistemas informáticos cuyo software está desactualizado. Otros errores de seguridad que se cometen son ser demasiado confiados, contraseñas débiles o reutilizadas, dar datos de más en las redes sociales, creer que “eso no va a pasar”, navegar con conexiones desprotegidas, ignorar las advertencias de los certificados SSL, descargar apps desde fuentes desconocidas y liberar dispositivos móviles.

Los equipos de cómputo del área de secretaría, coordinación, las aulas de sistemas, el equipo de impresiones y hasta los computadores personales de docentes y estudiantes, son constantemente infectados por los virus que se traspasan a través de las memorias USB o discos extraíbles. En donde se ocultan las carpetas, se borra toda la información o se crea accesos directos.

Errores del administrador: los errores de los administradores de TI (tecnología de la información) aumentan la pérdida de datos en entornos corporativos, tal como lo

[77] WELIVESECURITY – ESET. 11 errores de seguridad que probablemente sigues cometiendo. https://www.welivesecurity.com/la-es/2015/07/22/11-errores-de-seguridad-sigues-cometiendo/

explica Nicholas Green[78], director de Kroll Ontrack Iberia empresa proveedora de recuperación de datos que ha publicado los principales errores que suelen cometer los administradores del sistema y que conducen a una pérdida de datos o un mayor tiempo de inactividad de la red.

Los estudiantes del último semestre de sistemas reciben clases donde se les enseña a obtener claves de redes sociales como facebook y acceder a la red wifi del instituto haciendo vulnerable los sistemas de información del Instituto, por la información sensible que se lleva (notas, Pagos, datos personales, etc…). Existiendo la posibilidad de acceder a ella y ser usada en contra de la Institución.

Difusión de software dañino: software dañino toma su nombre del término “software malicioso” y es diseñado para entrar en el sistema del computador para causar un daño significativo. Guillen Hernández[79], expresa que se manifiesta marcando el teclado, robando palabras clave, observando los navegadores utilizados, desplegando ventanas no deseadas en la pantalla, recibiendo correos electrónicos no deseados, redirige el navegador hacia páginas fraudulentas, reporta información personal a otros servidores sin consentimiento y hasta puede hacerle recibir pornografía.

RIOJASALUD[80] indica que el correo electrónico es un medio de comunicación más barato que el teléfono o el correo postal, pero también una excelente herramienta comercial. La información más peligrosa que podemos recibir a través del correo

[78] GREEN, Nicholas. Director de Kroll Ontrack - Iberia. https://diarioti.com/los-errores-de-los-administradores-de-ti-aumentan-la-perdida-de-datos-en-entornos-corporativos/88229.
[79] GUILLEN HERNÁNDEZ, Oscar Armando. Universidad Juárez Del Estado De Durango. https://oacch.files.wordpress.com/2016/02/software-dac3b1ino-2.pdf.
[80] RIOJASALUD - Correo electrónico (virus informáticos) https://www.riojasalud.es/salud-publica-y-consumo/consumo/el-rincon-del-consumidor/4766-correo-electronico-virus-informaticos

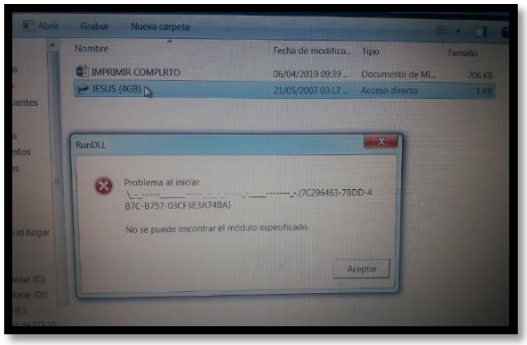
electrónico, son los virus informáticos lo que le convierte en el principal medio de propagación de códigos maliciosos.

Su acción comienza al abrir un archivo infectado, el código que conforma al virus se guarda en memoria y se añade a los programas que se ejecuten ya que toma el control del sistema operativo. Dependiendo de la programación del virus es el daño que causa en el equipo infectado.

Los problemas que se presentan a diario en los equipos de cómputo de la Institución, se presentan por el uso del correo electrónico personal, el ingreso de memorias USB, discos extraíbles en el equipo de impresiones o en los equipos de cómputo de las aulas de sistema, los cuales cuentan con conexión a Internet para realizar trabajos e investigaciones, pero no son seguros porque no cuentan con un antivirus que escanee periódicamente los dispositivos, alertando al usuario o bloqueando las páginas, provocando que se infecten con virus que crean accesos directos y ocultan las carpetas o los archivos.

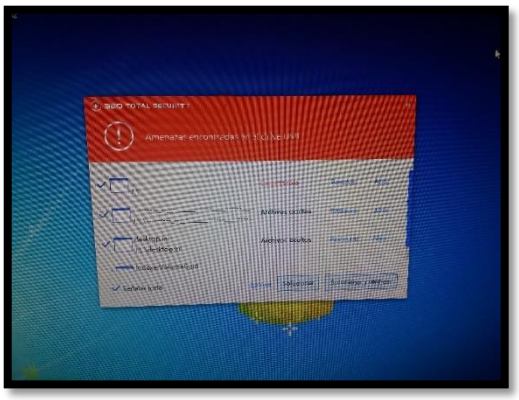
Aquí se evidencian algunos de los casos antes mencionados que se presentan en EDUTEC, por medio de la ilustración 8 virus de acceso directo en memoria USB, en la ilustración 9 un virus que rompe la carpeta que se encuentra dentro de la memoria USB, la ilustración 10 muestra el reporte del escaneo del antivirus, donde especifica qué tipo de virus troyano se encuentra en la memoria USB, el motor de análisis, la ruta, el tamaño etc., y en la ilustración 11 como los virus crean accesos directos y en las carpetas de la memoria USB.

Ilustración 8 Virus acceso directo en memoria USB



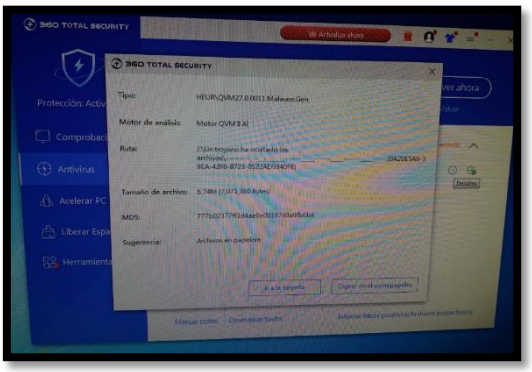
Fuente: La autora

Ilustración 9 Virus carpeta rota de memoria USB



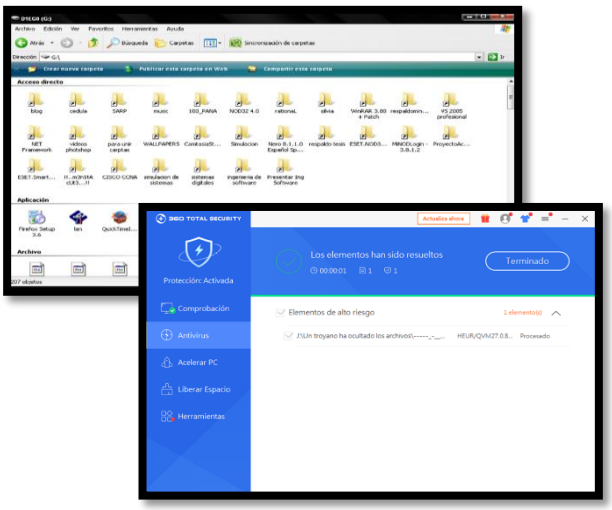
Fuente: La autora

Ilustración 10 Virus acceso directo en memoria USB



Fuente: La autora

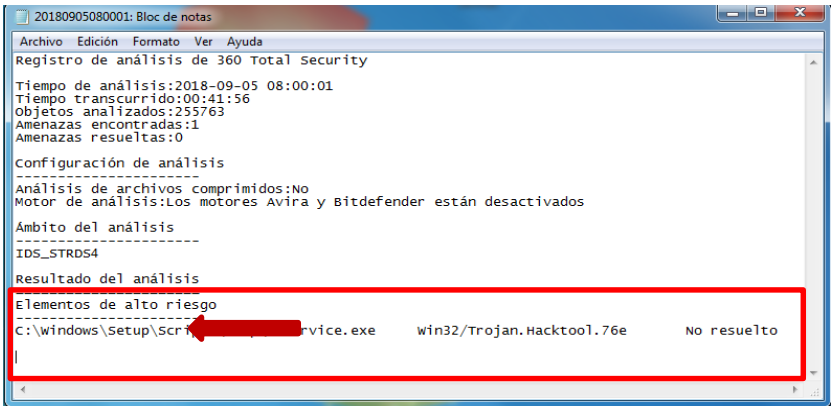
Ilustración 11 Virus que crea accesos directos y oculta las carpetas de la memoria USB (Drivesguideinfo)



Fuente: La autora

En la ilustración 12 se muestra el registro del análisis a una memoria USB, luego de ser ingresada en uno de los equipos del aula de sistemas. En un equipo personal, fuera de la Institución se escanea la memoria USB a través del Antivirus 360 Total Security, líder en detección antivirus; el cual arrojo como resultado un virus troyano, catalogado como elemento de alto riesgo.

Ilustración 12 Registro de análisis Antivirus 360 Total Security



Fuente: La autora

Errores de configuración: Un error de configuración se genera por una escritura incorrecta de las líneas del archivo de configuración o que el hardware este limitado a una configuración que no requiera de tantos recursos como esta, esto conlleva a una ejecución defectuosa del programa informático o sistema operativo o a la imposibilidad de ejecutarse. Los equipos de cómputo de las aulas y de impresión necesitan mantenimiento correctivo y preventivo periódicamente o cuando sea necesario para poder realizar satisfactoriamente los trabajos y practicas requeridas en el área de estudio.

Alteración accidental de la información: Alterar es cambiar las características, la esencia o la forma de una cosa, en este caso la información de la Institución, como activo principal e importante. En EDUTEC, se maneja información sensible y relevante utilizada en los procedimientos y ejecución de sus actividades, son el caso

de las notas de estudiantes, pagos, datos personales de estudiantes, docentes, administrativos, movimientos bancarios, entre otros. Se han evidenciado modificaciones en algunos casos como al digitar las notas los docentes en una hoja de Excel, como prevención de esto se protege la columna asignada de cada docente para evitar cambios o alteraciones por error, desconocimiento o daño.

Destrucción de información: Por el uso y manejo de información confidencial en el Instituto es clave, tener en cuenta como se debe proceder a la destrucción de esta información una vez determinado que ya no se necesita ni se va a necesitar, pero para ello hay que hacer una buena destrucción que impida el acceso de otros a estos datos. Es necesario que todo el proceso sea seguro, que garantice que la información desaparezca y no pueda ser recuperada, siempre comprobando antes que no se va a necesitar nunca más lo que se quiere eliminar y tras un tiempo prudencial, esto debe quedar consignado en un manual de buenas prácticas de conocimiento y uso de todo el personal de la Institución.

Escape o fuga de información: Bortnik, Sebastián[81] específica que se le denomina al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma (a todos o a un grupo reducido). Es el principal temor de las empresas latinoamericanas en materia de seguridad informática, según revelan los datos recopilados por el Eset Security Report 2012[82], es importante que todos los empleados en las empresas, implementen buenas prácticas de administración de los datos a partir de una comprensión de la problemática y una descripción de las principales amenazas informáticas que a diario se presentan. Según, gerente de educación & servicios de Eset Latinoamérica “Un empleado seguro es aquel que

[81] BORTNIK, Sebastián. 13 Apr 2010 - 12:17PM https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion.
[82] ESET LATINOAMERICA. Cómo prevenir y evitar la fuga de información empresarial. https://www.portafolio.co/mis-finanzas/ahorro/prevenir-evitar-fuga-informacion-empresarial-100890.

cuenta con la educación adecuada para utilizar los recursos de la empresa con eficiencia y seguridad" teniendo siempre presente que los tres pilares fundamentales de la seguridad de la información son confidencialidad, integridad y disponibilidad, el objetivo principal de este trabajo es diseñar un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001, a la Institución EDUTEC, para prevenir y evitar todo tipo de escape o fugas de información.

Vulnerabilidades de los programas (Software – Hardware): OSI oficina de seguridad del internauta[83] lanzó infografía enmarcada dentro de la campaña. Los ciberdelincuentes, ¿quiénes son? donde muestra información interesante que le sirva a las empresas y al público en general. Por eso hay que tener en cuenta cuales son las debilidades que tiene un sistema operativo, software o sistema, como permite a un atacante quebrantar la confidencialidad, integridad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Se debe tener en cuenta que tener en cuenta que todos los sistemas informáticos sea software o hardware están expuestos a vulnerabilidades, agujeros de seguridad, que si no se corrigen a tiempo, permiten que personas que realizan actividades ilegales en internet, hoy en día llamados ciberdelincuentes, quienes dispones de una gran variedad de programas informáticos, se aprovechen de errores humanos que son la puerta de entrada para ejecutar códigos maliciosos, utilizar la ingeniería social, robar credenciales, chantajear y extorsionar a víctimas potenciales instalando software malicioso (Malware) para tener control parcial o total de los dispositivos y así obtener beneficio.

[83] (OSI) Oficina de Seguridad del Internauta de INCIBE - ¿Quiénes son los ciberdelincuentes y qué buscan? https://www.osi.es/es/campanas/los-ciberdelincuentes-quienes-son/quienes-son-los-ciberdelincuentes-y-que-buscan.

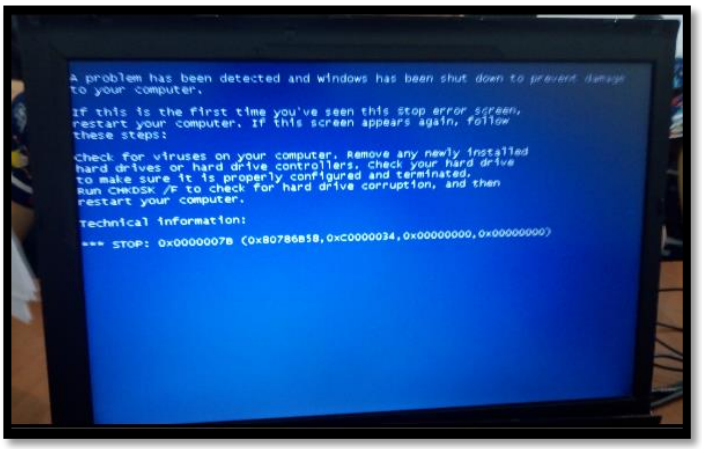
Entre ellos encontramos troyanos, gusanos, *ransomware, spyware, rootkit, adware*.

También se especializan en hacer ataques de denegación de servicio a través de solicitudes o peticiones que provocan algún fallo en un recurso o servicio hasta colapsarlo y dejarlo inaccesible, como es el caso de infectar los equipo de cómputo y controlarlos de manera remota. Ejemplo *Botnets* y Redes *Zombie.*

Errores de mantenimiento/actualización de programas (Software - Hardware): Dentro de los errores y fallas en los equipos de cómputo de las Aulas de sistemas, área de secretariado, impresiones y fotocopiado, se han presentado fallas de memoria, calentamiento del procesador, fallas del disco duro. En cuanto al software fallas en el sistema operativo, presencia de virus y conflicto entre programas.

La ilustración 13 muestra un mensaje de error en uno de los portátiles del aula 2 “Se detectó un problema y se cerraron ventanas para evitar daños en su computadora. Compruebe si hay virus. Retire cualquier disco duro recién instalado”.

Ilustración 13 Portátil Aula 2 Edutec



Fuente: La autora

Caída del sistema por agotamiento de recursos: MAGERIT[84] en su catálogo de elementos, muestra como la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Por tanto, las caídas del sistema pueden producirse debido a errores de software, problemas de Entrada /salida y mal funcionamiento del hardware.

Es importante y necesario hacer mantenimiento constante preventivo y correctivo en los equipos de cómputo de la Institución, con el fin de optimizar el rendimiento del sistema operativo, verificar que el sistema no se encuentre infectado por virus, troyano o algún tipo de malware, para esto es necesario contar con un antivirus que escanee periódicamente los ordenadores y detecte problemas de seguridad.

Perdida de equipos - Robo: González, Cecilia, corresponsal del diario LA NACIÓN[85] expresa en su artículo el preocupante panorama de seguridad en el Huila. El comandante del Ejército, General Nicasio Martínez se reunió en Neiva con empresarios y dirigentes de la región quienes denunciaron el regreso de la extorsión en el Huila. "Empresarios de la región y comerciantes expresaron su preocupación por la ola de inseguridad en distintas modalidades". Si bien es cierto que se ha incrementado la delincuencia en Colombia, en Pitalito también se presenta hurtos a las empresas y establecimientos comerciales, es por eso que EDUTEC, toma medidas preventivas a este caso de eventos como:

- ✓ Sistema de alarma de seguridad: Utilizada como elemento de seguridad pasiva que avisa en caso de intrusión de personas, inicio de fuego, desbordamiento de un tanque, entre otras.

[84] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html
[85] GONZALEZ, Cecilia - LA NACIÓN. Preocupante panorama de seguridad en el Huila. https://www.lanacion.com.co/2019/02/28/preocupante-panorama-de-seguridad-en-el-huila.

Como medida de seguridad ante cualquier clase de robo, fraude o atraco; el Instituto cuenta con alarma y cámaras de vigilancia marca CCTV camera en la entrada principal y pasillos.

- ✓ Platina de protección contra robo a los equipos de cómputo portátiles de las Aulas, instalada en las estaciones de trabajo.

- ✓ Los equipos de cómputo del área de secretariado, se encuentran asegurados a través de correas plásticas.

Indisponibilidad del personal: (No disponible). El grupo soluciones horizonte GSH[86], documenta sobre las etapas que se deben llevar para un proceso de selección de personal, el cual surge en primer lugar por la necesidad de la empresa de contar con un personal idóneo y acorde para realizar las funciones necesarias y llevar a cabo satisfactoriamente su objeto social o el cumplimiento de sus objetivos económicos y metas económicas. La selección de personal bajo esa premisa se convierte en uno de los procesos más importante dentro de la organización puesto que dependiendo de una buena gestión en este sentido, la empresa cumple su proyección de crecimiento.

