ANÁLISIS DE RIESGOS BASADO EN LA NORMA MAGERIT V3 DE LA RED WLAN DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL TOLIMA

AMPARO ORTIZ ARISTIZABAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA II
IBAGUÉ
2021

ANÁLISIS DE RIESGOS BASADO EN LA NORMA MAGERIT V3 DE LA RED WLAN DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL TOLIMA

AMPARO ORTIZ ARISTIZABAL

Monografía como trabajo de grado para optar por el título de

Especialista en Seguridad Informática

Director:

YESNIR ANTONIO REDONDO DANIEL

Universidad Nacional Abierta y a Distancia (UNAD)
Escuela de Ciencias Básicas e Ingeniería
Especialización En Seguridad Informática
Ibagué - Tolima
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Ibagué, mayo de 2021

DEDICATORIA

AMPARO ORTIZ ARISTIZABAL

Dedico este triunfo a Dios todo poderoso y a mi querida familia, quienes son mi mayor orgullo y ejemplo, me han enseñado a ser lo que soy, que me han mostrado el camino del bien y que me han alentado siempre a dar lo mejor. También dedico este trabajo a mi esposo por su valiosa colaboración y por los momentos tan maravillosos e inolvidables que compartimos.

AGRADECIMIENTOS

A la UNAD y su grupo de trabajo por permitirme avanzar en este proyecto a quienes expreso mis más sinceros agradecimientos.

Al Director del proyecto ingeniero Yesnir Antonio Redondo Daniel, por sus buenos consejos, apoyo incondicional en la orientación del presente proyecto para lograr los objetivos propuestos.

CONTENIDO

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

IP: La dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo que utilice el protocolo o (*Internet Protocol*), que corresponde al nivel de red del modelo TCP/IP.

MAGERIT: El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos).

SGSI: Un Sistema de Gestión de la Seguridad de la Información (SGSI) (en inglés: *Information Security Management System* ISMS) es un conjunto de políticas de administración de la información. Significa para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

WEP: *Wired Equivalent Privacy* (WEP), en español «Privacidad equivalente a cableado», es el sistema de cifrado incluido en el estándar IEEE 802.11, como protocolo para redes Wireless que permite cifrar la información que se transmite.

WiFi: es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi, pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica.

WLAN: (del inglés *wireless local area network*) es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas. Las redes de área local inalámbrica utilizan las ondas de radio para llevar la información de un punto a otro, sin necesidad de un medio físico guiado.

WPA: *Wi-Fi Protected Access* (WPA), en español “Acceso Wi-Fi protegido”, es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, *Wired Equivalent Privacy* (WEP).

INTRODUCCIÓN

Las instituciones de educación superior del Tolima, debido a las funciones masivas en cuanto a manejo de personal administrativo, estudiantado y toda la información digital que circula en torno a esta población y sus funciones y/o necesidades; requiere, para asegurar su estabilidad y confianza, establecer y seguir ciertas normas y reglas de seguridad, que son muy importantes para minimizar los riesgos que puedan amenazar al funcionamiento, la integridad de los procesos y por ende su funcionamiento.

En ese sentido, Perafán y Caicedo, señalan que: "Manejar datos tan delicados como son los relacionados a los historiales académicos de los estudiantes, los laborales de los funcionarios y demás registros importantes para las instituciones, se hace estrictamente necesario implantar políticas encaminadas a garantizar el correcto funcionamiento e integridad de todas las plataformas educativas y administrativas".[1]

---

[1] **ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012.** https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

Hoy en día se podría mencionar que los sistemas de información hacen parte de los procesos que conllevan al buen desempeño de las instituciones, empresas y entidades, en ellos encontramos un valor muy importante los “datos” que reposan en los motores de bases de datos y son accesibles mediante los sistemas de información, los cuales están enfocados a alcanzar los respectivos logros de los objetivos misionales, estos objetivos se pueden optimizar, mejorar y manteniendo un sistema de información y documentación, que vaya acorde con los intereses de las instituciones de educación superior.

El no disponer de sistemas de seguridad actualizados que garanticen la integridad de los procesos y sistemas de intercomunicación, podría exponerlos fácilmente a sufrir ataques tanto internos como externos, no solo a la red que la intercomunica, sino también a las bases de datos donde se almacena los materiales comunicativos.

Es por estos motivos que es necesaria la implementación de la “Planificación de un sistema de Información” (PSI) ya que en el caso contrario las organizaciones

---

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

pueden enfrentar problemas judiciales, desprestigio y falta de credibilidad, al no garantizar las condiciones para el correcto funcionamiento. Se debe optimizar el trabajo de los empleados y a su vez garantizar la seguridad e integridad de lo que circula en la red, pues se trata de información sensible y de vital importancia para las instituciones de educación superior del Tolima que serán el objeto de estudio de este proyecto.

Las redes WLAN son sistemas de comunicaciones de datos inalámbricos, que se constituyen como una alternativa a las redes de área local por medio de cable, o también como complemento a estas, utilizando la radiofrecuencia para transmitir y recibir datos, mediante el uso de ondas electromagnéticas. Esto genera mayor movilidad a los usuarios"[2] y su uso se puede realizar desde diferentes tipos de dispositivos.

Para lograr óptimas condiciones de seguridad en las instituciones de educación superior del Tolima, el presente proyecto radica y hace importante la implementación de una auditoría de seguridad (análisis de riesgos) en las redes WLAN, puesto que:

> El inconveniente más importante que supone el uso de este tipo de redes es el tema de la seguridad. Al ser el aire el medio de propagación empleado por las ondas, hace que la información esté expuesta a sufrir ataques. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz del de sus comienzos"[3].

Aplicando la tercera "versión de la metodología de análisis y gestión de riesgos de los sistemas de información (Magerit v.3)"[4], se busca trazar un protocolo que permita el uso más eficiente y seguro de esta red de información interna dentro de las instituciones de educación superior.

---

[2] AUTOR, D. N. (14 de 02 de 2013). *http://derechodeautor.gov.co/.* Obtenido de http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_

[3] CERVERA, R. C. (s.f.). *https://www.ucm.es/.* Obtenido de https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf

[4] españa, G. d. (10 de 2012). *https://www.ccn-cert.cni.es/.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

1. PLANTEAMIENTO DEL PROBLEMA

Como parte del funcionamiento habitual en las instituciones de educación superior del Tolima, se procesa un gran flujo de información delicada, relacionada con los procesos académicos de los estudiantes activos y egresados, así material esencial para los funcionarios y sus labores diarias y otro tipo de registros de tipo académico, como investigaciones e información institucional. La seguridad de toda esta cantidad de datos es el problema a solucionar, pues gran parte de ellos y de las operaciones que se derivan de su manejo, quedan guardados en los servidores con que cuentan cada institución de educación superior, lo que implica que tanto entes internos como externos a ella, tengan un posible control de la red y por tanto, acceso a archivos de vital importancia, cuyo seguimiento y restricciones para la red interna deben ser examinados. Por esa razón, se propone realizar un análisis de seguridad, que garantice un manejo adecuado y estable de la información.

1.1 DESCRIPCIÓN DEL PROBLEMA

Actualmente las instituciones de educación superior del Tolima[5] cuentan con oficinas de informática y telecomunicaciones. Estas oficinas tienen como objetivo asegurar, mantener y mejorar la topología de red en las instituciones, con el fin de contar siempre con la tecnología adecuada. También, tiene dentro de sus funciones proporcionar de forma confiable las herramientas informáticas para la comunidad universitaria, y así mejorar la calidad de sus servicios en cuanto a cobertura, seguridad y acceso.