En la tabla 6 se establece que amenazas a través de ataques intencionados, se pueden registrar en Edutec. Es importante tener en cuenta que un ataque informáticos es un intento organizado e intencionado causado por una o más personas para causar daño o problemas a un sistema informático o red. El problema de la propagación de los virus informáticos puede ser significativo teniendo en cuenta que un virus puede dañar o eliminar datos del equipo, usar el programa de correo electrónico para propagarse a otros equipos o incluso borrar todo el contenido del disco duro.

[86] GSH GRUPO SOLUCIONES HORIZONTE - Etapas de un proceso de Selección de Personal. https://www.gsh.com.co/blog/etapas-de-un-proceso-de-seleccion-de-personal.

Cuadro 6 Ataques intencionados

TIPO DE ACTIVO / AMENAZA		SERVICIOS	DATO	APLICACIONES	EQUIPOS INFORMÁTICOS	SOPORTES DE INFORMACIÓN	EQUIPAMIENTO AUXILIAR	INSTALACIONES	PERSONAL
CÓDIGO	**DESCRIPCIÓN**								
ATAQUES									
A3	Manipulación de los registro de actividad (Log)	X	X	X	X				
A4	Manipulación de la configuración.	X	X	X	X	X			
A5	Suplantación de la identidad del usuario.	X	X	X	X				
A6	Abuso de privilegio de acceso.	X	X	X	X	X			
A8	Difusión de software dañino.	X	X	X	X	X			
A11	Acceso no autorizado.		X	X					
A15	Modificación deliberada de la información.	X		X	X	X			
A18	Destrucción de información.		X	X	X	X	X	X	
A19	Divulgación de información _ Revelación de información.	X	X	X		X			
A22	Manipulación de programas.	X	X	X	X	X			
A23	Manipulación de los equipos - Daño.	X			X	X	X		
A25	Robo.	X			X	X	X	X	
A26	Ataque destructivo.	X			X	X	X	X	
A29	Extorsión.		X	X					X
A30	Ingeniería social.	X	X	X					X

Fuente: Metodología Magerit.

Al ver la lista que Magerit ha proporcionado sobre el tipo de ataques que se presentan, se puede concluir que la era digital llegó a las empresas y hogares para a través de equipos, dispositivos y aplicaciones poder acercarnos y ver el mundo con todas sus novedades, pero consigo trajo también problemas que afectan tanto el hardware, software, los datos personales, los activos y servicios de las empresas afectando y destruyendo la imagen o reputación por los riesgos que trae consigo, por el tipo de amenaza, por las vulnerabilidades que se crean y los ataques a las redes informáticas e intimidad de una empresa o persona (s).

Gómez Vieites[87] en la ponencia tipos de ataques e intrusos en las redes informáticas a la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos o a acceder a la información guardada o transmitida por el sistema".

Manipulación de los registro de actividad (*Log*): registro en español. ANKAMA SUPPORT[88] establece que *log* es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado. Son archivos de texto normales, sirven para detectar dónde y en qué momento se ha producido un error, son una fuente de información muy valiosa.

[87] GÓMEZ VIEITES, Álvaro. Ponencia - Tipos de ataques e intrusos en las redes informáticas. https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf.
[88] ANKAMA SUPPORT. https://support.ankama.com/hc/es/articles/203790076--Qu%C3%A9-es-un-log.

El control y manejo de los equipos de cómputo del instituto lo tiene el ingeniero encargado del mantenimiento preventivo y correctivo, él es el autorizado de manipular los registros de actividad.

Manipulación de la configuración: es hacer cambios, alteraciones o adaptando una aplicación software o un elemento hardware al resto de los elementos del entorno y a las necesidades específicas del usuario, para conseguir un fin determinado, como en este caso directamente configurar.

Suplantación de la identidad del usuario: son abusos informáticos cometidos por delincuentes para estafar a sus víctimas y obtener información personal, contraseñas, etc. de forma ilegal. El *Phishing* termino en inglés, mediante el uso de la ingeniera social, suplanta la identidad de una persona o empresa de confianza en una aparente comunicación oficial electrónica, puede ser vía *email*, WhatsApp, redes sociales, llamadas telefónicas o mensajes.

Abuso de privilegio de acceso: ONA SISTEMS[89] empresa experta en ciberseguridad, ciberdefensa y cumplimiento, especializada en seguridad informática e infraestructura, estableció un listado de 10 vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas, dentro de los cuales se encuentra el abuso de privilegios y los errores humanos, como los mayores riesgos en las empresas. Muchos de los usuarios pueden llegar a abusar de los privilegios de acceso de datos legítimos para fines no autorizados. Por ejemplo: suministrar información confidencial de un cliente, sustraer información de la compañía para su propio lucro.

[89] ONA SYSTEMS, Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas. https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas.

La estrategia para lograr esta solución está relacionada con la política de control de acceso que se aplican no sólo a lo que los datos son accesibles, pero ¿cómo se accede a los datos? Al hacer cumplir las políticas de seguridad web, sobre cosas como la ubicación, el tiempo, el cliente de aplicación y el volumen de los datos recuperados, es posible identificar a los usuarios que están abusando de los privilegios de acceso.

Difusión de software dañino: La forma más común de propagar o expandir software dañino son a través de virus, gusanos, troyanos, *adware* y *spyware*. Estos programas malignos entran al equipo de cómputo por medio de la red, pero también se pueden introducir por medio de correos electrónicos, mensajes instantáneos, discos, CD, y USB. Tal y como se presenta en EDUTEC.

Acceso no autorizado: Delta Asesores[90] el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del 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”. El Artículo 269ª tiene que ver con el acceso abusivo a un sistema informático así: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

[90] DELTA ASESORES - Ley de Delitos Informáticos en Colombia. https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia.

Secretaria Distrital del Hábitat[91] Al respecto es importante aclarar que en la Ley 1266 de 2008 se dictan las disposiciones generales del habeas data y 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.

Modificación deliberada de la información: la información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que se presenten. Alterar o modificar información relevante de la empresa, sin autorización o de forma accidental, de información crítica, sin conocimiento de los propietarios. Es por eso que se debe pensar en asignar un usuario a cada uno de los funcionarios que tienen acceso a los datos y establecer permisos y atributos con los que puede trabajar.

Introducción de información falsa: "la información falsa es la base de todo fraude" El ingeniero de sistemas Hervé Falciani[92], se convirtió en un símbolo de la lucha contra el fraude fiscal cuando sacó a la luz una lista con más de 130.000 posibles evasores fiscales con cuenta en el banco HSBC. Falciani, en la ponencia que ha pronunciado, «Sociedades justas y sinceras. Filosofía, ética y algoritmos», pone de manifiesto la importancia del concepto de realidad para analizar las noticias falsas (*fake news*).

Las noticias falsas pueden extenderse si no se incluye un concepto de diversidad. ¿Quién difunde noticias falsas en muchos casos? Un hacker al servicio de los intereses de un país. Si no hay modo de establecer la no-diversidad de las fuentes, no estamos hablando de información, sino de opinión. La diversidad del origen de

[91]SECRETARIA DISTRITAL DEL HÁBITAT - Ley 1266 de 2008. https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008.
[92]FALCIANI, Hervé. Universitat Oberta de Catalunya. https://www.uoc.edu/portal/es/news/entrevistes/2018/046-herve-falciani.html.

la información es el criterio de veracidad. Otro gran enemigo de la veracidad es la velocidad: los medios se copian unos a otros para llegar antes. Es capital la relación entre las noticias falsas y todo tipo de fraude: del voto, bancario, fiscal...

Destrucción de información: Es necesario dar disposición final adecuada a los documentos que ya han cumplido con el ciclo de vida de la información, el cual es determinado por las tablas de retención documental y lo dispuesto en la ley según el sector económico.

La destrucción efectiva de la documentación física o impresa que genera una empresa, sobre todo cuando contiene datos de carácter personal, tiene una labor previa que si no se realiza correctamente puede incurrir en incumplimiento de la Ley 1581 de 2012, Régimen General de protección de datos personales. Por tal razón es necesario establecer en las políticas y controles de seguridad de EDUTEC, establecer cuál será el procedimiento para la destrucción de dicha información que en su momento fue relevante, con el fin de proteger la información personal de los clientes, usuarios e incluso de empleados de la empresa.

Divulgación de información - Revelación de información: Irish Vivien[93] consultora, abogada especializada en el registro de patentes se pronuncia sobre lo que un empleado debe saber sobre el secreto comercial o la divulgación de información confidencial. En todo el mundo, la legislación protege la información comercial de carácter confidencial, es decir, los secretos comerciales.
La revelación de información constituye el principal mecanismo a través del cual se garantiza la transparencia, la ética, la rendición de cuentas empresarial y el respeto de los derechos de los usuarios y genera relaciones de confianza con todos sus

[93] IRISH, Vivien. OMPI – ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL. Divulgación de información confidencial. https://www.wipo.int/sme/es/documents/employees_confidentiality.htm.

grupos de interés. Se considera información reservada o confidencial toda aquella que sea de competencia exclusiva de la empresa o institución.

Manipulación de programas: Consiste en modificar los programas existentes en el sistema o en insertar nuevos programas, dentro de los tipos de delitos informáticos, encontramos:

- Fraudes cometidos mediante manipulación de computadoras:
  - Manipulación de los datos de entrada,
  - Manipulación de programas,
  - Manipulación de los datos de salida,
  - Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo.
- Falsificaciones informáticas:
  - Como objeto: Cuando se alteran datos de los documentos almacenados en el equipo de cómputo.
  - Como instrumentos: Los computadores pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.
- Daños o modificaciones de programas o datos computarizados:
  - Sabotaje informático,
  - Virus,
  - Gusanos,
  - Bomba lógica o cronológica.
- Acceso no autorizado a servicios y sistemas informáticos:
  - Piratas informáticos o hackers,
  - Reproducción no autorizada de programas informáticos de protección legal.

Manipulación de los equipos: Los equipos informáticos de la Institución, son importantes tanto por la actividad económica a la que se dedica, como por la información y procesos que se posee digitalizados y almacenados en la Base de

datos “MORO”. Casi toda la información de una organización hoy día, está informatizada, es decir se conserva en equipos informáticos. Consecuentemente, es esencial que estos equipos estén protegidos de cualquier amenaza externa y del entorno más próximo para prevenir o evitar robos, accesos no deseados o pérdidas importantes. ISOTOOLS - ISO 27001[94] en un SGSI es esencial contar con controles de los equipos informáticos, por ejemplo como medida preventiva cuando un equipo deja de funcionar o se piensa reutilizar o eliminar de la organización, hay que asegurarse que no contienen información sensible de la misma, que todo se ha borrado y que es imposible su recuperación. Si no es posible borrarla se debe pensar en destruir directamente el equipo en lugar de reutilizarlo. La norma ISO-27001 implantada en una organización protege la información que ésta maneja, y en el caso que estuviera almacenada en equipos informáticos se debería de aislar elementos que necesiten una protección especial, evaluar los impactos de posibles desastres en los alrededores como incendios, fugas de agua y salvaguardar los equipos de fallos de energía, para ello usar un sistema de alimentación Ininterrumpida, proteger el cableado de energía y telecomunicaciones que porten datos, mantenerlos separados y si fuera posible ponerlos bajo el suelo, guardar los papeles y soportes informáticos en habitaciones cerradas o armarios cuando no se estén usando, activar el bloqueo de pantalla con contraseña para proteger los equipos cuando no esté el empleado en su sitio de trabajo.

Robo: Abogado[95] El término robo se utiliza ampliamente para referirse a los delitos relacionados con la sustracción de los bienes de una persona sin su permiso. Sin embargo, el robo tiene un significado jurídico muy amplio que puede abarcar más de una categoría, y varios grados, de delitos. El robo se define a menudo como la sustracción no autorizada de los bienes de otra persona con la intención de privarla

[94] ISOTOOLS - ISO 27001 Seguridad de los equipos informáticos. https://www.isotools.org/2014/09/09/iso-27001-seguridad-equipos-informaticos.
[95] ABOGADO - ¿Qué es el robo? https://www.abogado.com/recursos/ley-criminal/descripcion-general-del-robo.html.

permanentemente de ellos. Dentro de esta definición, se encuentran dos elementos claves:

1) tomar la propiedad de otra persona y

2) la intención necesaria de privar a la víctima de sus bienes de forma permanente

Ataque destructivo: Fajardo de la Espriella[96], destaca en el documental de El Heraldo denominado “En el futuro los ciberataques serán más destructivos”, el reporte de ciberseguridad de mitad de año de Cisco en el 2017, donde revela que las actividades maliciosas venideras “serán más perjudiciales”, en comparación a los tradicionales. La conclusión es que pueden ser inmensamente más perjudiciales que los ataques tradicionales, debido a que pueden dejar a las empresas sin ninguna opción a recuperarse. Los atacantes continuaron beneficiándose de una variedad de engaños vía correo electrónico a empleados o vendedores, una técnica conocida como "phishing". Esta modalidad dio pérdidas por 1.300 millones de dólares en 2018, según el reporte.

Extorsión: esta técnica es uno de los delitos con mayor ocurrencia, según Puig Carles, Ignacio[97] dentro de los delitos informáticos esta figura cobra una forma especial con la “extorsión” y “amenazas” que puede sufrir una persona por internet, solicitando contenido sexual o a menores utilizando las redes sociales; pero también puede producirse a través de ciberataques a una página web o blog, atacando su estructura y funcionamiento o colapsando sus servidores y a cambio solicitar dinero para que todo vuelva a funcionar como antes.

[96] FAJARDO DE LA ESPRIELLA, Estefanía, EL HERALDO. En el futuro los ciberataques serán más destructivos. https://www.elheraldo.co/ciencia-y-tecnologia/en-el-futuro-los-ciberataques-seran-mas-destructivos-385293.

[97] PUIG CARLES, Ignacio, LEGALIS CONSULTORES. Delitos informáticos 9 – chantaje informático. https://www.legalisconsultores.es/2015/04/delitos-informaticos-9-chantaje-informatico/

OPD - Open Data Security[98] indica que la extorsión es una figura que se encuentra entre los delitos de:

- ✓ Apoderamiento: cuando hay ánimo de lucro,
- ✓ Estafa: porque requiere que el sujeto pasivo realice u omita un acto o negocio jurídico,
- ✓ Amenazas: porque el sujeto activo coacciona al pasivo para la realización del negocio jurídico.

Además, la extorsión es un delito pluriofensivo, es decir ataca a varios bienes jurídicos como propiedad, integridad física y libertad.

Ingeniería social: Técnicas de engaño. En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una habilidad que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos[99].

En el cuadro 7 catálogo de amenazas para cada activo de Magerit, se ven reflejadas las principales amenazas, 38 en total a considerar en el análisis de riesgos realizado a EDUTEC.

[98] FORO DE SEGURIDAD - Foro de Profesionales Latinoamericanos de Seguridad. Qué es la extorsión. www.forodeseguridad.com.
[99] DNP Departamento Nacional de Planeación – Guía metodológica para la administración de riesgos en seguridad de la información. https: //colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

Cuadro 7 Catálogo de amenazas

DESASTRES NATURALES
Fuego
Daños por agua
Desastres Naturales
INDÚSTRIAL
Corte del suministro eléctrico
Condiciones inadecuadas de temperatura o humedad
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Degradación de los soportes de almacenamiento de la información
Emanaciones electromagnéticas
ERRORES Y FALLOS NO INTENCIONADOS
Errores de los usuarios
Errores del administrador
Errores de configuración
Difusión de software dañino
Escapes de información
Alteración accidental de la información
Destrucción de información
Fugas de información.
Vulnerabilidades de los programas
Errores de mantenimiento/actualización de programas (Software)
Errores de mantenimiento/actualización de programas (Hardware)
Caída del sistema por agotamiento de recursos
Pérdida de equipos - Robo
Indisponibilidad del personal
ATAQUES
Manipulación de los registros (Log)
Manipulación de la configuración
Suplantación de la identidad del usuario
Abuso de privilegio de acceso
Difusión de software dañino
Acceso no autorizado
Modificación deliberada de la información
Destrucción de información
Divulgación de información - Revelación de información
Manipulación de programas
Manipulación de los equipos
Robo
Ataque destructivo
Extorsión
Ingeniería social

Fuente: La autora

4.3. VALORACIÓN DE LOS RIESGOS

El uso diario y constante de tecnologías de la información y comunicaciones (TIC) trae consigo grandes beneficios evidentes para los usuarios y el progreso de las empresas; pero también da lugar a ciertos riesgos que de no gestionarse y tomar medidas de seguridad pueden ser fatales para el desarrollo de las actividades, hasta llegar a acabar con el buen nombre, reputación y continuidad de la misma.

Para la valoración de los riesgos, una vez diligenciada en su totalidad la tabla de amenazas probables para los activos de la organización, según la "Metodología Magerit", se identificó riesgos y amenazas que atentan contra los activos del sistema de información de la Institución. Para poder medir y determinar la probabilidad de ocurrencia y el impacto que este tendría, se tomaron en cuenta cuatro (4) criterios donde 1 es (Bajo), 2 (Medio), 3 (Alto) y 4 Muy Alto.

En el cuadro 8 cálculo de la probabilidad, se da a conocer los criterios que se establecieron para medir y calcular la probabilidad de riesgo.

Cuadro 8 Cálculo de la probabilidad

PROBABILIDAD		
CUANTITATIVO	**CUALITATIVO**	**DESCRIPCIÓN**
1	Bajo	La amenaza se puede materializar más o menos una vez cada año.
2	Medio	La amenaza se puede materializar más o menos una vez cada mes.
3	Alto	La amenaza se puede materializar más o menos una vez cada semana.
4	Muy Alto	La amenaza se puede materializar más o menos una vez al día.

Fuente: La Autora.

Como se observa en el Cuadro 9 cálculo del impacto, se mide y calcula por el método cuantitativo y cualitativo el impacto del riesgo.