Dentro de sus funciones se encuentran:

- “Gestionar políticas y lineamientos de informática para cada una de las instituciones educativas
- Investigar las tendencias tecnológicas en teleinformática y evaluar su incorporación a las instituciones educativas, para buscar el apoyo tanto en la administración, la docencia, la investigación y la proyección social.
- Mantener un sistema de información integral y consistente, que brinde apoyo a la toma de decisiones.
- Vigilar que se cumplan todas las normas, leyes y estándares, que ayuden al buen uso de los servicios en la informática y las telecomunicaciones.
- Velar por el buen funcionamiento de los recursos informáticos y telecomunicaciones.
- Desarrollar e implantar soluciones al nivel de hardware y software.

[5] españa, G. d. (10 de 2012). Portal administracion electronica. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- Instalar, mantener y garantizar la disponibilidad de aplicaciones académico-administrativas.
- Asesorar y dar soporte técnico a todos los usuarios.
- Apoyo y capacitación en TIC para la docencia, investigación y extensión.
- Coordinar con el comité de desarrollo a la docencia la elaboración de planes de capacitación en TIC para los profesores de las instituciones educativas.
- Coordinar con las dependencias de talento humano la elaboración de planes de capacitación en TIC para el personal administrativo de las instituciones educativas"[6].Co

[6] Excellence, I. (21 de 05 de 2015). ISOTools Excellence. Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complemen

Es importante que cada institución de educación superior del Tolima, maneje y tenga mecanismos de seguridad como es el caso de la autenticación a la hora de autenticar un usuario a sus redes, si este mecanismo no existe, cualquier persona puede hacerlo sin problema alguno.

Es necesario que todas las instituciones de educación superior del Tolima diseñen políticas de control de acceso al campus universitario, debido a que si no existen pueden generar vulnerabilidades las cuales puede aprovechar terceros. Otro problema que se puede presentar es la mala implementación de contraseñas, por ello es necesario seguir todas las recomendaciones, para esto se pueden apoyar en los mecanismos de protección como la creadas por Wifi Alliance Quienes desarrollaron las configuraciones WPA y posteriormente la WPA2, dando la posibilidad de agregar claves mucho más robustas que las WEP

Otro problema que puede generar vulnerabilidad, es que haya muchos más usuarios conectados; es decir más de lo que normalmente debería usar la red, lo cual además hace que el ancho de banda de la red inalámbrica sea demasiado bajo para el número de accesos que está soportando la red.

1.2 FORMULACIÓN DEL PROBLEMA

ta%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

¿Cómo el análisis de riesgos basado en la norma MAGERIT V3, ayudará a mejorar la seguridad y control de acceso a la red WLAN en las instituciones de educación superior del Tolima?

2. JUSTIFICACIÓN

Es evidente que el ritmo actual de flujo de información en los distintos ámbitos de la sociedad y sus diferentes organizaciones como lo son en este caso las del campo educativo, más específicamente en las instituciones de educación superior del Tolima, requieren de un tratamiento especial para que el intercambio de información cumpla los requerimientos exigidos por dichas instituciones y por sus usuarios, para que la interrelación entre sus secciones y los clientes o comunidad académica, produzca como resultado el cumplimiento oportuno de todas las funciones y/o servicios esperados por las partes que los requieren.

Es precisamente esa cantidad actual de flujo de información en las instituciones, y la necesidad de su rápido y eficaz procesamiento, lo que hace indispensable el uso de recursos tecnológicos tanto de hardware como de software que garanticen eficacia tanto al momento de su almacenamiento como de su procesamiento, garantizando a su vez la respectiva seguridad de los datos durante el acceso a dichos procesos.

En las instituciones de educación superior del Tolima, se han venido presentando problemas con el acceso a las redes WLAN y falta de cobertura, aun contando con presencia de señal. Para esto, el estudio de investigación realizado identificará los problemas más comunes, los inconvenientes constantes de conectividad y el acceso sin autenticación de cualquier persona a la red, realizando un proceso de auditoría a nivel de MAGERIT V3.

Este proyecto ayudará al mejoramiento de la seguridad y calidad del servicio de acceso a internet, de los dispositivos móviles y de la comunidad estudiantil de la universidad, garantizando de esta forma los procesos académicos, administrativos y de formación, que son indispensables para el adecuado funcionamiento de las diferentes áreas de las instituciones.

De la realización del presente proyecto, se beneficiará la comunidad académica en general mediante la optimización del acceso a los diferentes servicios prestados por las universidades y el uso adecuado de los sistemas de información, ya sean clientes o administradores, los cuales gozarán de un control de acceso más adecuado, seguro y confiable.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar los riesgos y salvaguardas que se presentan en el control de acceso a las redes WLAN de las instituciones de educación superior del Tolima

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos informáticos, las vulnerabilidades, amenazas y riesgos de la red WLAN de las instituciones de educación superior del Tolima

- Sugerir los respectivos controles o salvaguardas necesarios para la seguridad y el control de acceso a las redes WLAN en las instituciones de educación superior del Tolima.

- Proveer lineamientos de seguridad mediante políticas y procedimientos que incluyen los controles de acceso a la red WLAN en las instituciones de educación superior del Tolima.

- Establecer mecanismos de sensibilización para el personal sobre temas de seguridad de la información

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

La realización de esta auditoría está orientada a toda la red WLAN de las comunidades universitarias, lo cual incluye subredes preestablecidas, también a los estudiantes y los funcionarios de las Secciones Administrativas de las instituciones de educación superior del Tolima; con el fin de lograr un manejo más seguro de la información y con un mayor rendimiento.

Específicamente, pasarán a ser objeto del presente análisis; las redes WLAN correspondientes o determinadas al uso restringido de las áreas administrativas de las universidades, proceso que incluye la revisión de rendimiento y seguridad tanto del hardware utilizado actualmente para la distribución física de las redes y la propagación de la señal inalámbrica de las mismas, como de los recursos de software o lógicos utilizados tanto para la administración de la información que circula por las redes, su procesamiento y almacenamiento, como para el control de acceso, seguridad y eficacia del sistema informático en su totalidad.

De esta misma manera se procederá con el respectivo análisis de aquellas redes que las universidades determinan como exclusivas para el uso de la comunidad estudiantil en general; comunidad que en su gran extensión está conformada por una inmensa cantidad de usuarios casi constantes y entre los cuales se encuentran generalmente las respectivas conexiones efectuadas mediante dispositivos portátiles como laptops y Smartphone, los cuales no son habitualmente gestionados dentro de un plan definido de seguridad y que están limitados a la seguridad y confiabilidad establecida por sus propios usuarios o en este caso propietarios. En estas redes “públicas” también se realizará el respectivo análisis de hardware y software implicado tanto en la difusión eficiente y oportuna de la señal, como de la gestión y garantías durante el procesamiento de datos y su seguridad.

El estudio realizado a las redes WLAN de las Universidades del Tolima, dejará plasmado en el presente proyecto pautas que puedan servir para futuras investigaciones que puedan conllevar a nuevas aplicaciones que complementen el informe en pro de la constante actualización de la seguridad informática en la Universidades.

5. MARCO REFERENCIAL

5.1 MARCO HISTÓRICO

Algunas universidades del Tolima han venido manejando sus redes WLAN sin ningún tipo de seguridad hasta el momento, cualquier persona, usuario o estudiante puede ingresar a la misma sin ningún tipo de autenticación o control para el ingreso, lo que hace de esto una gran vulnerabilidad; así mismo crea una gran exposición de seguridad para que pueda ser atacada la red por cualquier intruso o hacker que quiera realizar un ataque.