Cuadro 9 Cálculo del impacto

IMPACTO		
CUANTITATIVO	**CUALITATIVO**	**DESCRIPCIÓN**
1	Bajo	El daño derivado de la materialización de la amenaza tiene consecuencias relevantes para la Institución.
2	Medio	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la Institución.
3	Alto	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la Institución.
4	Muy Alto	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves reseñables para la Institución.

Fuente: La Autora.

El cuadro 10, criterios de aceptación del riesgo, especifica el rango y descripción de la aceptación del riesgo en la institución.

Cuadro 10 Criterios de aceptación del riesgo

ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento

Fuente: La Autora.

Cálculo del Riesgo

Se realiza el análisis cuantitativo, calculando:

Para cálcular el riesgo, se da valor a la amenaza según la probabilidad de que se llegue a presentar x el impacto derivado si se materializa; donde B es (Bajo), M (Medio), A (Alto) y MA (Muy Alto), tal como se observa en el cuadro 11 Cálculo del riesgo.

Cuadro 11 Cálculo del Riesgo

RIESGO / VALORACIÓN		PROBABILIDAD			IMPACTO			RIESGO			
		BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO	MUY ALTO
DESASTRES NATURALES								1 - 3	4	6	9
R1	Fuego		2			2		4			
R2	Daños por agua.		2			2		4			
R3	Desastres naturales.		2			2		4			
INDUSTRIAL											
R4	Corte del suministro eléctrico.		2			2		4			
R5	Condiciones inadecuadas de temperatura o humedad.	1			1			1			
R6	Fallo de servicios de comunicaciones.		2			2		4			
R7	servicios y suministros esenciales.	1					3	3			
R8	Degradación de los soportes de almacenamiento de la información.	1				2		2			
R9	Emanaciones electromagnéticas.			3			3	9			
ERRORES Y FALLOS NO INTENCIONADOS											
R10	Errores de los usuarios		2			2		4			
R11	Errores del administrador			3			3	9			
R12	Errores de configuración		2				3		6		
R13	Difusión de software dañino			3			3	9			
R14	Escapes de información			3			3	9			
R15	Destrucción de información			3			3	9			
R16	Alteración accidental de la información			3			3	9			
R17	Fugas de información			3			3	9			
R18	Vulnerabilidades de los programas (Software).			3			3	9			

R19	Errores de mantenimiento/actualización de programas (Software).			3			3	9
R20	Errores de mantenimiento/actualización de programas (Hardware).			3			3	9
R21	Caída del sistema por agotamiento de recursos.		2				3	6
R22	Perdida de equipos - Robo		2			2		4
R23	Indisponibilidad del personal.	1			1			1
ATAQUES								
R24	Manipulación de los registro de actividad (Log).	1			1			1
R25	Manipulación de la configuración.	1				2		2
R26	Suplantación de la identidad del usuario.			3			3	9
R27	Abuso de privilegio de acceso.		2				3	6
R28	Difusión de software dañino.			3			3	9
R29	Acceso no autorizado.			3			3	9
R30	Modificación deliberada de la información.			3			3	9
R31	Destrucción de información.			3			3	9
R32	Divulgación de información _ Revelación de información.			3			3	9
R33	Manipulación de programas.	1				2		2
R34	Manipulación de los equipos - Daño.		2			2		4
R35	Robo.		2			2		4
R36	Ataque destructivo.		2				3	6
R37	Extorsión.		2				3	6
R38	Ingeniería social.		2				3	6

Fuente: La Autora.

Se realizó el cálculo del riesgo, mediante un análisis cuantitativo dónde se evalúa la probabilidad de que se presente la amenaza y el impacto de que este ocurra. Este proceso es el que determina el valor del riesgo, recordemos que el valor menor o igual a 4 para EDUTEC será considerado de baja importancia, pero los valores mayores que 4 son significativos y de alarma, porque indica que hay que actuar inmediatamente y proceder a planear su tratamiento, para eliminar o bajar su nivel de criticidad.

La probabilidad es el cálculo matemático que evalúan las posibilidades que existen de que una cosa suceda cuando interviene el azar, es por eso que se debe anticipar a los acontecimientos que pueden o van a ocurrir, para poder predecir tanto peligros como oportunidades para el negocio o actividad que se está desarrollando.

Luego de realizar el cálculo del riesgo, el diagnostico detectó que hay 38 amenazas de riesgo que se pueden materializar y ocasionar daños que perjudican la continuidad e imagen del Instituto en cuanto al sistema de información en su disponibilidad, integridad y confidencialidad. Extrayendo un poco los datos, se observa que existe la probabilidad de riesgo de 16 amenazas con un nivel alto, 15 medio, y 7 bajo, las cuales se deben tratar, monitorear y asumir.

En cuanto al impacto que puede producir estos riesgos a través de las amenazas antes señaladas, donde observamos que 23 son de nivel alto, 12 medio y 3 bajo. De tal manera que las amenazas que están en nivel muy alto y alto, son la prioridad a tratar, eliminar o minimizar y los de nivel medio se deben reducir y controlar en cuanto a seguridad de la información se refiere. No podemos olvidar que el daño derivado de la materialización de la amenaza tiene consecuencias muy graves para la Institución y que los criterios de aceptación del riesgo menores de 4 son considerados poco reseñable y los mayores a 4 son los que se deben proceder a tratar rápidamente.

En el reporte anual de ciberseguridad de Cisco 2018[100], se presentan los últimos avances en la industria de seguridad diseñados para ayudar a las empresas y usuarios a defenderse contra los ataques, ofrece información sobre las técnicas y estrategias que utilizan los adversarios para romper esas defensas y evadir la detección. También subraya las principales conclusiones del estudio comparativo de capacidades de seguridad de Cisco 2018, que examina la postura de seguridad de las empresas y sus percepciones acerca de su preparación para defenderse de los ataques.

El análisis produjo una lista de los 10 principales que muestra que el grupo más frecuente de extensiones de archivos maliciosos en un 38% eran los formatos de Microsoft Office como Word, PowerPoint y Excel, que son usados diariamente en todos los procesos que se llevan en EDUTEC para el desarrollo de sus actividades.

SEMANA – Tecnología[101] De acuerdo al balance entregado por Comparitech, una plataforma especializada en el análisis de servicios tecnológicos, Colombia sufre problemas significativos de ciberseguridad pero esas falencias no son tan críticas si se comparan con las de otros países de la región, e incluso del mundo desarrollado.

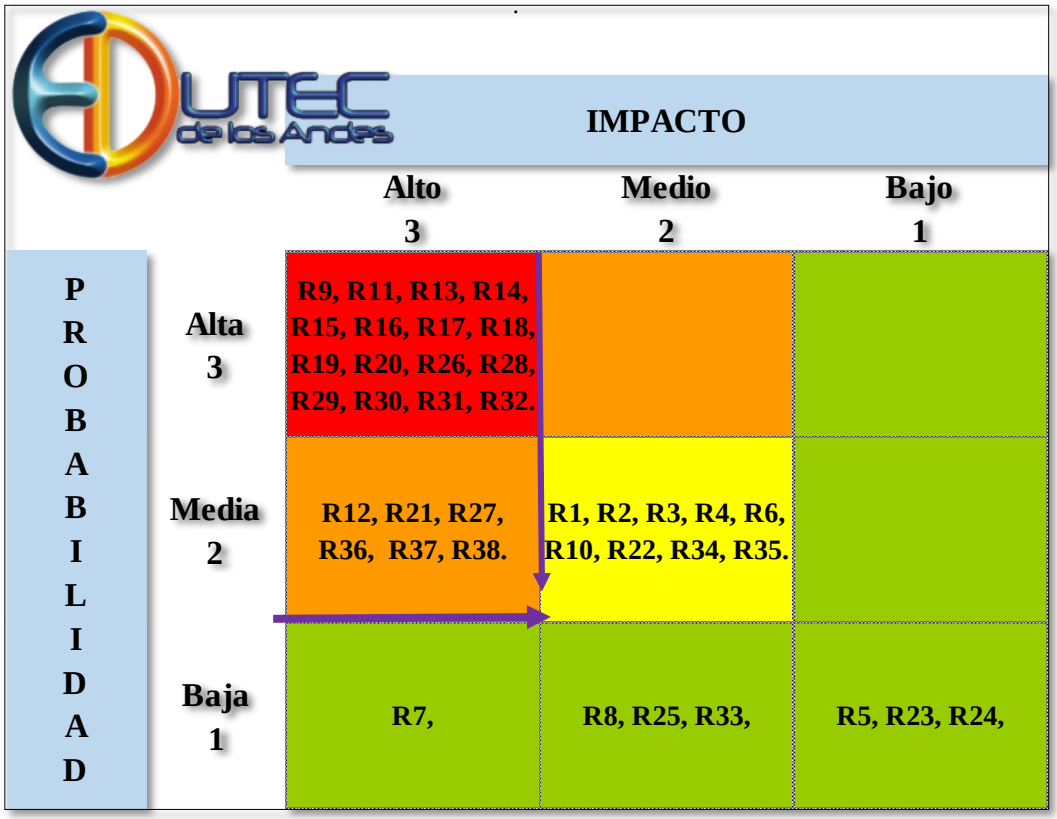
Para mitigar (reducir o atenuar) estos riesgos de desastre que se presentan en EDUTEC, se debe empezar reduciendo o eliminando los riesgos existentes, o aceptándolos, para que a través de los preparativos, procedimientos y sistemas de alerta, poder buscar disminuir las pérdidas y daños de la ocurrencia de estos fenómenos peligrosos que agreden la imagen y reputación de la empresa.

---

[100] CISCO - Reporte Anual de Ciberseguridad de Cisco 2018. https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf.
[101] SEMANA – Tecnología. Así está Colombia en el ranking de ciberseguridad mundial. https://www.semana.com/noticias/seguridad-informatica/103543.

A continuación se presenta el cuadro 12 matriz de riesgo, en dónde se ve reflejado la valoración que tomaron los riesgos, distinguiéndolos por colores según su nivel de criticidad, los cuales traen consigo consecuencias graves reseñables para la institución, especificando que el color rojo tiene un valor alto de 9, el color naranja medio de 6 junto con el amarillo y el color verde como bajo, que varía de 1 a 3 su valor, según lo leve que resulte.

Cuadro 12 Matriz de Riesgo



Fuente: La Autora.

Luego de darle valoración a los riesgos, se realiza la matriz de riesgo, donde se maneja probabilidad baja, media, y alta por impacto alto medio y bajo. Se agruparon las amenazas según el valor dado y representado como MA (Muy Alto) de color rojo, A (Alto) de color naranja, M (Medio) color amarillo y B (Bajo) de color verde.

En el cuadro 13 grupos de amenazas catalogadas, se dividió en 4 criterios, así: Desastres naturales con 3 amenazas, de origen industrial 6, errores y fallos no intencionados 14 y ataques intencionados 15, para un total de 38 amenazas detectadas con una valoración muy alta 16 identificada con el color rojo por considerarse las más catastróficas, 9 en el nivel alto muy críticos, de color naranja, 6 medio críticos con color amarillo y 7 bajo de color verde, como los más leves. Estas amenazas fueron encontradas en los sistemas de información del EDUTEC, las cuales deben ser asumidas, tratadas, reducidas y eliminadas.

Cuadro 13 Grupo de amenazas catalogadas.

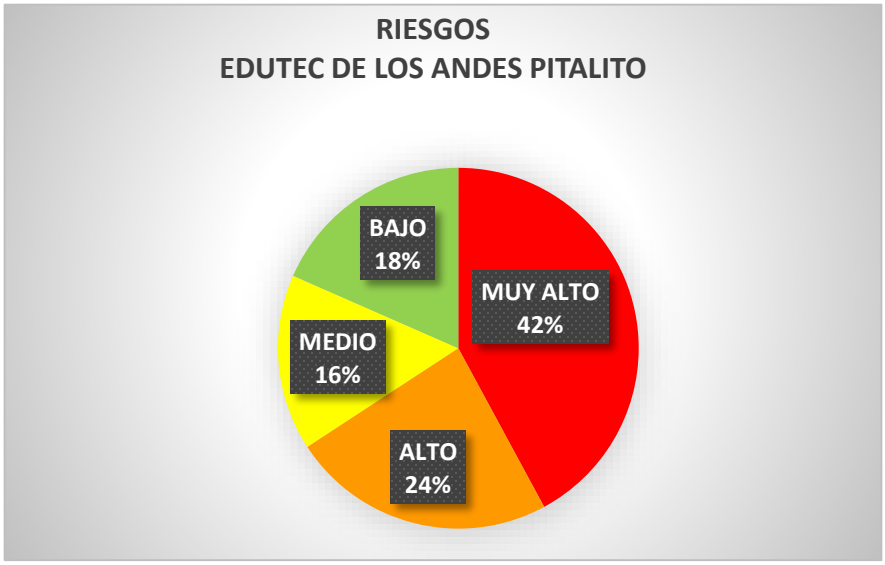
CATASTROFICO	MUY ALTO	16
MUY CRITICO	ALTO	9
CRITICO	MEDIO	6
LEVE	BAJO	7

Fuente: La Autora.

Del 100% de las vulnerabilidades que presenta Magerit en el catálogo de amenazas que atentan contra los activos de un sistema de información, se identificaron 38 vulnerabilidades en EDUTEC, con un porcentaje del 42% en el nivel muy alto catastrófico, un 24% alto nivel crítico, 16% medio y 18% bajo, como se puede

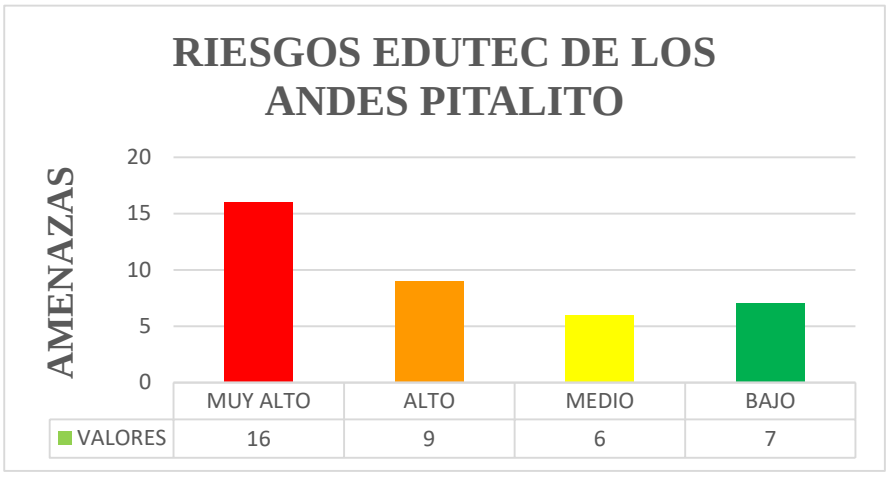
apreciar en la ilustración 14 de la gráfica circular y en la ilustración 15 de columnas con valores según el riesgo.

Ilustración 14 Gráfica circular con valores según riesgo



Fuente: La Autora.

Ilustración 15 Gráfica de columnas con valores según riesgo



Fuente: La Autora.

4.4. POLÍTICAS Y CONTROLES DE SEGURIDAD

Luego de realizar y conocer el inventario de activos informáticos y de información, para poder ejecutar el análisis de riesgo, cuyo objetivo final es diseñar un sistema de gestión de seguridad de la información (SGSI) para la Institución EDUTEC, argumentada en la norma ISO/IEC 27001; se proponen las siguientes políticas y controles de seguridad, con el fin de proteger y salvaguardar su bien más preciado, como lo es la información.

4.4.1 POLÍTICAS DE SEGURIDAD INFORMATICA

Corletti Estrada[102], una política de seguridad bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI, todo esto con el apoyo de las directivas que ayudan a incentivar a los involucrados a un buen manejo y aplicación de medidas y técnicas con el fin de salvaguardar y garantizar la seguridad de las tecnologías de información.

Este documento debe ser revisado y aprobado por sus directivos, manejado y controlado por el área de sistemas, en cabeza del ingeniero encargado de esta área y debidamente explicado a los empleados antiguos y a los nuevos al momento de su ingreso, con el objetivo de que todos los funcionarios conozcan lo importante que es la protección de la información. También se recomienda solicitar su compromiso para el cumplimiento de dichas normas a partir de la firma de un documento de consentimiento, para tranquilidad de las partes.

Al conocer y trabajar con datos reales que hacen parte de la información sensible y valiosa que utiliza el instituto EDUTEC y luego de identificar 38 vulnerabilidades,

[102] CORLETTI ESTRADA, Alejandro. ISO-27001 LOS CONTROLES (Parte I). Disponible en: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf.

con amenaza de riesgo de las cuales 16 tienen un porcentaje del 42% en un nivel catastrófico muy alto, 9 con un 24% en nivel crítico alto, 6 con un 16% critico medio y 7 con el 18% de nivel leve bajo; se procede a organizar una política de seguridad cuyo objetivo es definir los principios para identificar, analizar, evaluar, gestionar y comunicar los lineamientos que se deben seguir para que estos eventos no atenten con la continuidad y reputación de la Institución.

Para crear la política de seguridad se tomó en cuenta los riesgos mayores a 4, dentro de ellos se encuentra un 16% en el nivel medio, 24% alto y un 42% muy alto, todo esto sumado da un 82% de nivel crítico en cuanto a riesgos que debe tratar y eliminar EDUTEC, para que no siga atentando contra sus sistemas de información. Por tal razón se evalúa y propone la siguiente política de seguridad.

A. POLITICAS DE SEGURIDAD FISICA

1 **Acceso físico:** el ingreso a las instalaciones de la Institución se da normalmente a través de la puerta principal, para todos los estudiantes, docentes, administrativos y público en general; en algunas ocasiones y dada la necesidad, se utilizará la reja metálica para controlar y proteger el acceso a personal que no tenga relación directa con el Instituto como prevención de hurto o asalto.

   En la oficina del coordinador se encuentra ubicado un pequeño centro de telecomunicaciones, donde se monitorean las cámaras de seguridad de la entrada y pasillos. El paso será restringido al público en general, sólo los directivos o el personal autorizado, podrá ingresar, observar o manipular las cámaras en este lugar.