Las auditorías de seguridad en el procesamiento informático de datos, han venido, desde hace varios años, siendo establecidas en distintos países del mundo e instituciones inicialmente ligadas a entes de carácter público o gubernamental, donde desde el inicio de sus implementaciones y con la comprobación práctica de sus resultados, han logrado establecerse como procesos de carácter obligatorio debido a su importancia a la hora de garantizar seguridad e integridad de datos indispensables para el funcionamiento de las mismas instituciones y también al momento de ofrecer seguridad, eficacia y sobre todo confiabilidad a sus potenciales usuarios o clientes.

Recientemente, en el transcurso del año 2013, se realizó una propuesta de seguridad informática que incluía: "el diseño e implementación de un sistema de gestión de la seguridad información (SGSI), en el Hospital San Andrés de la ciudad de Tumaco, al que le dieron el nombre de INFOSALUD"[7], el cual presentaba

---

[7] Humanas, E. d. (s.f.). urosario.edu.co. Obtenido de https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf **ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012.** https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. **AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013.** http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_. **BLACUTT, Roberto Vargas. 2009.** https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y. **CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018.** http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.
CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.
CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.
ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.

problemas de seguridad en el acceso de los usuarios al sistema, en la base de datos y en los servidores Windows Server. En este proyecto, se utilizó dentro del marco

LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

de referencia y junto a otras la metodología MAGERIT, y se realizó mediante objetivos como los presentados en el presente proyecto.[8]

[8] Informática, O. d. (2020). esap.edu.co. Obtenido de https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.

GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017.

https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..
OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.
PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

Estos procesos llevados a cabo, hacen evidente la necesidad de efectuar este tipo de análisis a los sistemas de información para garantizar su funcionamiento oportuno, respectiva seguridad y así transmitir confianza a sus usuarios.

5.2 MARCO TEÓRICO

Lo más importante en las empresas tanto públicas como privadas es la información, por lo que en las instituciones de educación superior del Tolima se hace necesario garantizar la seguridad tanto física como lógica, por medio de políticas que ayuden a salvaguardar, proteger la información. Esto quiere decir que es necesario asegurar su privacidad y de la misma manera proteger las operaciones por daños ya sean de forma intencional o no, dentro del entorno de la red.

La proyección de la seguridad en el diseño de la red es muy importante, debido a que es necesario conservar la integridad, confidencialidad y disponibilidad de la información. La seguridad no se basa solo en la implementación y creación de usuarios y contraseñas, aunque en el tema de las redes es de mucha ayuda, debido a que es de gran ayuda para garantizar su buen funcionamiento, evitando que se realicen trabajos posteriores, ayudando a minimizar la pérdida de información y posibles daños a las redes universitarias. Generando confianza, que es uno de los valores críticos, especialmente sensibles en organizaciones públicas[9].

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

[9] informatica, O. d. (s.f.). instituciones.sld.cu. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1

MAGERIT V3 en la cual está basado el presente proyecto, contempla primeramente la visión conjunta de la gestión de riesgos, “En otras palabras, esta metodología implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información”[10]

“Siguiendo la terminología de la normativa ISO 31000, MAGERIT divide en dos grandes tareas a realizar”[11]:

[10] John Jairo Perafán Ruiz, M. C. (2014). repositorio unad.edu.co. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3

[11] Jorge Eliécer Ojeda-Pérez, F. R.-R.-F.-M. (12 de 2010). SciELO. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones.

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

1. El análisis de riesgos (Que determina que posee la organización y lo que le podría pasar en su estado actual de seguridad).
2. El tratamiento de los riesgos (ayuda a establecer la defensa y el camino a las posibles emergencias).

Seguidamente, dentro del primer punto, MAGERIT considera los siguientes elementos:

1. La determinación de activos y el coste de sus posibles daños.
2. Determinar las amenazas a las cuales están expuestos aquellos activos y los posibles perjuicios causados a la organización en caso de daño.
3. Determinar las salvaguardas (contra medidas) dispuestas y su actual efectividad.

   Con estos elementos ya previamente determinados, se pueden realizar las siguientes estimaciones:

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

- ✓ Estimar el impacto sobre los activos tras la materialización de las amenazas.
- ✓ Estimar el riesgo o expectativas de probable materialización de las amenazas.

Para luego continuar tras este análisis metódico y sus respectivas conclusiones, con el proceso de gestión de los riegos:

En el primero, "a la vista de los impactos y riesgos concluidos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores"[12]:

1. La gravedad del impacto y/o del riesgo.
2. Las instituciones del Tolima también presenta obligaciones a las que por ley debe estar sometidas.
3. Por medio de los reglamentos sectoriales o internos la universidad presenta obligaciones a las que debe estar sometida.
4. Por último existen obligaciones por contrato a los que debe estar sometida la Universidad.

En este marco las instituciones de educación superior, pueden presentar un margen de maniobra por medio del cual, surgen consideraciones adicionales sobre los impactos de naturaleza intangible:

1. La imagen pública de cara a la Sociedad (aspectos que tiene que ver con el buen nombre o de confiabilidad de la institución).
2. Política interna: Como son las relaciones con los propios funcionarios, si existe la capacidad para contratar al personal idóneo, si es posible retener a los mejores y soportar rotaciones de personas, etc.
3. Vínculos con proveedores, capacitados para lograr algunos acuerdos que sean beneficiosos a corto, medio o largo plazo y de conseguir un trato prioritario, etc.
4. Se debe tener nexos con los clientes o usuarios (comunidad universitaria), definidos como la capacidad para ayudar a retener, incrementar la oferta, y distinguirse frente a la competencia.
5. Afinidad con otras organizaciones, Esto puede ayudar a conseguir acuerdos estratégicos, alianzas, trabajo colaborativo, etc.
6. Nuevas oportunidades de negocio, implementando diferentes mecanismos que ayuden a recuperar la inversión en seguridad, que permitan salvaguardar la información.
7. Acceso a sellos, calificaciones o certificaciones reconocidas de seguridad, que a su vez brindan una imagen confiable al cliente potencial.

[12] López, G. (s.f.). IMF Blog de Tecnologia. Obtenido de https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/

Todo esto ayuda a desarrollar una calificación de cada uno de los riesgos significativos determinados de la siguiente forma:

1. Es crítico cuando la atención requerida es urgente.
2. Es grave cuando requiere atención médica.
3. Es apreciable, puede ser objeto de estudio para su debido tratamiento.
4. Es asumible, no se tomarán acciones para detener el riesgo.

En esta última, se presenta la aceptación del riesgo, pero, es muy importante tomar buenas acciones ya que es una decisión arriesgada y hay que abordarla con prudencia y justificación y se pueden presentar; "cuando el impacto residual es asumible, el riesgo residual es asumible, el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales"[13].

"La calificación de los riesgos tendrá consecuencias en las tareas consecuentes, siendo este un factor básico para instaurar la prioridad relativa de las diferentes actuaciones"[14] dentro del tratamiento posterior. A partir de aquí, las decisiones son de los órganos de gobierno o dirección de la organización, en este caso de las directivas de la Universidades del Tolima, quienes deberán actuar según los siguientes 2 pasos:

1. Evaluación (es importante interpretar cuales son los valores de impacto y su riesgo residual).
2. Tratamiento (donde la dirección decide si aplica se hace necesario algún tratamiento al sistema de seguridad para su protección), donde es necesario aplicar las siguientes opciones:

    - Reducir el riesgo residual (aceptar un riesgo pequeño).
    - Ampliar el riesgo residual (aceptar un riesgo mayor).

Tras la correspondiente evaluación detallada de los resultados obtenidos (interpretación de los valores de impacto y riesgo residual) y aceptación de los riesgos comprobados, esta parte del proceso (Tratamiento) está directamente involucrada para su posterior efectividad, con el estudio cuantitativo de costes/beneficios y la toma de decisiones de las correspondientes directivas para su respectiva aplicabilidad. [15]

---

[13] LUNA, J. F. (2017). repository.unad.edu.co. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y

[14] españa, G. d. (10 de 2012). *https://www.ccn-cert.cni.es/.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[15] españa, G. d. (10 de 2012). https://www.ccn-cert.cni.es/. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Es así como desde el inicio del presente proceso, el seguimiento y la revisión de sus etapas, son parte fundamental junto a los estudios cuantitativos económicos para la exitosa realización y finalización de la gestión de seguridad en las universidades del departamento del Tolima.

5.3 MARCO CONCEPTUAL

Se describen algunos actores que en general conforman el departamento de sistemas de las diferentes universidades del Tolima, con el fin de concretar una uniformidad en los posibles actores que brindan el soporte técnico de los diferentes sistemas de información, y servicios que en ellas se disponen al servicio de la comunidad, de los cuales se describen a continuación:

Administrador de Redes 1: Es la persona que se encarga de la supervisión a los proveedores en cuanto a las instalaciones y suministros del cableado de las redes de internet y eléctrica, los equipos computacionales y de comunicaciones.

Administrador de Redes 2: Es la persona que aplica las políticas de seguridad y se encarga de asegurar la integridad de la información.

El área de infraestructura y redes: Es la que se encarga de la topología tecnológica, por ello debe velar por su seguridad y aplicar las mejoras que ayuden a mantener una buena infraestructura, para brindar un buen servicio a los usuarios en general.

Estudiante: Es toda persona académicamente activa en las Universidades del Tolima.

Aceptación del riesgo: Decisión que debe ser informada a favor de abordar un riesgo teniendo en cuenta las probabilidades obtenidas.

Activo: Se refiere a lo que tiene las Universidades del Tolima en materia informática, con son los componentes o funcionalidades del sistema de información, este puede presentar riesgos, lo cuales se pueden presentar por atacante de forma deliberada o accidental, cualquiera de las dos opciones representa peligro para la información manejada o almacenada y a su vez sobre las aplicaciones, equipos, recursos administrativos, físicos, problemas en las comunicaciones entre otros.

Análisis de riesgos: Se utiliza para evaluar los riesgos, cuál es su magnitud, a los que están expuestas.

Auditoría de seguridad: Para realizar el proceso de validación e identificación de las diferentes actividades del sistema de información buscando el cumplimiento de las políticas de seguridad, con el fin de comprobar si los controles aplicados ayudan al funcionamiento correcto, verificar si existen brechas de seguridad por medio de los procedimientos de acuerdo a su estructura, para establecer si son necesarios aplicar algunos cambios[16]

[16] MinEducacion. (15 de 07 de 2019). *https://www.mineducacion.gov.co/*. Obtenido de https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1**ADMINISTRACIONES, MINISTERIO DE HACIENDA Y.**

2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.
AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.
BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.
CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.
CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.
CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.
CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.
ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.

HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.

HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.

Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.

Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.

LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.

LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

5.4 MARCO LEGAL

En este aparte se hace referencia a las normativas legales nacionales e internacionales a que está sujeto el campo del análisis de gestión de riesgos en seguridad informática, cabe anotar que la relación no puede determinarse como definitiva, puesto que está sujeta a un proceso legislativo activo, por esta continua evolución normativa, es importante la obligación de estar al tanto de las novedades normativas que vayan apareciendo.

El software es producto de la imaginación de los seres humanos, considerada como "una de las estructuras más complicadas que la humanidad conoce; amparado por el Decreto 1360 del 23 de junio de 1989 por la cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derechos de Autor"[17] , el cual

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

[17] MINTIC. (s.f.). *https://www.mintic.gov.co/.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.
CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.
ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

será considerado como obra inédita, propia del dominio literario, comprendiendo uno o varios elementos. Y será inscrito frente a dicha oficina de registro.

La Ley 1273 de 2009, clasificó algunos delitos informáticos como una sucesión de procesos los cuales están relacionados con el manejo de datos personales, debido a esto es de mucha importancia que todas las organizaciones hoy en día reciban asesoría jurídica, con el fin de estar preparados y afrontar este tipo de sanciones penales. Teniendo en cuenta las modificaciones realizadas en "el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la Protección de la información

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

y de los datos buscando la preservación de los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".[18]

[18] Novoa, J. M. (16 de 10 de 2018). *http://openaccess.uoc.edu/.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.

GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017.

https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..
OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.
PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

Además, aplican otras leyes internacionales sobre seguridad electrónica, para la protección de los datos personales, firma electrónica, e información clasificada, que son relevantes para la gestión de riesgos, que bien lo exigen, sustentan o son de utilidad en el proceso.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

6. DISEÑO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

Se plantea un proceso de revisión, que pretende determinar las falencias de las redes WLAN de las instituciones de educación superior del Tolima, realizando una auditoría y pensando en la seguridad y protección de los datos como un componente fundamental dentro de un plan de administración y gestión importante, lo que conlleva en un futuro a tener más cuidado y seguimiento con la seguridad de sus redes.

El enfoque metodológico está en el análisis del estado actual del sistema informático de las Universidades, con el fin de, tras un profundo estudio e investigación de los sistemas de seguridad, determinar las medidas necesarias para asegurar la estabilidad y seguridad del acceso a sus redes WLAN, por esto el presente proyecto pertenece a la categoría de análisis y gestión de riesgos.[19]

---

[19] Otoya Verástegui, M. R. (2018). *Universidad cesar vallejo.* Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/16120

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012.

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

Para el presente análisis, se propone una metodología descriptiva-analítica, que permite recabar información y estudiarla en detalle, para finalmente ejecutar un diagnóstico adecuado.

> Por un lado, el método descriptivo se desprende de la observación directa que realiza el investigador y/o del conocimiento que ha adquirido a través de las informaciones indirectas obtenidas. Por tanto se trata de un método cuya finalidad es obtener, interpretar y presentar, con el máximo rigor o exactitud posible, la información sobre una realidad de acuerdo con ciertos criterios previamente establecidos por cada ciencia[20].

Por su parte, la investigación también será de tipo analítico, el cual busca a través de la descripción de una determinada realidad, interpretar, clasificar y explicar

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..
OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.
PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.
PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.
RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.
SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.
SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.
tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

[20] Pizarro, R. H. (05 de 2010). *core.ac.uk*. Obtenido de https://core.ac.uk/download/pdf/30043589.pdf

diferentes fenómenos y sus relaciones. Es posible así dar una explicación a todas las partes que componen dicho fenómeno. [21]

Primeramente se evaluará la efectividad de las conexiones inalámbricas teniendo en cuenta el hardware implicado en la estructuración de las redes y la difusión de las señales, el rendimiento lógico de la red, de la distribución de los anchos de banda y su respuesta ante el tráfico intenso de datos, también se analizarán los niveles de seguridad de las mismas, la confiabilidad de las autenticaciones de acceso, permisos y privilegios, por último, se realizará un análisis a la confiabilidad en el almacenamiento seguro de datos, al igual que al rendimiento de aplicaciones y hardware implicados en dicho proceso.