   En el área de secretariado solo tendrá acceso y uso de los equipos de cómputo el personal autorizado para realizar las labores propias del cargo, cada uno con

un usuario y clave de identificación de ingreso a la base de datos (Moro), planilla de notas, entre otros.

A las tres aulas de sistemas, tienen accesos todos los usuarios internos (estudiantes, docentes, administrativos), bien sea para recibir clase o para desarrollar trabajos e investigaciones, bajo la supervisión o autorización del personal docente o de secretaría.

Al equipo que está al servicio de impresiones, puede acceder todo tipo de usuario, aplicando medidas preventivas para el uso y la conservación de su unidad extraíble. No podrá acceder como administrador, ni hacer cambios al sistema.

Sólo el personal autorizado por el director, coordinador o el encargado del área de mantenimiento, podrá mover, cambiar o extraer los equipos de cómputo en la Institución.

Los equipos estarán protegidos y ubicado de acuerdo con los controles necesarios para mantener un ambiente idóneo, en cuanto a temperatura, humedad, inundación, electricidad, etc… de acuerdo con lo establecido en la política.

Riesgos de seguridad en el acceso físico: según Parson[103], los ataques de ingeniería social, que hoy en día son los más comunes, porque pueden acceder físicamente al sistema, a través de una persona que vaya a hacer una reparación, un electricista o un administrador de red, este puede ser un intruso disfrazado para robar información sensible de la empresa, la cual puede ser física o digital. La mayoría de los sistemas operativos tienen formas de ganar

[103] PARSON, Aaron ¿Cuáles son las diferencias entre acceso lógico y acceso físico? https://techlandia.com/cuales-son-diferencias-acceso-logico-acceso-fisico-info_202346/

acceso si el usuario tiene acceso físico y si el objetivo es robar información, eliminar un disco puede ser una operación rápida o ataques más sutiles, como agregar una conexión a otra privada, puede también ser llevado a cabo rápidamente.

Por tal razón es indispensable establecer un tipo de protección contra el acceso físico y lógico sin autorización, lo cual se puede llevar a cabo mediante métodos o procedimientos que sean la clave para la seguridad y asumir que el acceso no autorizado puede suceder. Además de la seguridad física y el software de protección, el software de audio y monitoreo son importantes para determinar si ha ocurrido una amenaza y priorizar eventos para que un operador los supervise de forma rápida.

2 **Protección Física:** es el conjunto de elementos que conforman un plan de seguridad, para proteger un espacio determinado con el fin de evitar daños y minimizar amenazas. Para prestar un buen servicio de seguridad es necesario identificar los posibles riesgos y amenazas que hay en el lugar y buscar los elementos físicos que se requieran para suministrar una excelente protección.

SEGURIDAD SUPERIOR[104] plantea que las amenazas que se pueden bloquear con los elementos de la seguridad física, son los incendios, robos, secuestros, homicidios, suplantación y robo de información, que se analizan y designan según la probabilidad de amenaza (altamente probable, probable, poco probable y probabilidad desconocida)

3 **Centro de datos:** No hay.

[104] SEGURIDAD SUPERIOR. ¿Qué es la Seguridad Física? https://www.seguridadsuperior.com.co/que-es-la-seguridad-fisica.

4 **Infraestructura:** para Ceupe[105], hacen parte del conjunto de sistemas; todos los ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos; junto con la manera que se ha elegido para gestionarlos (incluye procesos y herramientas de gestión de los equipos, de medición de su rendimiento, de seguridad ante incidencias y catástrofes además de los sistemas operativos básicos).

En el instituto ya hay unas reglas o procedimientos establecidos por el director general, específicamente la secretaria y auxiliares son los encargados de hacer que se cumplan, como es el caso del paso o acceso a la oficina del coordinador académico y a las aulas de clase del primer y segundo piso tienen acceso restringido a personal no autorizado. Por tanto en horas donde hay baja afluencia de estudiantes en cada una de las jornadas o poco personal administrativo, la reja de la puerta de entrada debe permanecer con candado y evitar así que se entre sin permiso cualquier individuo que pueda atentar con la integridad personal o material de la empresa.

El área de sistemas es el encargado de resguardar los equipos de cómputo, controlando su ubicación física. Como medida de protección los equipos de cómputo se encuentran agarrados y fijos a la mesa con una platina de metal y los cables del monitor, teclado y mouse con una correa de plástico por debajo de los escritorios.

Ante cualquier clase de robo, fraude o atraco, EDUTEC, cuenta con alarma y cámaras de vigilancia marca CCTV camera.

[105] CEUPE – CENTRO EUROPEO DE POSTGRADO. La infraestructura tecnológica. https://www.ceupe.com/blog/infraestructura-tecnologica.html.

Este sistema de alarma es un aplicativo que envía información de alerta a las autoridades o activa una sirena para irrumpir en la tranquilidad del espacio y poner en estado de emergencia el lugar.

Una alarma por sí sola no evita una situación de hurto, lo que realmente hace es crear una alerta, algunas lo hacen solo por medio del sonido, mientras otras suenan y envían mensajes o llamadas automáticamente a los números de teléfono que estén configurados.

Los sistemas de alarmas funcionan con sensores de movimiento, gas, humo y agua, que activan y envían la alerta. Este es un elemento indispensable para tener una óptima seguridad física. Aunque también pueden activarse por medio de un botón de pánico que se ubica en un lugar clave del establecimiento.

Circuito cerrado de televisión (CCTV), sistema de video vigilancia, que permite observar todo un espacio por medio de cámaras de seguridad enlazadas y conectadas a pantallas de transmisión. Usualmente las pantallas de transmisión se agrupan en un cuarto donde hay personal de seguridad que se encarga de vigilar lo que sucede en el entorno, sin necesidad de estar fuera.

5 **Instalaciones de equipos de cómputo:** la instalación del equipo de cómputo, quedara sujeta a los siguientes lineamientos:

Los equipos ubicados en las aulas de sistemas y demás dependencias, se instalaran en un lugar adecuado, lejos del polvo y que no interfiera con el tráfico de las personas.

El área de tecnología y mantenimiento, como las directivas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones de los computadores ubicados en las aulas, secretaría y coordinación.

Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezcan la dirección y el área de tecnología y mantenimiento.

6 **Control:**

El administrador del área de tecnología y mantenimiento debe llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.

Los encargados del área de tecnología son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

Las directivas de EDUTEC deberá reportar al administrador del área de tecnología y mantenimiento cuando un empleado deje de laborar o de tener relación con la empresa con el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos asignados al usuario.

El empleado, en caso de retiro, deberá tramitar ante el área de tecnología y mantenimiento paz y salvo correspondiente.

7 **Respaldos:** copia de seguridad o en inglés *backup copy*.

La base de datos Moro será respaldada periódicamente en forma automática y manual, según los procedimientos generados por el encargado para tal efecto; que permita tener contingencia y continuidad de negocio.

El portal web estará alojado en un servidor del hosting https://www.siteground.com.

Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, con los estándares de calidad para almacenamiento de medios magnéticos.

Para reforzar la seguridad de la información, los usuarios de las dependencias de secretaría, coordinación y del área de tecnología y mantenimiento, deberán hacer bajo su criterio, respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio. Los respaldos de la base de datos Moro serán responsabilidad absoluta únicamente del encargado.

Se realizara copia de respaldo para asegurar y recuperar la información después de alguna falla, estableciendo un nivel de seguridad apropiado, por lo que esta copia se hará de forma periódica generando información 100% exacta y completa.

El administrador del área de tecnología y mantenimiento no podrá remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

8 Recursos de los usuarios

Uso:

Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de EDUTEC, de acuerdo con las políticas que en este documento se mencionan.

Los usuarios deberán solicitar apoyo del área de Tecnología y mantenimiento ante cualquier duda o daño en el manejo de los recursos de cómputo.

El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquello que sea ajeno a la Institución, tales como cadenas, publicidad, memes y propaganda comercial, política, social, etc.).

Los empleados No deberán hacer uso constante de redes sociales personales como *Facebook, WhatsApp, Twitter, Instagram*, etc. o juegos en línea que sirve de distracción en la realización de las actividades por las que fue contratado durante su horario de trabajo. Pero si hacer uso de las redes sociales y demás herramientas tecnológicas Institucionales para mejorar la imagen de la empresa, lograr notoriedad de marca y promocionar productos o servicios, bajo la supervisión de los directivos de EDUTEC.

9 Derechos de Autor:

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Institución bajo ninguna circunstancia sin la autorización escrita del director general o del coordinador académico. No está permitido instalar ningún programa en el computador sin dicha autorización o la clara verificación de que el instituto posee una licencia que cubre dicha instalación.

No está autorizada la descarga de Internet de programas informáticos no autorizados por la dirección o el encargado del Área de tecnología y mantenimiento de la Institución.

No se tolerará que un empleado realice copias no autorizadas de programas informáticos.

No se permitirá que un empleado cargue o descargue programas informáticos no autorizados de Internet.

No se consentirá que un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

Si se descubre que un empleado ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado, suspendido o despedido.

Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.

Si un usuario desea utilizar programas informáticos autorizados por el instituto en su hogar, debe consultar con las directivas o con el encargado del área de tecnología y mantenimiento para asegurarse de que ese uso este permitido por la licencia del editor.

El personal encargado del área de tecnología y mantenimiento deberán revisar los computadores constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si EDUTEC posee licencias para cada una de las copias de los programas informáticos instalados. Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

El Instituto autoriza el uso de programas informáticos de diversas empresas externas. El Instituto no es dueño de estos programas informáticos o la documentación vinculada con ellos y, a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.

Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

Los usuarios no descargarán ni cargarán programas informáticos no autorizados por la dirección a través de Internet.

Los usuarios no realizarán intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

El empleado o usuario que se entere de cualquier uso inadecuado que se haga en la Institución de los programas informáticos o la documentación vinculada a estos deberán notificar al director, coordinador académico o en su defecto al encargado del área de tecnología y mantenimiento.

Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

Los empleados que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias. Dichas sanciones pueden incluir pensiones y despidos justificados.

B. POLITICAS DE SEGURIDAD LÓGICA

1 Red:

El propósito principal que tiene las redes es servir en la transformación e intercambio de información dentro de la institución entre usuarios, dependencias, oficinas y hacia afuera a través de conexiones con otras redes.

El área de tecnología y mantenimiento no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito de las directivas del instituto.

No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la institución.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la Empresa y se usarán exclusivamente para actividades relacionadas con la labor asignada.

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

El uso de analizadores de red es permitido única y exclusivamente por los encargados del área de tecnología y mantenimiento para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las políticas de seguridad.

No se permitirá el uso de analizadores para monitorear o censar redes ajenas a EDUTEC y no se deberán realizar análisis de la red desde equipos externos a la entidad.

Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

2 Servidores

El Instituto EDUTEC no posee servidor.

El portal web http://www.edutecdelosandes.com/web/ está alojado en un servidor alquilado por un hosting.

Los servicios de internet sólo podrán proveerse a través del servidor de alquiler del hosting que paga las directivas.

Ellingwood,[106] presenta algunas medidas de seguridad que se pueden utilizar para proteger los servidores antes o durante la configuración.

[106] ELLINGWOOD, Justin. - Siete medidas de seguridad para proteger tus servidores. https://www.digitalocean.com/community/tutorials/siete-medidas-de-seguridad-para-proteger-tus-servidores-es.

Llaves SSH: son un par de llaves criptográficas que pueden ser usadas para autenticarse en un servidor SSH, es un método alternativo al uso de contraseñas. La creación del par compuesto por llave pública y privada es llevada a cabo como un paso anterior a la autenticación. La llave privada la conserva el usuario de manera secreta y segura, mientras que la llave pública puede ser compartida con otros usuarios sin restricción. Evitando que usuarios maliciosos puedan realizar intentos repetitivos de acceso al servidor.

Cortafuegos: pieza de software (o hardware) que controla cuáles servicios se encuentra expuestos a la red, bloquean o restringen el acceso a todo puerto exceptuando únicamente aquellos que deben estar habilitados para el público. Un cortafuego bien configurado restringirá el acceso a todo, exceptuando los servicios específicos que se requiere mantener abiertos. Al exponer solo el software necesario, se reducen los puntos en que puede ser atacado el servidor, limitando así los componentes vulnerables a la explotación.

VPN y redes privadas: las redes privadas son las redes que se encuentran habilitadas únicamente para ciertos usuarios o servidores. Usar una VPN es, en efecto, una forma de mapear una red privada que solo los servidores pueden ver. Las comunicaciones serán completamente privadas y seguras.

Infraestructura de llaves públicas y encripción SSL/TLS: sistema diseñado para crear, administrar y validar certificados que identifiquen individuos y encripta la comunicación. Los certificados SSL o TLS pueden ser usados para autenticar diferentes entidades entre sí. Cuando la autentificación se ha llevado a cabo, también pueden ser usados para establecer una comunicación encriptada.

Cada servidor puede configurarse para confiar en una autoridad certificadora central. De ese punto en adelante, se confiará implícitamente en cualesquier certificado firmado por esa autoridad.

Auditoría de servicio: la auditoría de servicio es un proceso para descubrir cuáles servicios están ejecutándose en los servidores de tu infraestructura. Regularmente, los sistemas operativos se encuentran configurados por defecto para ejecutar ciertos servicios al arranque. La instalación de software adicional, a veces puede incluir dependencias que se ejecutan, también, de manera automática.

La auditoría de servicio permite saber cuáles servicios se están ejecutando en el sistema, cuáles puertos usar para su comunicación, y cuáles protocolos se aceptan. Esta información puede ayudar a configurar los parámetros del cortafuego.

Auditoría de archivos y Sistemas de Detección de Intrusos:
La auditoría de archivos es el proceso de comparar el sistema actual contra un registro de los archivos y de las características de los archivos de su sistema, cuando se encuentra en un estado conocido. Esto se usa para detectar cambios que no han sido autorizados en el sistema.

Estas estrategias pertenecen al conjunto de procesos que permiten estar absolutamente seguro que el sistema no ha sido alterado por algún usuario o proceso.

Ambientes aislados de ejecución: Hacen referencia a cualquier método usado para que un componente individual se ejecute dentro de su propio espacio dedicado.

Aislar sus procesos en ambientes individuales de ejecución incrementa la habilidad para aislar cualquier problema de seguridad que se pueda presentar.

Para un servidor hosting, la seguridad debe ser lo más importante, tener vigilancia y prevención constante, contar con un equipo dedicado de expertos en seguridad que realicen seguimiento de las vulnerabilidades diarias del software a nivel servidor y a nivel de sitio web, que escriban activamente parches de seguridad y mejoras para evitar posibles ataques.

3 Correo Electrónico

Las directivas del instituto, se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores.

La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

La longitud mínima de la contraseña será igual o superior a ocho caracteres,

Se deberá utilizar:

Combinaciones de letras con números,

Insertar algún carácter especial como (!»#$%&/),

Utilizar letras mayúsculas y minúsculas,

Evitar palabras predecibles,

Se deberá cambiar la contraseña cada dos semanas.

No deberá aparecer escrita en ningún lugar del sitio de trabajo la contraseña,

Se deberá memorizar la contraseña y evitar que el navegador la recuerde.

4 Base de Datos Moro

Solo el director y el administrador de la base de datos Moro podrán eliminar información del sistema, cuando la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

El director o el administrador de la base de datos Moro serán los encargados de asignar las cuentas a los usuarios para el uso.

Las contraseñas serán asignadas por el administrador de la base de datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

En caso de olvido de contraseña de un usuario, será necesario ponerse en contacto con el administrador de la base de datos para reasignarle su contraseña.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

5 Recursos de Cómputo

Seguridad de cómputo: el área de tecnología y mantenimiento son los encargados de:

Suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad del computador. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

Debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

Son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

Deben aplicar medidas de seguridad al momento en que el usuario se levante de su sitio de trabajo o al estar inactivo el computador, que el teclado y la

pantalla se bloquee y solo se restablecerá al momento de ingresar el usuario con la contraseña asignada.

Para vigilar los documentos e información física, el usuario deberá guárdalos en un sitio confiable y de acceso único, esto debido a que las oficinas son lugares concurridos y la documentación impresa presenta un riesgo significativo, tanto en términos de robo como de negligencia.

6 **Escritorios limpios:**

Siempre que el personal se ausente de su estación de trabajo, deberá guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información pública de uso interno, pública clasificada o pública reservada.

Para el personal que esté ubicado en zonas de atención al público, al ausentarse de su estación de trabajo deberá guardar también los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

Al finalizar la jornada de trabajo, los colaboradores deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada, además bloquear los equipos de cómputo (por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L y no solo apagar el monitor).

7 **Pantallas limpias:** La Alcaldía Mayor de Bogotá[107], crea política de seguridad de escritorio limpio y bloqueo de pantallas. Como ejemplo es bueno tomar esta serie de medidas como que la pantalla del computador (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.

---

[107] ALCALDÍA MAYOR DE BOGOTÁ - Política de escritorio y pantalla limpia. https://www.google.com/search?q=escritorio+y+la+pantalla+limpia&oq=escritorio+y+la+pantalla+limpia&aqs=chrome...69i57.5610602j1j7&sourceid=chrome&ie=UTF-8.

Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo.

Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, definido por el área de tecnología y mantenimiento, encargados de la seguridad de la información.

Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y utiliza.

Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo, este deberá activarse después de 5 minutos de inactividad de cualquiera de estos equipos.

La información pública reservada y pública clasificada, cuando se imprima se deberá retirar inmediatamente de las impresoras.

8 **Ingenieros de Soporte:** los ingenieros de soporte tendrán las siguientes atribuciones y responsabilidades:

Podrán ingresar de forma remota a los computadores exclusivamente para la solución de problemas y bajo solicitud explícita de las directivas de la institución.

Deberán utilizar los analizadores previa autorización del director, informando de los propósitos y los resultados obtenidos.

Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

Deben actualizar la información de los recursos de cómputo del instituto, cada vez que adquiera e instale equipos o software.

Deben registrar cada máquina en el inventario de control de equipos de cómputo y red.

Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música,

configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

Reportar a dirección los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

9 **Renovación de equipos:** Jiménez[108], da su concepto acerca de ¿Es hora de cambiar su computador? a lo que responde que en Colombia habitualmente son reemplazados aproximadamente cada seis años, tanto para uso personal como corporativo. De los casi dos millones de unidades vendidas en el país en 2017, 65% de ellas fueron adquiridas por los hogares y 35% por las empresas, una cifra que abre un interrogante sobre la renovación de equipos a nivel empresarial.

Entre los beneficios de adquirir nuevos equipos con última tecnología están:

Mejorar la conectividad. Los computadores ahora vienen con teclas funcionales que agilizan el encendido, la conexión a las redes y a otros dispositivos inteligentes de la oficina.

Actualizar en la nube plataformas, paquetes de oficina, licencias y aplicativos para trabajar sobre las últimas versiones.

Mejorar la seguridad, al considerar las nuevas características de autenticación, ingeniería de los discos de almacenamiento y procesadores cada vez menos vulnerables a la acción delictiva.

Aumentar su portabilidad a partir de estructuras más livianas y delgadas, lo que beneficia la asistencia a reuniones y la salud de quien lo lleva.

---

[108] JIMÉNEZ, Carolina. La República. ¿Es hora de cambiar su computador? https://www.larepublica.co/internet-economy/es-hora-de-cambiar-su-computador-2765719.

Incrementar la disposición para el uso de los últimos accesorios (audio, video, impresión, almacenamiento y juegos, entre otros), al contar con mayor cantidad de puertos y funciones.

La vida útil de los equipos de cómputo y telecomunicaciones será de tres años, según concepto emitido por el personal encargado del área de tecnología y mantenimiento, para programar con anticipación su renovación.

Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar la petición al área de tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno del área de tecnología y mantenimiento no podrá liberarse una orden de compra.

Por tal razón, el personal encargado del área de tecnología y mantenimiento, tienen a cargo esta importante responsabilidad.

10 Uso de servicios de red

Dirección:

La dirección definirá los servicios de internet a ofrecer a los usuarios y se coordinará con el área de tecnología y mantenimiento para su otorgamiento y configuración.

La dirección puede utilizar la infraestructura de la red para proveer servicios a los usuarios externos y visitas previa autorización del área de tecnología y mantenimiento.

Dirección y el área de tecnología y mantenimiento son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas académicas en la institución, excepto por orden expresa del director.

Usuarios: entre los usuarios de Edutec contamos con personal administrativo, docentes y estudiantes.

11 Identificación de usuarios y contraseñas

Todos los usuarios con acceso a un sistema de información o a la red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Ningún usuario recibirá un identificador de acceso a la red, recursos informáticos o aplicaciones hasta que no acepte formalmente la política de seguridad vigente.

El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por la dirección.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de dirección y los encargados del área de tecnología y mantenimiento, con el fin de contribuir a la seguridad en los siguientes casos:

- Cuando ésta sea una contraseña débil o de fácil acceso.
- Cuando crea que ha sido violada la contraseña de alguna manera.
- El usuario deberá notificar a los encargados del área de tecnología y mantenimiento en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual).

  Si tiene problemas en el acceso a los servicios proporcionados.

  Si un usuario viola las políticas de uso, los encargados del área de tecnología y mantenimiento podrán cancelar totalmente su cuenta de acceso, notificando rápidamente a dirección.

12 Responsabilidades Personales

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Los usuarios no deben revelar bajo ningún concepto su identificador o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar al director y éste reportar al responsable de la administración de la red.

El usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.

En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

13 Uso apropiado de los recursos

Los recursos informáticos, datos, software, red y sistemas de comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operatividad para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

14 Queda Prohibido

El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del software o de los estándares de los recursos informáticos propios de la Institución.

Introducir en los Sistemas de Información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

Introducir voluntariamente programas, virus, macros, *applets*, *controles ActiveX* o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.

Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Cualquier fichero introducido en la red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas políticas y, en especial, las referidas a propiedad intelectual y control de virus.

15 Antivirus: Se hace necesario adquirir y disponer de un antivirus con licencia en EDUTEC, debido a que tiene un amplio uso de internet, correo electrónico, servicios web y de mensajería, por tal razón es importante considerar en una solución que incluya tecnologías y software de seguridad de internet que protejan las actividades, datos, ordenadores, etc., que a diario se realizan y utilizan.

Un antivirus protege los equipos de cómputo contra virus o programas maliciosos (malwares). Estos virus se pueden contagiar fácilmente a través de las aplicaciones que se usan a diario, poniendo en riesgo los ordenadores cuando se descargan programas de sitios de confianza. También se encuentra el adware, un software que despliega publicidad de distintos productos o servicios, que incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario, que generalmente agregan ícono gráficos en las barras de herramientas de los navegadores de internet o en los clientes de correo, la cuales tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que esté buscando. Dentro de los programas conocidos que incluyen *Adwares* están: Alexa, *MyWebSearch*, *Ask*, *Yac, Gator*, *GoHit*, *Qone8*, *Lop*, *Hotbar*, *SearchProtect*, *C2Media*, *CID*, *InstallCore, Softonic, OpenCandy*, etc…

Como bien es sabido, dentro de las principales vías de infección se encuentran las redes sociales, sitios webs fraudulentos, redes P2P (descargas con regalo), dispositivos USB/CDs/DVDs infectados, sitios webs legítimos pero infectados, adjuntos en correos no solicitados (spam), entre otros.

La función del antivirus es escanear archivos y programas que se utilizan y compararlos con los virus y malware conocidos, también revisa los programas para detectar cualquier rastro de un virus nuevo o desconocido, y así alerta al usuario de cualquier actividad sospechosa.

Se debe pensar en comprar un antivirus de calidad, que garantice que los equipos de cómputo estarán a salvo de amenazas, que proporcione una buena defensa frente a nuevas amenazas en tiempo real, además de soporte técnico

con funciones como: controles parentales, protección de Firewall, cifrado de archivos y filtrado de spam.

Existe una amplia gama de antivirus para prevenir y acabar con los malware molestos, que generan tanto daño en las empresas. Topratedantivirus[109], elaboro una lista donde muestra los mejores antivirus para MAC del 2019. A continuación se presenta la lista de opciones que poseen soluciones de seguridad de alta calidad, de acuerdo a las necesidades.

- ✓ Airo (Solo para MAC): Detección y prevención en tiempo real, análisis de sistema 24 horas al día, 7 días a la semana, protección de datos y privacidad, potente tecnología de IA, protección de navegación privacidad y protección de datos.
- ✓ Alwil Avast Internet Security: Posee muy buenas funciones para la seguridad en internet. Su capacidad disminuye al momento de detectar nuevas amenazas. No contiene algunas funciones vitales.
- ✓ AVG Internet Security: Es muy confiable en términos de detección de virus y desinfección. No es muy costoso pero su punto débil es su complicada interfase que complica su uso.
- ✓ Avira Antivirus: Todo en la Internet Security Suite, + VPN prémium y System Speedup Pro, Aplicaciones prémium para dispositivos Android e iOS, Servicio al cliente VIP.
- ✓ BitDefender Internet Security: Provee de una fuerte protección a sus usuarios. A pesar de su alta capacidad para identificar y eliminar amenazas, aún sigue dejando rastros en su trabajo, lo cual le resta efectividad.
- ✓ BullGuard: Protección con múltiples capas de protección para mantener su seguridad y asegurar que sus dispositivos funcionen correctamente, zona para niños, facilidad y privacidad, zona para niños protección en internet, de fácil

[109] TOPRATEDANTIVIRUS - EL MEJOR ANTIVIRUS PARA MAC DEL 2019. https://www.top10antivirussoft.com/es/bestmacav/.

instalación, soporte técnico gratuito, privacidad de datos y documentos importantes.

- ✓ Eset Nod 32: Líder en la industria de la seguridad informática, de modo que siempre se encuentran actualizados y un paso delante de posibles ataques, posee un método antirrobo, el cual es avanzado. Su diseño es agradable, se adapta a tablet y Smartphone; igualmente, tiene una eficaz manera de detectar amenazas.
- ✓ Heimdal Security: inspección de sandbox y backdoor, protección contra malware basado en el tráfico, detección de malware de segunda generación, con soporte 24/7.
- ✓ Kaspersky Internet Security: provee de una adecuada seguridad a los usuarios mientras se encuentran conectados y desconectados de internet. Tiene un gran desempeño en la detección de 'malware'.
- ✓ McAfee: protección antivirus galardonada, navegación web segura, expertos en seguridad y soporte online, administrador de contraseñas, optimización del rendimiento, almacenamiento cifrado, protección de la red doméstica, protección en distintas plataformas y en varios dispositivos.
- ✓ Norton Internet Security by Symantec: es el mejor para la seguridad al navegar por internet. Una de sus principales características es la detección de 'malware', la cual se basa en el análisis de su comportamiento como una amenaza.
- ✓ Panda: provee de todas las funciones básicas de seguridad. Es muy seguro con los dispositivos USB conectados a la PC y nos da la posibilidad de tener 2Gb de backup en línea.
- ✓ PC Tool Internet Security: a pesar de que se han hecho muchas mejoras a través de los años, aún tiene deficiencias. Carece de términos de control para padres y de una opción de ayuda en línea.
- ✓ Total AV: interfaz sencilla y precisa cubre todos los aspectos de protección, rendimiento y limpieza constante para pc. El programa System Boost, retardar programas de inicio, la aplicación *disk cleaner* localiza archivos ocultos, que

ocupan espacio en el disco duro, el programa antivirus dispone de videos tutoriales, para guiar a un buen uso del antivirus, gracias a la aplicación *Ad Block*, puedes eliminar los constantes anuncios de la web que dificultan tu navegación.

Algo fundamental que se debe tener en cuenta es que el antivirus debe permanecer activado y actualizado para proteger los equipos de cómputo de EDUTEC, de todas las amenazas que se encuentran en internet. El personal de tecnología y mantenimiento será quienes establecen los tiempos de configuración y actualización del antivirus o cada que sea necesario.

16 Antivirus de la Red

Todos los equipos de cómputo del instituto deberán tener instalada una solución antivirus.

Periódicamente se debe hacer el rastreo en los equipos de cómputo del instituto, y realizar la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la red.

17 Responsabilidad del área de tecnología y mantenimiento

Deberá implementar una solución antivirus en las computadoras del instituto.

Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.

Configurar el analizador de red para la detección de virus.

El área de tecnología y mantenimiento aislará el equipo o red, notificando a las directivas correspondientes, en las condiciones siguientes:

- ✓ Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.
- ✓ Si el usuario viola las políticas antivirus.

- ✓ Cada vez que los usuarios requieran hacer uso de discos, USB', éstos serán examinados por una solución antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo.

B. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El área de tecnología y mantenimiento implementará soluciones lógicas y físicas que garanticen la protección de la información de Edutec de posibles ataques internos o externos.
Rechazar conexiones a servicios comprometidos,
Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https),
Proporcionar un único punto de interconexión con el exterior,
Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (red interna),
Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
Auditar el tráfico entre el exterior y el interior.
Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

1 *Firewall* (Cortafuegos)

La solución de seguridad perimetral debe ser controlada con un *Firewall* por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir,

de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.

El área de tecnología y mantenimiento establecerá las reglas en el *Firewall* necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la red.

El f*irewall* debe bloquear las conexiones extrañas y no dejarlas pasar para que no causen problemas.

El *firewall* debe controlar los ataques de denegación de servicio y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

Controlar las aplicaciones que acceden a internet para impedir que programas a los que no se le ha permitido explícitamente acceso a internet, puedan enviar información interna al exterior (tipo troyanos).

2 Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es una aplicación usada para detectar accesos no autorizados a un computador, servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

El área de tecnología y mantenimiento implementará soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos de la Institución como:

- Detección de ataques en el momento que están ocurriendo o poco después.
- Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.

- Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
- Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.
- Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los *logs*.
- Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los *logs* puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
- Automatizar tareas como la actualización de reglas, la obtención y análisis de *logs*, la configuración de cortafuegos.
- La red del Instituto sólo podrá acceder a los parámetros que el *Firewall* tenga permitido o posibilite mediante su configuración.

3 Redes Privadas Virtuales (VPN)

Los usuarios móviles y remotos del Instituto no podrán tener acceso a la red interna privada, salvo las autorizadas y habilitadas por el director a los encargados del área de tecnología.

Los encargados de tecnología y mantenimiento serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

4 Conectividad a Internet

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de EDUTEC tienen las mismas responsabilidades en cuanto al uso de Internet.

El acceso a Internet se restringe exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con *Firewall* incorporado en la misma.

No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

5 Red inalámbrica (WIFI)

Acceso a funcionarios de las empresas:

La red inalámbrica es un servicio que permite conectarse a la red de internet sin la necesidad de algún tipo de cableado. La red inalámbrica le permitirá utilizar los servicios de red.

Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de internet de manera controlada.

Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, *IPod*, celulares, etc.) con capacidad de conexión *Wireless*.

El director y el área de tecnología y mantenimiento, son los encargados de la administración, habilitación y bajas de usuarios en la red inalámbrica del instituto.

6 Identificación y activación

Para hacer uso de la red inalámbrica, el solicitante necesariamente deberá ser usuario identificado como administrativo, docente o alumno del instituto EDUTEC.

Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante el llenado de un formulario y presentando el dispositivo que se conectará a la red inalámbrica. Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.

La activación de la cuenta se realizará por un periodo semestral como máximo; salvo casos de fuerza mayor o anormalidades en el registro (usuarios inexistentes, apagones, fallas, etc.).

Para conectarse a la red inalámbrica se deberá emplear autenticación, para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

7 Seguridad

El área de tecnología y mantenimiento determinarán las medidas pertinentes de seguridad para usar las redes inalámbricas.

Tecnología y mantenimiento se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.

No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal.

No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.

Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a los encargados de tecnología y mantenimiento para su respectiva baja del equipo de la red inalámbrica.

8 Tecnología

La red inalámbrica del instituto usa el estándar 802.11b/g/n con cifrado WPA2. Por lo tanto las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar y soportar los requerimientos descritos. Caso contrario se debe realizar algunas actualizaciones previas de tratarse de un computador portátil.

A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura de la institución.

El área de Tecnología se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios.

No se permiten la operación ni instalación de puntos de acceso (*access points*) conectados a la red cableada del Instituto sin la debida autorización por parte del director y de los encargados de tecnología y mantenimiento.

No se permite configurar las tarjetas inalámbricas como puntos de acceso o la configuración de equipos como servidores adicionales.

9 Restricciones/prohibiciones de acceso a Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (*Peer to Peer*).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "*On line*" en la red.
- El acceso a páginas interactivas, estará bajo el criterio del área de tecnología y mantenimiento dependiendo de la capacidad de la red y la demanda del servicio.
- El uso de páginas relacionadas con música, descarga de archivos, películas, video juegos, archivos ejecutables u otros similares, que atenten con la confidencialidad, integridad y disponibilidad de la información que posee la Institución.

10 Excepciones

Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.

En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.

En el caso de estos eventos las restricciones para acceder podrán ser anuladas temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

11 Plan de contingencias informáticas

El área de tecnología y mantenimiento creará un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo para soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

12 Actualizaciones de la política de seguridad

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el Instituto se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios de la Empresa.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la política de seguridad más reciente.

13 Disposiciones

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo de las directivas; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones o penalidades por el incumplimiento de las mismas.

El Área de Tecnología y mantenimiento de EDUTEC. Bajo la orientación de las directivas son los responsables de la administración de los equipos de cómputo, sistemas de información y redes. Vela por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

4.4.2 CONTROLES DE SEGURIDAD

Corletti[110], define un control como lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

[110] CORLETTI ESTRADA, Alejandro. ISO-27001 LOS CONTROLES (Parte I). Disponible en: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf.

KOSUTIC[111] El anexo A de la norma ISO 27001 es probablemente el anexo más famoso de todas las normas ISO – ello porque provee una herramienta esencial para la gestión de la seguridad: una lista de los controles (o medidas) de seguridad que pueden ser usados para mejorar la seguridad de la información.

Hay 114 controles listados en ISO 27001, distribuidos en 14 secciones, así:

1. Políticas de seguridad de la información: controles acerca de cómo deben ser escritas y revisadas las políticas.
2. Organización de la seguridad de la información: controles acerca de cómo se asignan las responsabilidades; también incluye los controles para los dispositivos móviles y el teletrabajo.
3. Seguridad de los recursos humanos: controles antes, durante y después de emplear.
4. Gestión de recursos: controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento.
5. Control de acceso: controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.
6. Criptografía: controles relacionados con la gestión de encriptación y claves.
7. Seguridad física y ambiental: controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.
8. Seguridad operacional: muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.

[111] KOSUTIC, Dejan. ADVISERA - Resumen del Anexo A de la Norma ISO 27001:2013. Disponible en: https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/

9. Seguridad de las comunicaciones: controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.
10. Adquisición, desarrollo y mantenimiento de sistemas: controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.
11. Relaciones con los proveedores: controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores.
12. Gestión de incidentes en seguridad de la información: controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.
13. Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio: controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI.
14. Cumplimiento: controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información

La norma ISO 27001 está enfocada en la TI (Tecnología de la información), pero por sí sola no puede proteger la información. La seguridad física, la protección legal, la gestión de recursos humanos, los aspectos organizacionales – todos ellos juntos son requeridos para asegurar la información.

El Anexo A es un catálogo de 114 controles de seguridad del que se pueden seleccionar solo los que apliquen, para EDUTEC, se proponen los siguientes controles de acuerdo a la norma ISO/IEC 27001.

Cuadro 14 Anexo A controles de seguridad EDUTEC

CONTROL ISO	CONTROLES	CUMPLE SI	CUMPLE NO	CONTROL / DESCRIPCIÓN
				A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
A5.1	**A5.1.1** Documento de la política de seguridad de la información.		**x**	Se identifican los riesgos a los que se enfrenta los sistemas de información del Instituto y se define un conjunto de políticas para la seguridad de la información, que sea aprobada por sus directivas, publicada y comunicada a los empleados y partes externas pertinentes.
	A5.1.2 Revisión de la políticas de seguridad de la información		**x**	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad a intervalos planificados o si ocurren cambios significativos, para asegurar su convivencia, adecuación y eficacia continúa y poder gestionar el Sistema de Gestión de Seguridad Informática.
A6.1	**A6.1.1** Compromiso de la dirección con la seguridad de la información.		**x**	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.
	A6.2.1 Política para dispositivos móviles	**x**		Se deberían adoptar políticas y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A7.1	**A7.1.1** Investigación de antecedentes	**x**		Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinente, y deberían ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	A7.1.2 Responsabilidades de la Dirección		**x**	La Dirección debería exigir a todos los empleados administrativos y contratistas la aplicación de seguridad de la información de acuerdo con las políticas y procedimientos establecidos por el Instituto.
A8.2	**A8.1.1** Inventario de Activos	**x**		Convendría identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos actualizado.
	A8.2.1 Clasificación de la información	**x**		La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

	A8.2.3 Manejo de activos		**x**	Convendría desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información que adapte la Institución.
A9.1	**A9.1.1** Política control de acceso		**x**	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	A9.1.2 Política sobre el uso de los servicios de Red		**x**	Se debería solo permitir acceder a la Red y sus servicios, a los usuarios que hayan sido autorizados específicamente.
	A9.2.3 Gestión de derechos de acceso privilegiado		**x**	Se debería especificar, restringir y controlar la asignación y uso de derechos de acceso privilegiado
A9.4	**A9.4.1** Restricción de acceso a la información	**x**		El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
	A9.4.2 Procedimiento de ingreso seguro		**x**	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
	A9.4.3 Sistema de gestión de contraseñas		**x**	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
	A9.4.4 Uso de programas utilitarios privilegiados		**x**	Se debería limitar y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A11	**A11.1.3** Seguridad de oficinas, recintos e instalaciones	**x**		Se convendría diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	A11.1.4 Protección contra amenazas externas y ambientales	**x**		Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
	A11.2.2 Servicios de suministros	**x**		Los equipos de cómputo se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
	A11.2.4 Mantenimiento de equipos	**x**		Es indispensable proteger y mantener correctamente los equipos de cómputo, para así asegurar su disponibilidad e integridad.
A12	**A12.2.1** Controles contra códigos maliciosos		**x**	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios, para proteger contra códigos maliciosos.
	A12.3.1 Respaldo de información	**x**		Se deberían hacer copias de respaldo de la información, del software e

				imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
	A12.4.1 Registro de eventos	**x**		Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	A12.4.2 Protección de la información de registro		**x**	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
	A12.5.1 Instalación de software en sistemas operativos		**x**	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos
	A12.6.2 Restricciones sobre la instalación de Software			Se debería establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A13	**A13.1.1** Control de Red	**x**		La Red se debería gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A13.2.3 Mensajería electrónica	**x**		Convendría proteger adecuadamente la información incluida en la mensajería electrónica.
A15	**A15.1.2** Tratamiento de la seguridad dentro de los acuerdos con proveedores	**x**		Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinente con cada proveedor que tenga acceso, procese, almacene, comunique o suministre componentes de infraestructur15.2.1a de TI para la información de la Institución.
	A15.2.1 Seguimiento y revisión de los servicios de los proveedores	**x**		La Institución debería hacer seguimiento, revisión y auditoría con regularidad en la presentación de servicios de los proveedores.
A16	**A16.1.3** Reporte de debilidades de seguridad de la información	**x**		Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
	A16.1.7 Recolección de evidencia		**x**	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A17	**A17.1.2** Implementación de la continuidad de la seguridad de la información	**x**		El instituto debería 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.
	A18.1.3 Protección de registros		**x**	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación contractual y de negocio.
	A18.1.4 Privacidad y protección de datos personales	**x**		Cuando sea aplicable, se debería asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinente.
A18	**A18.2.2** Cumplimiento con las políticas y normas de seguridad		**x**	Las directivas de la Institución deberían 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.
	A18.2.3 Revisión del cumplimiento técnico		**x**	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: La Autora.

4.5. PLAN DE COMUNICACIÓN Y CUALIFICACIÓN DE LOS USUARIOS

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
0.1	Agosto 2019	Versión inicial del documento

Contenido

4.5.1 INTRODUCCIÓN

El presente documento describe de forma detallada el Plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad informáticas contempladas en el diseño de un sistema de gestión de seguridad de la información (SGSI) para la institución Edutec de los Andes Pitalito, argumentada en la Norma ISO/IEC 27001; que surge de la necesidad de conocer, actualizar, proteger y salvaguardar la información, contribuyendo a mejorar su seguridad y a la continuidad del negocio.

Este manual pretende servir de guía a través de las políticas de seguridad informática, a todos los usuarios que gestionan y manipulan información relevante de la Institución, con el apoyo de sus directivas; quienes son los encargados de ayudar e incentivar a los involucrados a tener un correcto manejo y aplicación de medidas y técnicas

4.5.2 PRESENTACIÓN

El presente Plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad contempladas en el SGSI, incluye la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en las dependencias y aulas de Edutec de los Andes Pitalito.

Para realizar esta actividad se tomó como referencia, de la página MINTIC, el Modelo de seguridad, Guía No. 14 - Plan de capacitación, sensibilización de seguridad y privacidad de la información[112].

Donde establece que un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la institución requiere que sean cumplidos por parte de todos los usuarios del sistema. Este punto es fundamental porque de esta manera todos los usuarios (administrativos, docentes y estudiantes) conocen y se documentan de las políticas de seguridad que tiene la institución como conducto regular en cuanto a seguridad de la información se refiere.

Que ante cualquier incumplimiento a las políticas, puede llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

[112] MINTIC. Modelo de Seguridad. Guía 14 - Plan de comunicación, sensibilización, capacitación. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

4.5.3 JUSTIFICACIÓN

El modelo de seguridad y privacidad de la información MSPI del Estado Colombiano[113], establece que un punto importante dentro de la fase de planificación, es la realización del plan de comunicación, el cual debe incluir la estrategia para que la seguridad de la información se convierta en cultura organizacional, que permita generar competencias y hábitos en todos los niveles (directivos, administrativos, estudiantes) de Edutec de los Andes Pitalito.

El Plan de comunicación, sensibilización y capacitación, es un programa efectivo que busca que todos los funcionarios de Edutec de los Andes Pitalito cumplan las políticas de seguridad de la información mediante capacitaciones y socializaciones.

El Plan de comunicación, sensibilización y capacitación sobre las políticas de seguridad se deben realizar teniendo en cuenta lo siguiente:

- Existe la mentalidad que no hay nada importante por proteger en su computador.
- Se tiene el concepto errado que la tecnología por si misma puede resolver los problemas de seguridad.
- Continuamente se generan nuevos métodos mediante engaños que buscan obtener información confidencial.
- Se deben conocer tanto las amenazas externas como las internas.

Debido a las anteriores razones, el plan de comunicación, sensibilización y capacitación se diseñó tomando como referencia los requerimientos exigidos por Gobierno en Línea, logrando que los funcionarios conozcan los motivos y razones que generan los diferentes tipos de incidentes en seguridad de la información que existe alrededor de cada uno y acojan las debidas precauciones recomendadas a través de las diferentes actividades de sensibilización.

[113] MINTIC. Modelo de Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

4.5.4 OBJETIVOS

4.5.4.1 Objetivo General

Dar a conocer a todos los usuarios (administrativos, docentes y estudiantes) del instituto EDUTEC, las políticas de seguridad que deben seguir, para así asegurar que todos los funcionarios del Instituto Edutec de los Andes Pitalito, cumpla con sus roles y responsabilidades de seguridad y privacidad de la información, buscando:

- Definir las necesidades de capacitación.
- Definir los temas para la capacitación en seguridad de la información, de acuerdo a las partes interesadas.
- Proponer estrategias para sensibilización y entrenamiento.

4.5.4.2 Objetivos Específicos

- Diseñar un plan de capacitaciones.
- Dar a conocer los objetivos de la campaña.
- Captar la atención de los funcionarios para que interactúen con las actividades de seguridad de la información.
- Relacionar e interactuar la campaña con todos los requerimientos de la estrategia de seguridad mediante afiches con información relacionada.
- Concientizar a todo el personal de EDUTEC, mediante talleres y capacitaciones relacionadas con la seguridad de la información.

4.5.5 ACTIVIDADES

A continuación, se describen las actividades incluidas en el plan de comunicaciones:

4.5.5.1 Diseño del programa de comunicación, sensibilización y capacitación.

En esta fase se identifican las actividades necesarias para cumplir con las metas de socialización en la Institución Edutec de los andes Pitalito.

Lo primero que se realizó fue definir el modelo de administración del programa de entrenamiento, y sensibilización, el cual es centralizado, lo anterior teniendo en cuenta que las políticas, la estrategia y la implementación son fijadas por EDUTEC, a través de su director general y el área de tecnología y mantenimiento, para luego ser distribuidos de igual manera a todas las dependencias de la institución mediante afiches con información relacionada y que sean aplicadas de manera homogénea en cada una.

4.5.5.2 Identificación de necesidades

Para identificar las necesidades se utilizó como método la entrevista a un pequeño grupo de personas, donde se encuentran directivos, administrativos, docentes y estudiantes seleccionados, encontrando que:

- Los directivos manifiestan que reconocen la importancia que tienen el tema de seguridad y apoyan 100% esta temática.
- Hay usuarios que comparten la clave de usuario.
- Los usuarios desconocen sobre temas de seguridad de la información y en especial, el alcance del tema.
- Se desconocen las políticas de seguridad y privacidad de la información.
- No existe un procedimiento de copias de seguridad de la información por parte de los usuarios finales.

- Existe desconocimiento de las normas de seguridad informática.
- Hay disentimiento de las políticas de seguridad y protección de datos personales, además, en la inspección se pudo establecer que no hay hábitos adecuados en los sitios de trabajo como:

✓ Consumo de líquidos y alimentos junto a los equipos de cómputo.
✓ Más de una persona comparte y conoce la clave de los correos electrónicos y de la base de datos de la Institución.
✓ En el momento de abandonar el sitio de trabajo temporalmente no cierran sesión en sus equipos de cómputo.

4.5.5.3 Diseño del plan de capacitación y sensibilización

Una vez identificadas las necesidades de capacitación, se procede con la elaboración de la propuesta de capacitación, el cual consta de los siguientes elementos:

4.5.5.3.1 Políticas del plan de comunicación, sensibilización y capacitación.

Este plan de comunicación, sensibilización y capacitación está diseñado con base en las políticas de seguridad y privacidad de la información, registrados en el punto 4.4. Políticas y control de seguridad.

4.5.5.3.2 Roles y responsabilidades

El Director general y el personal del área de tecnología y mantenimiento, liderarán las actividades del plan de sensibilización, comunicación y capacitación, quienes gestionarán la logística y presupuesto necesarios para el desarrollo de las actividades.

Temas y acciones de información y sensibilización. Algunos de los aspectos que se deben tratar en este plan de comunicación, sensibilización y capacitación son:

- ✓ Política de seguridad física, lógica, perimetral.
- ✓ Plan de contingencia informática,
- ✓ Actualización de la política de seguridad.
- ✓ Controles de seguridad de la información.

Se recomienda que los ponentes sean funcionarios del área de tecnología y mantenimiento, que realicen dichas capacitaciones a través de exposiciones magistrales y prácticas, utilizando para ello equipos de cómputo y recursos visuales.

- ➢ **Talleres de capacitación para todo el personal**
- ➢ **Capacitación inductiva:** Orientada a facilitar la integración de nuevos usuarios (administrativos, docentes o estudiantes).

  Organizar programas de capacitación para el conocimiento de políticas, buen uso y aprovechamiento de recursos tecnológicos.
- ➢ **Capacitación preventiva:** Orientada a prever los cambios que se producen en el personal, preparar al personal para enfrentar con éxito nuevas formas de ataque cibernético, nuevos virus, cambios en la metodología de trabajo informático, actualizaciones e implementación de nuevos procesos en las asistencias tecnológicas.
- ➢ **Capacitación correctiva:** Orientada a solucionar problemas identificados mediante los estudios de diagnóstico del sistema de seguridad de la información del instituto.

a. Tema

   Acciones seguras para proteger la información.

b. Ponentes

   Área de tecnología y mantenimiento EDUTEC.

c. Metodología a utilizar.

   Exposición teórico y práctico utilizando recursos visuales.

- **Desarrollo de material visual**

- Letrero alusivo a la campaña expectativa
- Imagen y nombre de la campaña
- Folletos y volantes: Se elaborarán folletos y volantes con información relativa a los temas de seguridad y privacidad de la información y gestión de riesgos.
- Afiches: Se elaboraran afiches en papel con la finalidad de generar expectativa e interés en las acciones emprendidas por los encargados del área de tecnología y mantenimiento.
- **Financiamiento del plan de comunicación, sensibilización y capacitación.** El financiamiento del plan de comunicación, sensibilización y capacitación, estará a cargo de la Dirección general de Edutec.
- **Resultados y logros esperados.** Se tiene como resultados y logros esperados, informar, sensibilizar y comprometer al 100% de los usuarios de Edutec, sobre la implementación y fortalecimiento del sistema de gestión de seguridad y privacidad de la información.
- **Evaluación.** Dirección general, junto con el área de tecnología y mantenimiento, se encargarán de evaluar el desarrollo de las acciones de capacitación y socialización, en función a los informes de evaluación y desarrollo.

  La campaña de sensibilización se realizará según cronograma de actividades organizado por la Institución durante el semestre, que iniciarán con el plan de comunicación, sensibilización y capacitación, apoyado por medio de los afiches y folletos para dar a conocer masivamente la campaña para todo el personal de la entidad.

5. CONCLUSIONES

Gracias al desarrollo de este trabajo y mediante la técnica de investigación cualitativa y cuantitativa, se elaboró el inventario de activos informáticos y de información que posee EDUTEC, dónde al indagar sobre las medidas de seguridad implementadas se evidenció que en ninguna área se utiliza un sistema de antivirus con licencia, que cubra las necesidades de seguridad, debido a la alta exposición de virus informático que afecta los equipos de cómputo y pone en peligro la existencia de información sensible del instituto, además los ordenadores no poseen UPS y en caso de un bajón o perdida de energía los puede afectar o quemar, dejando perdías económicas altísimas, en caso de un siniestro. A pesar de que ningún sistema puede garantizar una completa seguridad de la información, es una manera de controlar y prevenir futuros daños a los equipos, al sistema, a la reputación y a la continuidad del negocio; demostrando que es necesario e indispensable diseñar un Sistema de Gestión de Seguridad de la Información (SGSI), bajo la norma ISO/IEC 27001.

Con el fin de valorar el grado de riesgo de la información, como el activo más valioso del Instituto, se realizó a través de la metodología Magerit el análisis de Riesgo informático para conocer las vulnerabilidades y amenazas que generan peligro, dónde se identificaron 38 vulnerabilidades; las cuales deben ser asumidas, tratadas, reducidas o eliminadas.

Por tal razón se proponen políticas y controles de seguridad del Anexo A de la Norma ISO 27001, que protegen y salvaguardan los sistemas de información de la Empresa, en dónde la dirección y todas sus directivas deben autorizar y difundir a los funcionarios la hoja de ruta que deben seguir para evitar daños, perjuicio y problemas en sus actividades diarias, a través del plan de comunicación y

cualificación de los usuarios, sobre las políticas de seguridad contempladas en el SGSI.

La mejor manera de contribuir a mejorar la seguridad de la información en el Instituto Edutec de los Andes Pitalito, es que tanto directivos como los usuarios que intervienen en cada una de sus actividades, conozcan el plan de comunicaciones y cumplan las políticas y controles de seguridad, a través de un sistema de gestión de seguridad SGSI.

6. RECOMENDACIONES

Se invita al director de Edutec de los Andes Pitalito, a revisar, analizar y aprobar las siguientes políticas y controles de seguridad propuestas en este trabajo, para luego de ser aprobadas difundirlas, promoverlas e implementarlas con todos los usuarios (administrativos, docentes y estudiantes) de la Institución.

Se sugiere realizar semestralmente capacitaciones a todo el personal administrativo y docente, como a los estudiantes de las diferentes jornadas, para el buen uso, manejo y aplicación de los recursos y equipos de cómputo de las aulas como el de impresión, esto con el fin de salvaguardar y garantizar la seguridad de las tecnologías de información, como proceso que contribuye a la mejora continua por medio de la implantación de sistemas y capacitación a los usuarios.

En la matriz de riesgo se estableció que 16 amenazas quedaron en riesgo muy alto, con una valoración de 9, por tal razón se recomienda que éstas sean las primeras en ser atendidas, como es el caso de adquirir un antivirus con licencia, que proteja contra todo tipo de virus de los que se contagian fácilmente a través de aplicaciones que a diario se usan como el correo electrónico, los navegadores web, las redes sociales y al descargar programas en sitios donde la conexión no es segura, difundiendo software dañino en los equipos de cómputo de la institución, como en los ordenadores personales de docentes y estudiantes. Así mismo a través del uso de memorias USBs y discos duros extraíbles, que transportan todo tipo de virus que crean accesos directos.

Es de suma importancia un antivirus licenciado que sea de calidad, que ofrezca detectar y controlar el mayor número de virus en los equipos de cómputo de las diferentes áreas, libre de amenazas en tiempo real. Para ello existe una amplia gama de antivirus para prevenir y acabar con todo tipo de malware. Dicha decisión

de escoger la mejor solución en cuanto a seguridad de la información se refiere, recae directamente en el director general bajo la asesoría del personal de tecnología y mantenimiento.

Entre los problemas que más se presentan están la suplantación de identidad del usuario, escapes, destrucción y alteración accidental de la información, vulnerabilidades de los programas (Software), errores de mantenimiento y actualización de programas (software - hardware), acceso no autorizado, modificación deliberada, destrucción de la información entre otras amenazas, que se pueden solucionar a través de una aplicación modelo cliente-servidor que es un sistema distribuido entre múltiples procesadores donde hay clientes que solicitan servicios y servidores que los proporcionan. La tecnología cliente/servidor, es un modelo que implica productos y servicios enmarcados en el uso de la tecnología de punta, y que permite la distribución de la información en forma ágil y eficaz a las diversas áreas de una organización (empresa, institución pública o privada), así como también fuera de ella[114].