Durante esta revisión, también se hará un seguimiento constante al activo humano implicado en los procesos que atañen al rendimiento de las redes así como de las aplicaciones que hacen uso constante de ellas, también se realizará un estudio de seguridad referente a los equipos externos que generalmente se conectan a diario a las redes de las universidades; equipos como Smartphone y laptops propiedad de la comunidad estudiantil y que actualmente no son parte activa de las políticas de seguridad de la institución, esto con el fin de encontrar políticas seguras y fácilmente ejecutables que aseguren la interacción confiable y efectiva de estos equipos con las redes y aplicativos de las instituciones de educación superior.

6. 2 METODOLOGÍA DE DESARROLLO

El desarrollo metodológico, se realizará por medio de fases como son:

1. Identificar los activos a la fecha de las instituciones de educación superior del Tolima mediante inventarios físicos y lógicos.
2. Comprobar el rendimiento del hardware de redes mediante test.
3. Comprobar las garantías actuales que ofrece el hardware utilizado para almacenaje y procesamiento de información.
4. Analizar la disposición de los anchos de banda y comprobarlos en las redes tanto de uso externo como interno en las universidades.
5. Caracterizar los aplicativos de software actuales utilizados en las universidades y que interactúan con las redes.
6. Identificar los niveles actuales de seguridad de acceso a las redes, la disposición de permisos y privilegios de aplicativos.
7. Hacer pruebas a las salvaguardas actuales del sistema de procesamiento de información.
8. Realizar pruebas mediante software especializado a los controles propuestos según los resultados de las pruebas anteriores.

[21] Roberto Hernández Sampieri, C. F. (s.f.). https://www.uv.mx/. Obtenido de https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf

9. Seguir de cerca el rendimiento de los procedimientos manuales efectuados tanto por el personal como por la comunidad estudiantil.
10. Establecer la aplicación de medidas que mejoren el rendimiento manual sin afectar la productividad.
11. Implementación a mediano y largo plazo de cualquiera de los aspectos adicionales exigidos en el modelo MAGERIT para alcanzar un mayor nivel de seguridad.
12. Preparación y capacitación del personal en seguridad informática y disposiciones derivadas del resultado del presente análisis.
13. Organización y ejecución de controles para realizar auditorías constantes que garanticen seguridad en las redes a largo plazo. [22]

[22] **HUMANAS, ESCUELA DE CIENCIAS.** urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.

7. METODOLOGÍA DE IDENTIFICACIÓN DE RIESGOS UTILIZADA

La metodología escogida es MAGERIT ya que "implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que las directivas tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información, persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista". [23]

[23] tdx.cat. (s.f.). *www.tdx.cat.* Obtenido de https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complemen

Magerit persigue los siguientes objetivos:

Directos:

- Generar conciencia a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, ofreciendo unos métodos sistemáticos, que permitan analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Brinda ayudas para descubrir, evaluar y planificar el tratamiento oportuno para mantener los riesgos bajo control y estos no afecten otros procesos

Indirectos:
Permite preparar a la Organización para abordar procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Se ha tratado de buscar uniformidad en los informes que recogen los hallazgos y las conclusiones de las actividades resultado del análisis y gestión de riesgos:

- Modelo de valor: Se realiza un proceso de caracterización para diferenciar el valor que representan los activos informáticos intangibles y tangibles para la Organización, de igual manera las dependencias entre los diferentes activos.

---

ta%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..
OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.
PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.
PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.
RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.
SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.
SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.
tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

- Mapa de riesgos: Se define un mecanismo para relacionar las amenazas a que están expuestos los activos de la empresa.
- Declaración de aplicabilidad: Se define para un conjunto de salvaguardas, se brindan las indicaciones para saber sin son de aplicación en el sistema de información o si están bajo estudio, o por el contrario, carecen de sentido.
- Evaluación de salvaguardas: Se realiza la evaluación de la eficacia y eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- Estado de riesgo: se define una caracterización de los activos, este proceso se realiza por su riesgo residual; esto quiere decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- Informe de insuficiencias: Representa las ausencias o debilidad de las salvaguardas que no son oportunas para reducir los riesgos sobre el sistema. Estas recogen las vulnerabilidades del sistema, y se entienden como puntos que no están adecuadamente protegidos, esto puede causar que las amenazas se materialicen.
- Cumplimiento de normativa: Es la satisfacción y cumplimiento de unos requisitos. En la cual se brinda una declaración de que es adecuada a la normativa correspondiente.
- Plan de seguridad: Son un conjunto de proyectos de seguridad, los cuales permiten concretar las decisiones de tratamiento de riesgos.

Por todo lo anterior y debido a los aportes presentados se escogió dicha metodología.

8. IDENTIFICACIÓN DE RIESGOS

El proceso de análisis de riesgos nos permite tener una idea del valor y de qué manera están protegidos los activos de las organizaciones, realizando una evaluación según el método aplicado, esto con el fin de obtener conclusiones que fundamenten un proceso de un SGSI. Por tal motivo nos centraremos a realizar el respectivo análisis resaltando aquellas amenazas que son muy frecuentes y orientados por las directrices de un análisis de riesgos los cuales se describen a continuación:

a) Proceso de identificación de activos más importantes que poseen las organizaciones
b) Proceso de identificación de las diferentes amenazas que están expuestos los activos
c) Identificar las diferentes salvaguardas que están definidos para los activos
d) Realizar el proceso de valoración si en algún momento se materializa alguna amenaza

Un análisis de riesgos mal elaborado o sin la aplicación de una metodología puede ser una muy mala elección para salvaguardar los activos, ya que puede implicar una selección de mecanismos de control de seguridad los cuales no se ajustarán a las necesidades de las universidades y repercutir en un plan de contingencia que no sea el adecuado para los diferentes activos críticos.

El análisis de riesgo para las universidades, les permitirá tener una visión más clara sobre su estado de seguridad actual y brindan mecanismos para reducir las vulnerabilidades de los sistemas de información ya que estos son accesibles mediante diferentes mecanismos incluyendo la utilización de las redes WLAN que consultan información de procesos académicos. Para esto es necesario realizar un proceso de análisis de las amenazas y el impacto para todos los activos de las universidades.

Existen diversas metodologías para llevar a cabo el proceso de identificación de riesgo, En este caso se va a utilizar la metodología "MAGERIT, esta fue elaborada por el Consejo Superior de Administración Electrónica (CSAE), su uso es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España"[24]. Está dirigido a los medios electrónicos, informáticos y telemáticos. El fin de este método es inspeccionar todos los riesgos que llevan los sistemas de información para que se pueda indicar cuales son las medidas adecuadas para un buen control.

[24] **ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012.** https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

Mediante esta tecnología la universidad, tomara conciencia de la existencia de riesgos de la información y su infraestructura y la necesidad de brindar un mejor proceso de gestión de estos recursos, podrá descubrir y generar planes para el tratamiento oportuno para cada riesgo, brindando controles que le facilitara la preparación para procesos de valoración, auditoría y certificación, este proceso le permitirá ser una organización acreditada y con un alto reconocimiento.