Es necesario que a través del servidor donde tiene alojado EDUTEC su sitio web y donde paga alquiler del hosting para proveer de este servicio; la empresa garantice el manejo y conservación de una aplicación dónde los docentes, administrativos y directivos puedan registrar las notas de los estudiantes, accediendo a través de una *URL* del sitio en mención, dejando atrás el uso de planillas de notas en hojas de cálculo Excel que son inseguras, poco confiables y fáciles de alterar. Dando así solución a un problema recurrente a través de las Tics.

Por ser la información uno de los activos más valiosos y sensible que tiene EDUTEC, es indispensable pensar en mantener dicha información segura a través

[114] ECURED - Cliente-Servidor. Disponible en: https://www.ecured.cu/Cliente-Servidor.

de técnicas, barreras y procedimientos que resguarde el acceso a todos los datos y aplique restricciones a los usuarios autorizados que forman parte de la Institución y tienen el privilegio de acceder a los archivos importantes.
Se propone política de seguridad donde se establece los derechos de acceso a los datos y los recursos con los que se cuentan, estableciendo herramientas de control y mecanismos de identificación que faciliten el uso de los permisos otorgados a los usuarios.

La norma ISO-27001, deja abierto el camino a la aplicación de cualquier tipo de metodología, siempre y cuando la misma sea metódica y completa, es decir satisfaga todos los aspectos que se mencionan en ella[115].

Se debe actuar rápidamente para proteger los sistemas y la información relevante que maneja EDUTEC, tomando medidas preventivas que permitan llevar a cabo actividades que controle debilidades críticas del hardware, para eso lo mejor será aplicar parches, y actualizaciones de los fabricantes. Se puede pensar también en el uso de software libre. “Muchas empresas desconfían del software libre por ser gratuito, sin analizar el resto de ventajas que puede ofrecer al negocio[116]”. Dentro de las ventajas más significativas que se obtienen son:

- ✓ Valor más económico o gratuito,
- ✓ Compatibilidad con otros programas,
- ✓ Instalación en los dispositivos que requiera,
- ✓ Posibilidad de modificarlo,
- ✓ Seguros y tienen menos fallos,
- ✓ Y Mejora continua.

[115] CORLETTI ESTRADA, Alejandro. ISO-27001 LOS CONTROLES (Parte I). http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf.
[116] EAE BUSINESS SCHOOL - Software libre para empresas. ¿Qué ventajas tiene? https://www.eaeprogramas.es/empresa-familiar/software-libre-para-empresas-que-ventajas-tiene.

BIBLIOGRAFÍA

Abogado [En línea] https://www.abogado.com/recursos/ley-criminal/descripcion-general-del-robo.html..

Actualicese. [En línea] https://actualicese.com/normatividad/2012/10/17/ley-estatutaria-1581-de-17-10-2012..

Alcaldía de Pitalito. [En línea] http://www.alcaldiapitalito.gov.co/web1/index.php/pitalito/informacion-general/item/1303-geografia..

Alcaldía de Pitalito, Huila. [En línea] http://www.alcaldiapitalito.gov.co/web1/index.php/la-alcaldia/oficina-comunicaciones/boletines-de-prensa/item/606-alcalde-de-pitalito-pidio-a-electrificadora-del-huila-dar-solucion-rapida-a-deficiencias-que-generan-fallas-constantes-en-servicio-de-energia.

Alcaldía Mayor de Bogotá . Alcaldía Mayor de Bogotá - Política de escritorio y pantalla limpia. [En línea] https://www.google.com/search?q=escritorio+y+la+pantalla+limpia&oq=escritorio+y+la+pantalla+limpia&aqs=chrome...69i57.5610602j1j7&sourceid=chrome&ie=UTF-8..

ÁLVAREZ MARAÑÓN, Gonzalo, GARCÍA PEDRO, Pablo Pérez. 2004. *Seguridad informática para empresas y particulares.* España : McGraw-Hill, 2004.

ANKAMA SUPPORT. [En línea] https://support.ankama.com/hc/es/articles/203790076--Qu%C3%A9-es-un-log..

ASENCIO, Gonzalo. 2006. *Seguridad en Internet.* Madrid : Ediciones Nowtilus., 2006.

BERRÍO LOPEZ, Juan Pablo. *Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la Norma ISO/IEC 27001. Tesis Magister en Ingeniería, Ingeniería de Sistemas.* Antioquia : s.n.

BOJACA, Edgar Alonso. *Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco De Gacheta. Tesis, Especialización en seguridad informát.* Universidad nacional abierta y a distancia. .

BORTNIK, Sebastián. WELIVESECURITY. [En línea] https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion..

BORTNIK, Sebastián*. 13 Apr 2010 - 12:17PM. https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion.*

CAMBRONERO IBAÑEZ, Antonio. 2018. Redacción cuadernos de seguridad . [En línea] 2018. https://cuadernosdeseguridad.com/2018/03/pautas-para-prevenir-incendios-en-la-industria/.

CCM . CCM - Introducción a WIFI (802.11 o WiFi). [En línea] https://es.ccm.net/contents/789-introduccion-a-wifi-802-11-o-wifi.

CEPAL Biblioguías . CEPAL Biblioguías – Biblioteca de la CEPAL. Métodos de almacenamiento y respaldo de datos. . [En línea] https://biblioguias.cepal.org/c.php?g=495473&p=4398069.

CEUPE. CEUPE – CENTRO EUROPEO DE POSTGRADO. La infraestructura tecnológica. . [En línea] https://www.ceupe.com/blog/infraestructura-tecnologica.html..

CIDECAME.UAEH.EDU.MX. [En línea] http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/135_definicin_de_red_de_comunicaciones_y_su_importancia.html..

CISCO . 2018. CISCO - Reporte Anual de Ciberseguridad de Cisco 2018. . [En línea] 2018. https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf..

Concepto Definición. Concepto Definición Error. [En línea] https://conceptodefinicion.de/error/.

Congreso de la República. NOTINET. [En línea] https://notinet.com.co/Ley 1273 de 2009.php?idinv=237957..

CORLETTI ESTRADA, Alejandro. ISO-27001 LOS CONTROLES (Parte I). .

DACCACH T, José Camilo. Ley de Delitos Informáticos en Colombia. [En línea] https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia.

DE PABLOS HEREDERO, Carmen. LÓPEZ HERMOSO AGIUS, José Joaquín. Organización y transformación de los sistemas de información en la empresa.. Organización y transformación de los sistemas de información en la empresa.

Delta Asesores. *Ley de Delitos Informáticos en Colombia.*

Derecho Informático. SEGURIDAD INFORMÁTICA: Mientras los hackers mejoran en ofensiva, las empresas desmejoran en defensa. [En línea] https://derechoinformatico.co/seguridad-informatica-mientras-los-hackers-mejoran-en-ofensiva-las-empresas-desmejoran-en-defensa.

DIAZ PEÑA, Yamileth. RCN Radio. [En línea] https://www.rcnradio.com/colombia/region-central/nevado-del-huila-se-mantiene-en-alerta-amarilla..

DNP Departamento Nacional de Planeación. *Guía metodológica para la administración de riesgos en seguridad de la información. .* [En línea] Https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.

EAE BUSINESS SCHOOL. Software libre para empresas. ¿Qué ventajas tiene? . [En línea] https://www.eaeprogramas.es/empresa-familiar/software-libre-para-empresas-que-ventajas-tiene..

ECURED. ECURED - Cliente-Servidor. [En línea] https://www.ecured.cu/Cliente-Servidor.

ELLINGWOOD, Justin. Siete medidas de seguridad para proteger tus servidores. [En línea] https://www.digitalocean.com/community/tutorials/siete-medidas-de-seguridad-para-proteger-tus-servidores-es..

ESCRIVÁ, Gema y ROMERO, Rosa y RAMADA, David. 2013. *Seguridad informática.* s.l. : Macmillan Iberia, S.A., 2013.

ESPITIA BERNAL, Iván David. Administración Informática. . [En línea] https:/

SEYMOUR, Joseph. HORSLEY, Terry – APC by Schneider Electric. Revisión 1 - Los siete tipos de problemas en el suministro eléctrico. Informe interno 18./administacioninformatica.wordpress.com/.

FAJARDO DE LA ESPRIELLA, Estefanía. EL HERALDO. En el futuro los ciberataques serán más destructivos. [En línea] https://www.elheraldo.co/ciencia-y-tecnologia/en-el-futuro-los-ciberataques-seran-mas-destructivos-385293..

FERNANDEZ ALARCÓN, Vicenc. *Desarrollo de sistemas de información. Una metodología basada en el modelado. 2006.* s.l. : Ediciones UPC.

Foro de Seguridad. Foro de Profesionales Latinoamericanos de Seguridad. Qué es la extorsión. [En línea] www.forodeseguridad.com..

GARCIA BALAGUERA, Vivian Andrea, ORTIZ GONZALEZ, Jhon Jarby. Análisis de Riesgos según la Norma ISO 27001:2013 para las Aulas Virtuales de la Universidad Santo Tomás, Modalidad Presencial. Cundinamarca: Tesis Especialización en Seguridad Informática. B. [En línea]

GIMÉNEZ ALBACETE, José Francisco. 2014. *Seguridad en equipos informáticos (MF0486_3),.* s.l. : IC Editorial, ProQuest Ebook Central, 2014.

GÓMEZ FERNÁNDEZ, Luis y ÁLVAREZ, Ana Andrés. 2012. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes,.* s.l. : AENOR - Asociación Española de Normalización y Certificación ProQuest Ebook Central, 2012.

GÓMEZ VIEITES, Álvaro. *Ponencia - Tipos de ataques e intrusos en las redes informáticas.*

GONZALEZ, Cecilia. *LA NACIÓN. Preocupante panorama de seguridad en el Huila.*

GSH Grupo Soluciones Horizonte. Etapas de un proceso de Selección de Personal. . [En línea] https://www.gsh.com.co/blog/etapas-de-un-proceso-de-seleccion-de-personal.

GTDI. Tecnologías de la Información y Consultoría. Publicadas correcciones (Cor1:2014) a la ISO/IEC 27001:2013 e ISO/IEC 27002:2013. . [En línea] https://www.gtdi.pe/correccion_a_27001_27002..

GUILLEN HERNÁNDEZ, Oscar Armando. Universidad Juárez Del Estado De Durango. . [En línea] https://oacch.files.wordpress.com/2016/02/software-dac3b1ino-2.pdf..

INCIBE. Instituto Nacional de Ciberseguridad (INCIBE) Vídeo SGSI - 07 (INTECO) Los activos de Seguridad de la Información. . [En línea] https://www.youtube.com/watch?v=THnQ2FH7NtU..

SME Instituto Nacional de Ciberseguridad de España MP, S.A. [ES] – INCIBE: Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? . [En línea] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian..

INDECOPI [En línea] 2014. https://canvas.utp.edu.pe/courses/8870/files/42244/download?download_frd=1..

INTYPEDIA. Video Lección 11: Análisis y gestión de riesgos (intypedia) . [En línea] https://www.youtube.com/watch?v=EgiYIIJ8WnU..

ISO. Sistema de Gestión de Seguridad de la Información. S.P.I. . [En línea] www.ISO27000.ES..

ISOTOOLS. ISO 27001 Seguridad de los equipos informáticos. h. [En línea] ttps://www.isotools.org/2014/09/09/iso-27001-seguridad-equipos-informaticos..

JIMÉNEZ, Carolina. *La República. ¿Es hora de cambiar su computador?*

JIMÉNEZ, José Alfredo. 2009. *Evaluación: seguridad de un sistema de información, , .* s.l. : El Cid Editor apuntes, 2009.

KOSUTIC, Dejan. *ADVISERA - Resumen del Anexo A de la Norma ISO 27001:2013.*

LATINOAMERICA, ESET. Cómo prevenir y evitar la fuga de información empresarial. [En línea] https://www.portafolio.co/mis-finanzas/ahorro/prevenir-evitar-fuga-informacion-empresarial-100890.

MAGERIT . *Método de Análisis de Riesgo – Activos. MAGERIT VERSIÓN 3.O: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I- Método.*

MAGERIT. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.*

MICROSOFT ACCESS. [En línea] https://www.ecured.cu/Microsoft_Access.[En línea] https://www.ecured.cu/Microsoft_Access.

Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. [En línea]

MINTIC. Modelo de Seguridad y Privacidad de la Información. . [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Modelo de Seguridad. Guía 14 - Plan de comunicación, sensibilización, capacitación. [En línea] https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html..

MORENO, Letty y PALACIOS, Yaciry. *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2013 para la empresa Unisanar IPS de Quibdó. Tesis Especialización en Seguridad Informática, Chocó: Universidad abierta y a dis.*

MOVISTAR. [En línea] http://atencionalcliente.movistar.co/proteccion-al-usuario/pdf/Factores%20de%20la%20velocidad%20de%20Internet.pdf..

MOVISTAR - Mejorando el Wifi. [En línea] https://comunidad.movistar.es/t5/Soporte-Fibra-y-ADSL/Mejorando-el-Wi-Fi/td-p/989996..

NIEVES, Arlenys Carolina. *Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) basados en la Norma ISO/IEC 27001:2013. Tesis Especialización en Seguridad de la Información.* Cesar : Institución Universitaria Politécnico Gran Colombiano.

NOTINET. [En línea] https://notinet.com.co/leermas_noticiasinv.php?idinv=237957..

Congreso de la República. Ley 1581 de 2012 - NOTINET. . [En línea] https://notinet.com.co/leermas_noticiasinv.php?idinv=237957..

NUÑEZ, William Andrés y VERGARA, Édison Andrés. *Diseño del Sistema de Gestión de Seguridad de la Información para la Empresa "Serexcel" Servicios Funerarios. Tesis Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas.* Bogotá D.C : s.n.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN RODRÍGUEZ, Fernando y ARIAS FLÓREZ, Miguel Eugenio & DAZA-MARTÍNEZ, Libardo Alberto. 2010). *Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.* 2010).

ONA SYSTEMS. *Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas.*

OSI - Oficina de Seguridad del Internauta de INCIBE - ¿Quiénes son los ciberdelincuentes y qué buscan? . [En línea] https://www.osi.es/es/campanas/los-ciberdelincuentes-quienes-son/quienes-son-los-ciberdelincuentes-y-que-buscan.

PANDA SECURITY - TEMPEST y EMSEC. PANDA SECURITY - TEMPEST y EMSEC: ¿Son posibles los ciberataques a partir de las emanaciones electromagnéticas? [En línea]

https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberataques-emanaciones-electromagneticas/.

PANDA SECURITY. ¿Qué es un Ransomware? . [En línea] Un Nuevo Modelo de Ciberseguridad ha nacido. [En línea] https://www.pandasecurity.com/es/business/adaptive-defense/.

PANDASECURITY. [En línea] https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/.

PARSON, Aaron. ¿Cuáles son las diferencias entre acceso lógico y acceso físico? [En línea] https://techlandia.com/cuales-son-diferencias-acceso-logico-acceso-fisico-info_202346/.

PERPIÑAN, Antonio. 2011. *Seguridad de sistemas GNU/Linux. Fundación código libre dominicano.* 2011.

PESO NAVARRO, Emilio del, GONZÁLEZ RAMOS, Miguel Ángel. 2015. *La seguridad de los datos de carácter personal 2003. .* s.l. : Ediciones Díaz de Santos, 2015.

PUIG CARLES, Ignacio,. *LEGALIS CONSULTORES. Delitos informáticos 9 – chantaje informático.*

RESTREPO, Jenny Fernanda. *Diagnóstico del estado actual de la Seguridad de la Información basado en la Norma ISO 27001:2013, de la Institución Educativa Técnico Industrial Sede Mercedes Pardo de Simmonds de la Ciudad de Popayán. Tesis Especialización en.*

RIOJASALUD. Correo electrónico (virus informáticos). [En línea] https://www.riojasalud.es/salud-publica-y-consumo/consumo/el-rincon-del-consumidor/4766-correo-electronico-virus-informaticos.

Secretaria Distrital del Hábitat. SECRETARIA DISTRITAL DEL HÁBITAT - Ley 1266 de 2008. [En línea] https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008.

Seguridad Informática*. Actualidad TIC, Revista del Instituto Tecnológico de Informática, 1.* GADALMEZ, Pablo. 2003. 2003.

Seguridad Superior. SEGURIDAD SUPERIOR. ¿Qué es la Seguridad Física? [En línea] https://www.seguridadsuperior.com.co/que-es-la-seguridad-fisica..

SEMANA. Tecnología. Así está Colombia en el ranking de ciberseguridad mundial. [En línea] https://www.semana.com/noticias/seguridad-informatica/103543..

SHUM XIE, Yi Min. Situación digital y social media en Colombia 2019. yiminshum.com/digital-social-media-colombia-2019. [En línea]

TOLA FRANCO, Diana Elizabeth. *Implementación de un sistema de gestión de seguridad de la seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. Tesis Facultad de Ingeniería en Electricidad y Computación.*

TOPRATEDANTIVIRUS - *EL MEJOR ANTIVIRUS PARA MAC DEL 2019.*

UTN.BA Universidad Tecnológica Nacional. Seminario ISO 27001 - 09 Septiembre 2014. [En línea]

UTN.BA 2014 Universidad Tecnológica Nacional. Seminario ISO 27001. [En línea] 09 de 2014. https://es.slideshare.net/cgcutn/seminario-iso-27001-09-septiembre-2014..

VANGUARDIA. ¿Qué es un antivirus informático? TECH 29 dic 2018. [En línea] https://vanguardia.com.mx/articulo/que-es-un-antivirus-y-para-que-sirve..

VILLASEÑOR, Benjamín. UHMASALUD. Salud laboral: La temperatura en el trabajo. [En línea] https://www.uhmasalud.com/bid/285662/salud-laboral-la-temperatura-en-el-trabajo..

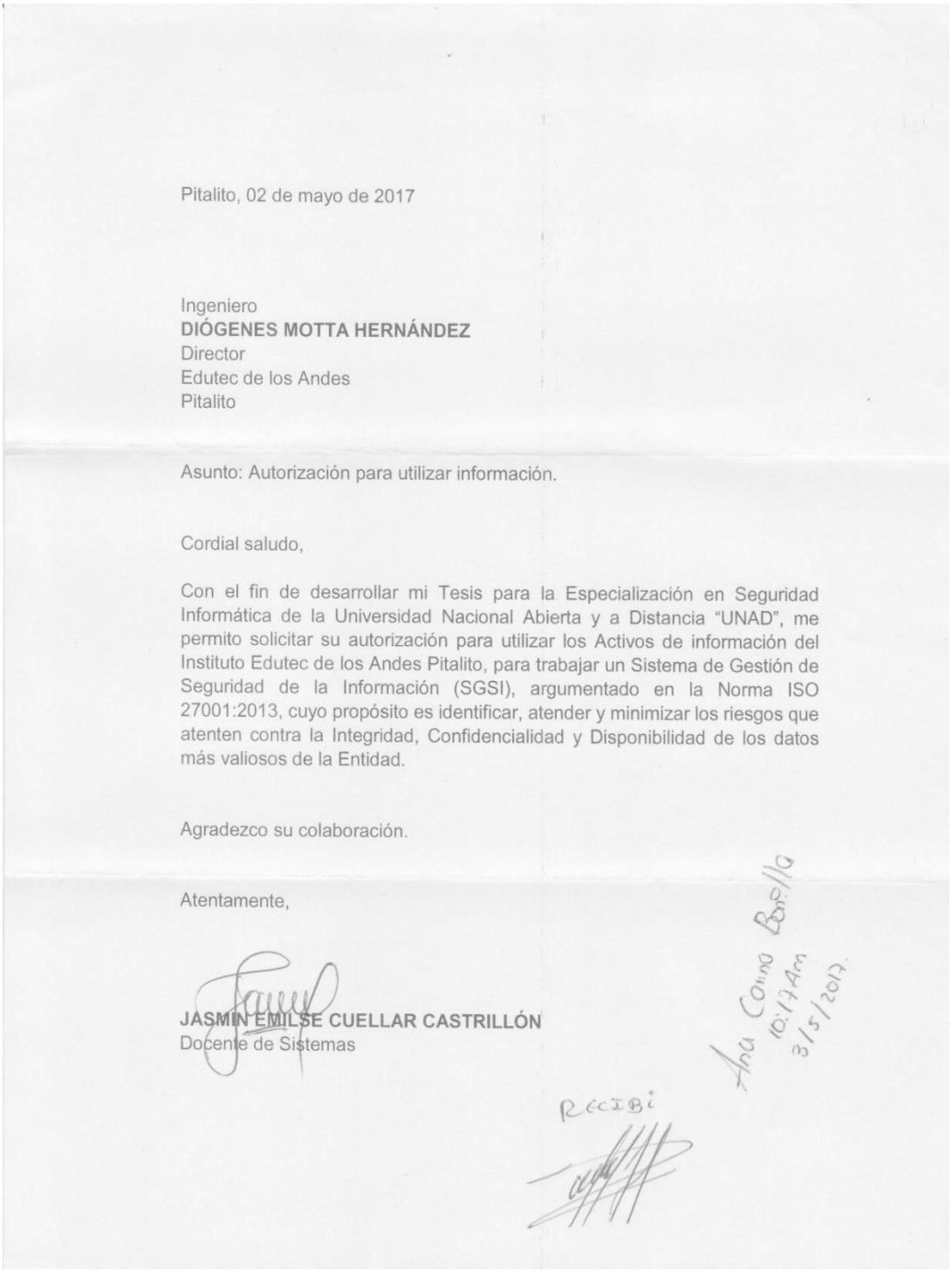
WELIVESECURITY – ESET. 11 errores de seguridad que probablemente sigues cometiendo. [En línea] https:/www.welivesecurity.com/la-es/2015/07/22/11-errores-de-seguridad-sigues-cometiendo.

YÁÑEZ CÁCERES, Nelson Alejandro. *Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño. Tesis Magister en Tecnologías de la Información. Facultad de Ciencias Físicas y Mat.*

ZONAECONOMICA. Concepto de Control. [En línea] https://www.zonaeconomica.com/control.

ANEXOS

Anexo 1 Carta de permiso y autorización de utilizar información para tesis.



Pitalito, 02 de mayo de 2017

Ingeniero
DIÓGENES MOTTA HERNÁNDEZ
Director
Edutec de los Andes
Pitalito

Asunto: Autorización para utilizar información.

Cordial saludo,

Con el fin de desarrollar mi Tesis para la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia "UNAD", me permito solicitar su autorización para utilizar los Activos de información del Instituto Edutec de los Andes Pitalito, para trabajar un Sistema de Gestión de Seguridad de la Información (SGSI), argumentado en la Norma ISO 27001:2013, cuyo propósito es identificar, atender y minimizar los riesgos que atenten contra la Integridad, Confidencialidad y Disponibilidad de los datos más valiosos de la Entidad.

Agradezco su colaboración.

Atentamente,

JASMIN EMILSE CUELLAR CASTRILLÓN
Docente de Sistemas

Ana Carina Bonilla
10:17 Am
3/5/2017.

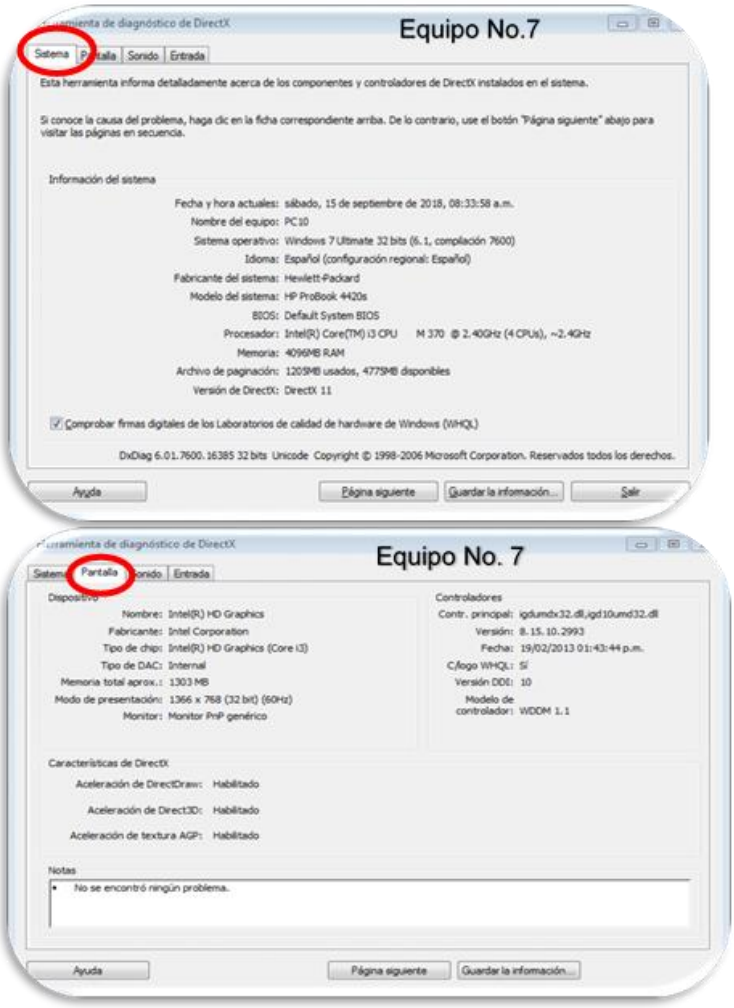
RECIBI

Fuente: La autora.

EXTRACCIÓN DE INFORMACIÓN

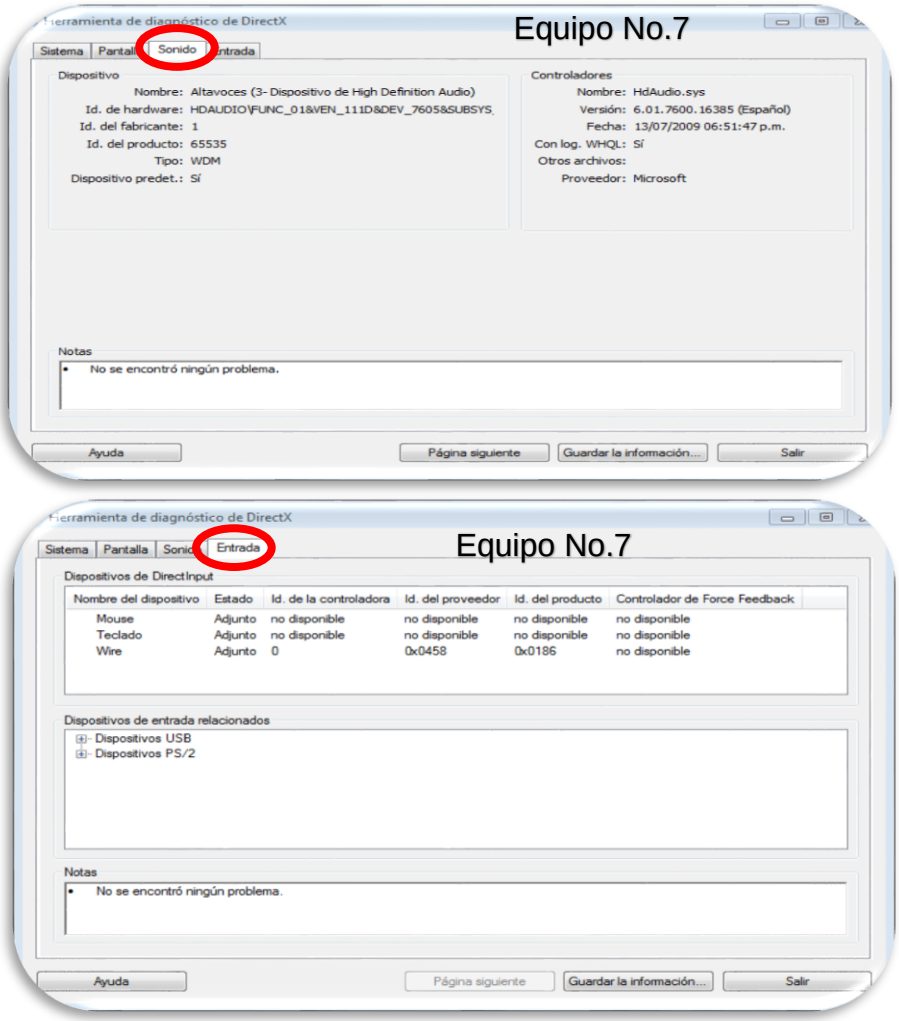
Mediante la herramienta Dxdiag.exe, se extrae la información de los equipos informáticos que hacen parte de las aulas de sistema y la parte administrativa de la institución. En este diagnóstico se obtiene información relevante del sistema, pantalla, sonido y entrada del equipo.

Anexo 2 Diagnostico a equipo No. 7 dxdiag



Fuente: La autora.

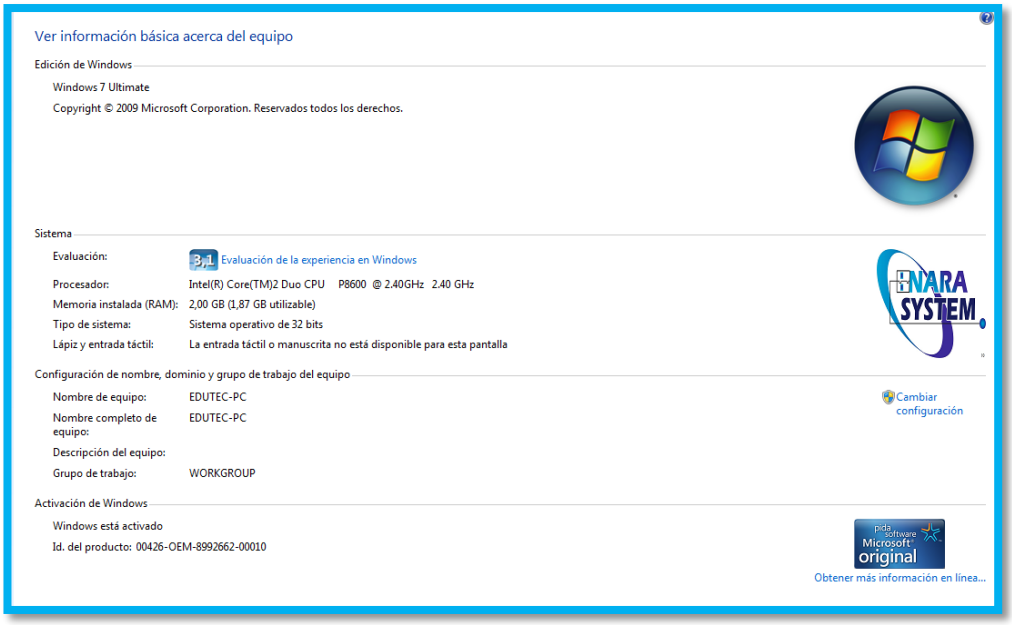
Anexo 3 Diagnostico a equipo No. 7 dxdiag



Fuente: La autora.

Por panel de control, dando clic en sistema se obtiene la siguiente información del equipo seleccionado:

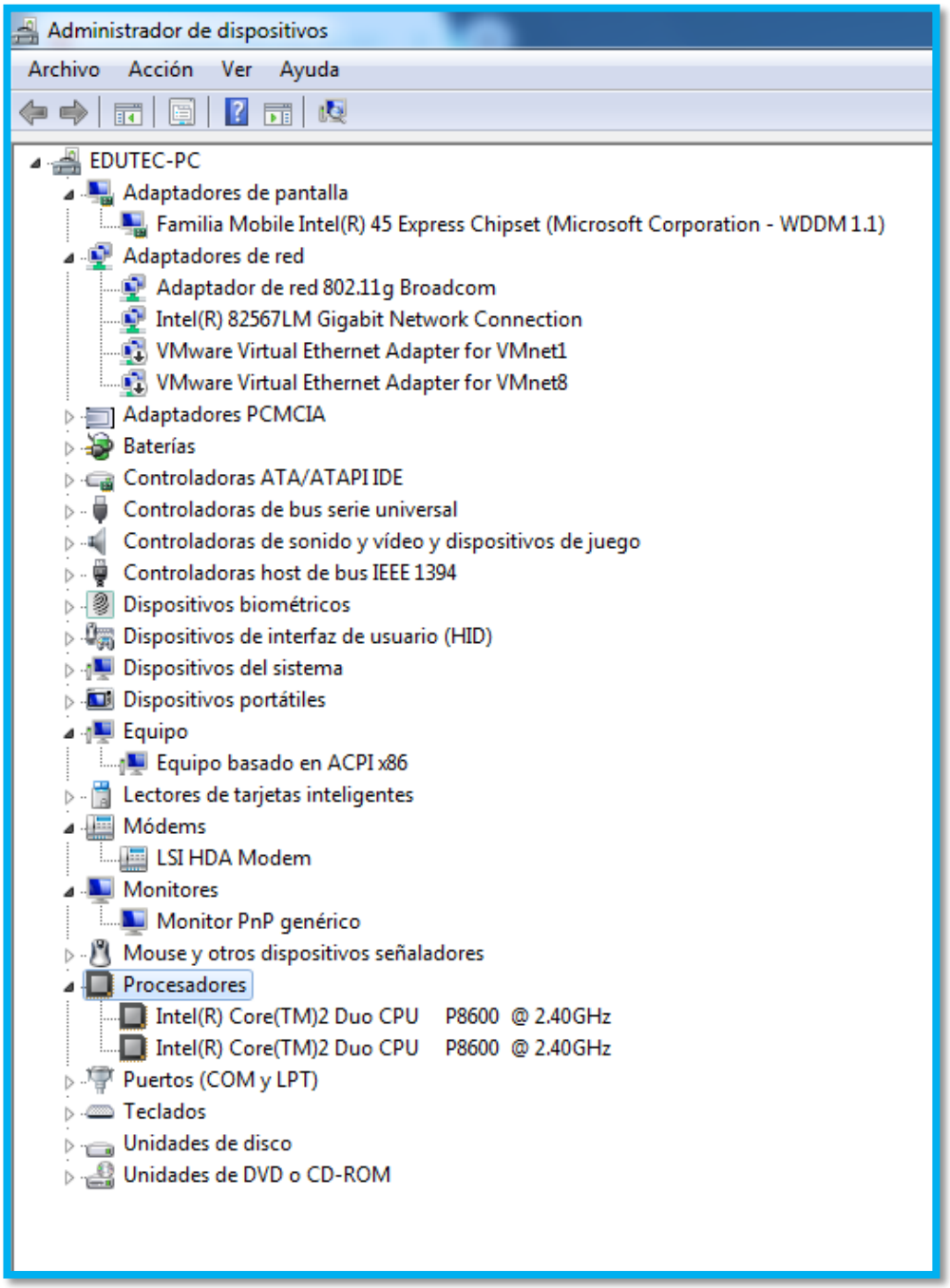
Anexo 4 Información básica del equipo.



Fuente: La autora.

Con el comando msinfo32, se extrae información del sistema. Este programa está diseñado para dar a los usuarios de Windows, una lista que comprende el hardware de la computadora, los recursos generales, el software y la configuración de Internet.

Anexo 5 Información extraída con el comando msinfo32.



Fuente: La autora.

Anexo 6 Formato reporte de daños e incidentes.

Se propone el siguiente formato para reportar daños e incidentes en los ordenadores.

EDUTEC DE LOS ANDES PITALITO
APROBADO SEGÚN RESOLUCIÓN 268 DE 2011

REPORTE No.	
FECHA:	
AULA DE SISTEMAS:	

HORA:	

REPORTE DE DAÑOS EN EQUIPOS INFORMÁTICOS		
EQUIPO No.	DESCRIPCIÓN DEL INCIDENTE	FIRMA

FIRMA DE QUIEN REALIZA EL REPORTE

Fuente: La autora.