8.1 IDENTIFICACIÓN DE ACTIVOS

Para las universidades los activos son los "recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección, definiendo como activo esencial la información"[25] que manejan los diferentes sistemas, esto quiere decir que los

[25] **ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012.** https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-

datos y alrededor de los mismos se puede llevar a una identificación de otros activos que son relevantes y que también integran los Sistemas de Información, estos son los diferentes servicios que son prestados y que hacen parte de esos datos, adicionalmente se mencionan los que necesitan para poder gestionar como son:

- Los sistemas de información desarrolladas por la empresa que permiten el manejo de los datos
- Las redes de datos que permiten el intercambio de información
- Los medios de información que son mecanismos de almacenamiento de datos
- Los dispositivos que complementan el material informático
- Las instalaciones que refugian los equipos informáticos y de comunicaciones
- El personal que explota u operan los elementos del sistema

Tabla 1. Identificación de activos

[S]DATOS / INFORMACIÓN	● [files]Ficheros ● [conf]Datos de configuración ● [int]Datos de gestión interna ● [password]Credenciales ● [auth]Datos de validación de credenciales ● [acl]Datos de control de acceso

14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

	• [log]Registro de actividad
[SW]SOFTWARE	• [os] Diversos Sistemas operativos entre los más utilizados Microsoft Windows 7, 8 10 Professional licenciado (estaciones de trabajo para desarrolladores e integradores). • [wu]Windows Update • [prp]Desarrollo propio • [hypervisor]Gestor de máquinas virtuales

Continuación tabla 1

[SW]SOFTWARE	• [app]Aplicaciones de reporte de horas, plataforma de E-Learning, bases de datos de conocimiento y otros. • [app]Servidor de directorio LDAP
[HW]HARDWARE	• [dbms]Servidor de base de datos contiene: BBDD corporativas y las empleadas por el desarrollo y pruebas. • [app]Servidor de aplicaciones: entorno de desarrollo y pruebas • [app]Mainframe: No existe, se está utilizando los entornos de pruebas para este fin. • [print]Servidor de ficheros e impresión • []Workstations de desarrollo • [app]Servidor proxy + firewall nivel de aplicación • [app]Servidor DNS interno + Host IDS • [app]Servidor DNS externo + Host IDS • [app]Servidor web interno + host IDS • [app]Servidor web externo + host IDS • [pabx]Servidor de acceso remoto telefónico • [email server]Servidor de correo electrónico + host IDS • [network]Network IDS (2) • [firewall]Firewall interno (2) • [firewall]Firewall externo • [firewall]Firewall Zona Wifi
[COM]COMUNICACIONES	• [internet]Acceso internet ISP • [pstn]Red Telefónica básica o RDSI • [wifi]Red WIFI • [lan]Red LAN

	• [internet]Internet • [vpn]Red VPN
[AUX]EQUIPOS AUXILIARES	• [power]Fuentes de alimentación • [ups]Sistemas de alimentación interrumpida • [gen]Generadores eléctricos Diesel • [wire]Cable eléctrico • [fiber]Fibra óptica

Continuación tabla 1

[AUX]EQUIPOS AUXILIARES	• [sei]Sistema de extinción de incendios • [ac]Equipos de climatización
[S]SERVICIOS	• [email]Correo electrónico • [file]Almacenamiento de ficheros • [edi]Intercambio electrónico de datos • [ftp]Transferencia de ficheros • [internet]Internet
[L]INSTALACIONES	• [buildong]Oficinas o delegaciones • [cpd]CPD
[P]PERSONAL	• [ur]Usuarios remotos • [des]Desarrolladores • [adm]Funcionarios para la gestión de infraestructura
[SI]SOPORTES DE INFORMACIÓN	• [san]Almacenamiento en red • [seg]Tarjeta de identificación • [electronic]Electrónicos

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

8.2 VALORACIÓN DE ACTIVOS

El proceso de valoración de activos está definido por los diferentes cambios que se pueden presentar y que impactan de forma negativa a las universidades impidiendo tener un valor estimado inicial, costos de recuperación, configuración, uso de activos, generando pérdidas de oportunidad, el valor que se asigne a cada activo de acuerdo al grado de importancia, además a esto siempre resguardando la disponibilidad, integridad, confidencialidad y disponibilidad de cada uno de ellos.
Además, debe ser lo más objetiva posible, se debería contar con la participación de todas las áreas de la organización para que se involucren en este proceso, aunque no sean las encargadas de realizar el Análisis de riesgos, con esta participación se lograrse obtener un resultado más acertado a la realidad sobre los activos de las organizaciones.

Es por ello que es necesario realizar un proceso de valoración de activos, con miras a identificar las diversas posibilidades cuando es el momento de darle un valor a determinado activo, debido a la actual situación de las instituciones de educación superior del Tolima. Teniendo en cuenta los activos con mayor valor y que los mismos pueden generar riesgos que afecten el correr del negocio, por lo tanto, se definen los siguientes:

Servidores de Bases de Datos: En estos dispositivos se almacenan los datos académicos de toda la comunidad universitaria y también se incluye un proceso sistema de gestión de proyectos, donde también se evidencia que guardan el código fuente correspondiente de los desarrollos propios y software administrativo. Este servidor es esencialmente útil para el funcionamiento académico administrativo de las universidades y su pérdida se vería reflejada en su sistema de seguridad poniendo en riesgo su Autenticidad (A), Confiabilidad (C), Integridad (I), Disponibilidad (D), Trazabilidad del servicio (T) de la información. Adicionalmente no se evidencia un plan de backups o si se maneja un espejo de la información en servidores externos, el desconocimiento del sistema de seguridad que resguarda la información y el acceso físico y lógico a estos servidores, en los cuales reposa el activo más importante. “La Información y el código fuente de los desarrollos”.

Servidores de aplicaciones: Hace referencia al software de gestión académica y administrativa, en el cual se evidencia dos ambientes de desarrollo y pruebas, no se recomienda este tipo de configuraciones en un mismo servidor, esto puede ocasionar que se genere negación en el servicio, por lo tanto, se sugiere que las universidades deben contar con ambientes controlados en servidores apartes para evitar posibles fallas del servicio.

8.3 IDENTIFICACIÓN DE LAS AMENAZAS

Una vez realizado la identificación de activos de las organizaciones, se procede a la identificación de amenazas que pueden afectar a cada activo, este tipo de situaciones son “eventos que pueden desencadenar un incidente en las instituciones, produciendo daños materiales o pérdidas inmediatas en sus activos”[26], relaciono un cuadro de amenazas más comunes a continuación:

La identificación de las amenazas se realiza de acuerdo a la metodología Magerit, las cuales se clasifica en:

Tabla 2. Clasificación de amenazas

[26] españa, G. d. (10 de 2012). *https://www.ccn-cert.cni.es/.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[N] Desastres Naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques intencionados

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 3. Clasificación de Amenazas herramienta PILAR

[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escapes de información
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

[A] Ataques intencionados
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.11] Acceso no autorizado
Continuación tabla 3
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 4. Identificación de las amenazas.

Activos
DATOS / INFORMACIÓN
Ficheros, Datos de configuración, Datos de gestión interna, Credenciales, Datos de control de acceso, Copia de respaldo y Registro de actividad
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
Continuación tabla 4
[A.19] Divulgación de información
[I.8] Fallo de servicios de comunicaciones
SERVICIOS
Internet, Intercambio electrónico de datos, Transferencia de ficheros, Almacenamiento de ficheros y Correo electrónico
[E. 1] Errores de los usuarios
[E.2] Errores del administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.19] Divulgación de información
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[I.8] Fallo de servicios de comunicaciones
SOFTWARE
Sistema operativo Microsoft Windows 7Professional licenciado (estaciones de trabajo para desarrolladores e integradores), Windows Update, Gestor de máquinas virtuales, Desarrollo propio (aplicaciones bancarias) y Aplicaciones corporativas
[I. 5] Avería de origen físico y lógico
[E. 1] Errores de los usuarios

[E.2] Errores del administrador
[E. 8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
Continuación tabla 4
[E.19] Fugas de información
[E. 20] Vulnerabilidades de los programas (software)
[E. 21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A. 7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
HARDWARE
Servidor de base de datos, Servidor de aplicaciones, Servidores Web, Mainframe, Work stations de desarrollo y Firewalls
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[I.*] Desastres industriales
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos

[A.6] Abuso de privilegios de acceso
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Continuación tabla 4
REDES Y COMUNICACIONES
Red LAN , Red de área local 802.1X, Red VPN, Acceso internet ISP y Red Telefónica básica o RDSI
[E.2] Errores del administrador
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
E.19] Fugas de información
E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A. 7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
EQUIPAMIENTO AUXILIAR
Sistemas de alimentación ininterrumpida, Generadores eléctricos Diésel, Cableado, Fibra óptica, Equipos de climatización, Sistema de extinción de incendios
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.25] Robo
[A.26] Ataque destructivo
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética

[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.9] Interrupción de otros servicios y suministros esenciales
[I.11] Emanaciones electromagnéticas
Continuación tabla 4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.25] Pérdida de equipos
SOPORTES DE INFORMACIÓN
Tarjeta de proximidad y código PIN, Electrónicos
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
Continuación tabla 4
[A.19] Divulgación de información
[A.23] Manipulación de los equipos
[A.25] Robo
[A.26] Ataque destructivo
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.10] Degradación de los soportes de almacenamiento de la información
[E. 1] Errores de los usuarios
[E.2] Errores del administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información

[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.25] Pérdida de equipos
INSTALACIONES
Oficinas o delegaciones, CPD
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
Continuación tabla 4
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[A.11] Acceso no autorizado
[A. 7] Uso no previsto
[A.15] Modificación deliberada de la información
[A.19] Divulgación de información
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[N.*] Desastres naturales
[E.18] Destrucción de información
Continuación tabla 4
[E.19] Fugas de información
PERSONAL
Usuarios remotos, desarrolladores, funcionarios para la gestión infraestructura y demás usuarios
[E.7] Deficiencias en la organización
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

8.4 VALORACIÓN DE LAS AMENAZAS

Este paso se desarrolla para evaluar todas las amenazas que se pueden presentar en las diferentes áreas de sistemas, ya sea por las tareas que realizan los usuarios o en los daños que sufren sus activos, ocurridos durante a lo largo del tiempo estimando la frecuencia con la que se presentan dichas vulnerabilidades y el porcentaje de degradación.

- “Evaluar la probabilidad de ocurrencia de cada amenaza correspondiente a cada activo, esta representa la ocurrencia anual de cada cuanto se materializa una amenaza”.[27]

[27] españa, G. d. (10 de 2012). *https://www.ccn-cert.cni.es/.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.

GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017.

https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.
LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.
MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.
MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.
OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..
OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.
PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

- Estimar el grado de degradación el cual determina el posible impacto que este generará al llegar a materializarse.

Teniendo en cuenta lo descrito anteriormente y a partir de su importancia y el papel que representan para el cumplimiento de su actividad, se dispone a identificar y valorar las amenazas que pueden afectar los activos, “por lo que debe presentarse especial atención a aquellos que son críticos en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos”[28].

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

[28] Excellence, I. (21 de 05 de 2015). *ISOTools Excellence*. Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.
CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.
ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.
—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.
GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.
GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.
GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.
GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.
HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.
HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.
Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.
Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.
LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

En la siguiente tabla se exponen valores que permiten identificar y calificar el rango de la amenaza

Tabla 5. Probabilidad de ocurrencia

Alto (A)
Medio (M)

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

Bajo (B)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.htm

Tabla 6. Dimensiones de seguridad

Autenticidad (A)
Confiabilidad (C)
Integridad (I)
Disponibilidad (D)
Trazabilidad del servicio (T)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 7. Escala de rango porcentual Dimensión de Seguridad

Alto (A)
Medio (M)
Bajo (B)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

La posibilidad de que ocurra una amenaza y esta pueda materializarse, según el proceso de identificación, valoración y análisis realizado para las instituciones de educación superior del Tolima, este se realizó de manera general para los activos que posee y sus respectivas amenazas, el proceso de dimensionar la seguridad respectiva va de acuerdo a las afectaciones en las propiedades. Los resultados de las consecuencias y sus respectivos impactos están clasificados en cualitativas y cuantitativas, definidas también como pérdidas económicas y de su información vital en sus procesos académicos, generando desconfianza en las comunidades universitarias.

Tabla 8. Identificación de riesgo

Activo/Amenazas	Probabilidad de Ocurrencia	[A]	[C]	[I]	[D]	[T]
Activos						
DATOS / INFORMACIÓN						
Ficheros, Datos de configuración, Datos de gestión interna, Credenciales, Datos de control de acceso, Copia de respaldo y Registro de actividad						
[E.1] Errores de los usuarios	A		M	A	B	
[E.2] Errores del administrador	B		B	M	A	
Continuación Tabla 8						

Activo/Amenazas	Probabilidad de Ocurrencia	[A]	[C]	[I]	[D]	[T]
Activos						
DATOS / INFORMACIÓN						
Ficheros, Datos de configuración, Datos de gestión interna, Credenciales, Datos de control de acceso, Copia de respaldo y Registro de actividad						
[E.3] Errores de monitorización (log)	B			A		M
[E.4] Errores de configuración	M			A		
[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	B				A	
[E.19] Fugas de información	M		A			
[E.24] Caída del sistema por agotamiento de recursos	M				A	
[A.3] Manipulación de los registros de actividad (log)	B			A		A
[A.4] Manipulación de la configuración	B		A	A	A	
[A.5] Suplantación de la identidad del usuario	B	M	A	B		
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A.11] Acceso no autorizado	B		A	M		
[A.15] Modificación deliberada de la información	M			A		
[A.18] Destrucción de información	B				A	
[A.19] Divulgación de información	M		A			
[I.8] Fallo de servicios de comunicaciones	M				A	
SERVICIOS						
Internet, Intercambio electrónico de datos, Transferencia de ficheros, Almacenamiento de ficheros, Correo electrónico						
[E. 1] Errores de los usuarios	A		M	A	B	
[E.2] Errores del administrador	B		B	M	A	
[E.15] Alteración accidental de la información	A			A		
Continuación tabla 8						
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
E.24] Caída del sistema por agotamiento de recursos	A				A	
[A.5] Suplantación de la identidad del usuario	M	A	A	A		
[A.6] Abuso de privilegios de acceso	M		A	M	B	
[A.11] Acceso no autorizado	B		A	A		
[A.12] Análisis de tráfico	A				A	
[A.14] Interceptación de información (escucha)	A		A			
[A.19] Divulgación de información	M		A			
[A.24] Denegación de servicio	A				A	
[A.25] Robo	M		A		A	
[A.26] Ataque destructivo	B				A	
[I.8] Fallo de servicios de comunicaciones	M				A	
SOFTWARE						
Sistema operativo Microsoft Windows 7Professional licenciado (estaciones de trabajo para desarrolladores e integradores), Windows Update, Gestor de máquinas virtuales, Desarrollo propio (aplicaciones bancarias), Aplicaciones corporativas						

Activo/Amenazas	Probabilidad de Ocurrencia	[A]	[C]	[I]	[D]	[T]
[I. 5] Avería de origen físico y lógico	B				A	
[E. 1] Errores de los usuarios	M		M	A	M	
[E.2] Errores del administrador	B		B	M	A	
[E. 8] Difusión de software dañino	A		B	M	A	
[E.9] Errores de [re-]encaminamiento	B		A			
[E.10] Errores de secuencia	B			A		
[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
[E. 20] Vulnerabilidades de los programas (software)	B		B	A	M	
[E. 21] Errores de mantenimiento / actualización de programas (software)	B			A	M	
[A.5] Suplantación de la identidad del usuario	M	A	M	B		
[A.6] Abuso de privilegios de acceso	M		A	M	M	
[A. 7] Uso no previsto	B		A	B	M	
[A.10] Alteración de secuencia	B		A			
[A.11] Acceso no autorizado	B		A	M		
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.22] Manipulación de programas	M		A	M	B	
HARDWARE						
Servidor de base de datos, Servidor de aplicaciones, Mainframe, Work stations de desarrollo, Firewalls						
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
Continuación Tabla 8						
[I.4] Contaminación electromagnética	B				A	
[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	
[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.11] Emanaciones electromagnéticas	B		A			
[I.*] Desastres industriales	B					
[E.2] Errores del administrador	B		B	M	A	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
E.24] Caída del sistema por agotamiento de recursos	M				A	
[E.25] Pérdida de equipos	B		M		A	
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A. 7] Uso no previsto	B		A	B	M	
[A.11] Acceso no autorizado	B		A	M		
[A.23] Manipulación de los equipos	B		A		M	
[A.24] Denegación de servicio	M				A	
[A.25] Robo	B		M		A	
[A.26] Ataque destructivo	B				A	

Activo/Amenazas	Probabilidad de Ocurrencia	[A]	[C]	[I]	[D]	[T]
Activos						
REDES Y COMUNICACIONES						
Red LAN , Red de área local 802.1X, Red VPN, Acceso internet ISP y Red Telefónica básica o RDSI						
[E.2] Errores del administrador	B		M	M	A	
[E.9] Errores de [re-]encaminamiento	B		A			
[E.10] Errores de secuencia	B			A		
E.19] Fugas de información	M		A			
E.24] Caída del sistema por agotamiento de recursos	A				A	
[A.5] Suplantación de la identidad del usuario	M	M	A	B		
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A. 7] Uso no previsto	M		A	M	A	
[A.9] [Re-]encaminamiento de mensajes	B		A			
[A.10] Alteración de secuencia	B		A			
[A.11] Acceso no autorizado	M		A	M		
[A.12] Análisis de tráfico	A				A	
[A.14] Interceptación de información (escucha)	A		A			
[A.24] Denegación de servicio	A				A	
EQUIPAMIENTO AUXILIAR						
Sistemas de alimentación interrumpida, Generadores eléctricos Diésel, Cableado, Fibra óptica, Equipos de climatización, Sistema de extinción de incendios						
[A. 7] Uso no previsto	M		A	B	M	
[A.11] Acceso no autorizado	M		A	M		
[A.23] Manipulación de los equipos	M		A		M	
[A.25] Robo	B		M		A	
Continuación Tabla 8						
[A.26] Ataque destructivo	B				A	
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	
[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.9] Interrupción de otros servicios y suministros esenciales	M				A	
[I.11] Emanaciones electromagnéticas	B		A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
[E.25] Pérdida de equipos	B		M		A	
SOPORTES DE INFORMACIÓN						
Tarjeta de proximidad y código PIN, Electrónicos y no electrónicos						
[A. 7] Uso no previsto	B		A	B	M	

[A.11] Acceso no autorizado	M		A	M		
Continuación Tabla 8						
Activo/Amenazas	**Probabilidad de Ocurrencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Activos						
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.23] Manipulación de los equipos	M		A		M	
[A.25] Robo	B		M		A	
[A.26] Ataque destructivo	B				A	
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	
[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.10] Degradación de los soportes de almacenamiento de la información	B				A	
[E. 1] Errores de los usuarios	M		M	A	B	
[E.2] Errores del administrador	B		B	M	MA	
[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
[E.25] Pérdida de equipos	B		M		A	
Continuación Tabla 8						
INSTALACIONES						
Oficinas o delegaciones, CPD						
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[A.11] Acceso no autorizado	B		A	M		
[A. 7] Uso no previsto	B		A	M	M	
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.26] Ataque destructivo	B				A	
[A.27] Ocupación enemiga	B		M		A	
[N.*] Desastres naturales	B					
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
PERSONAL						
Usuarios remotos, desarrolladores, funcionarios para la gestión infraestructura y otros						
[E.7] Deficiencias en la organización	M				A	

[E.19] Fugas de información	M		A			
[A.5] Suplantación de la identidad del usuario	M	M	A	M		

Continuación Tabla 8

Activo/Amenazas	**Probabilidad de Ocurrencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Activos						
[A.28] Indisponibilidad del personal	M				A	
[A.29] Extorsión	M		A	M	B	
[A.30] Ingeniería social (picaresca)	M		A	M	B	

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

8.5 RIESGOS POTENCIALES Y RESIDUALES

Una vez realizado el proceso de identificación y la probabilidad de ocurrencia de una amenaza sobre un activo, se puede valorar el impacto potencial en caso de que se presente o materialice, este proceso se realiza con fines de definir mecanismos de prevención, que permitan tener un control en caso de que se lleguen a materializar, esto conlleva a iniciar los mecanismos del plan que permita salvaguardar la información, no obstante se deben definir "los activos esenciales que requieren mayor atención que es donde se centra la información académica junto con los diferentes servicios prestados (datos y servicios). Se debe garantizar que las universidades cuenten con la continuidad del negocio bajo cualquier circunstancia y ofrecer total confianza a los usuarios en cuanto a la confidencialidad, integridad y disponibilidad del servicio"[29].

8.6 PLAN DE TRATAMIENTO DE RIESGO PARA LA WLAN DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL TOLIMA

Las instituciones de educación superior del Tolima en este momento tienen seguridad sobre sus activos, contemplada sobre la protección de las localidades físicas donde están físicamente sus activos de información con una protección lógica a nivel de antivirus o firewall, pero no se perciben las medidas o salvaguardas para cada uno de los activos que hay. Comenzamos el desarrollo de la organización de seguridad para satisfacer las necesidades encontradas por el análisis, organizado con los objetivos, políticas de la organización y estratégicas, estas tareas de gestión de riesgos permiten realizar un plan de seguridad que implantado y operado cumpla con el nivel de riesgos aceptado por las universidades del Tolima y con los objetivos propuestos.

El proceso de tratamiento de riesgos de la seguridad de la información, consiste en una orientación estratégica que requiere el desarrollo de una cultura de carácter

[29] españa, G. d. (10 de 2012). *Portal administracion electronica.* Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

preventivo, seleccionar y aplicar los controles o medidas más adecuadas, de manera que al comprender el significado de los riesgos, se planteen acciones que reduzcan la afectación a la universidad en caso de que se materialicen, con el fin de poder controlar el riesgo y evitar de este modo, daños que perjudiquen las propiedades de la seguridad y afecten de esta manera los activos más importantes de las universidades. Debe garantizar como mínimo:

- El respectivo funcionamiento efectivo y eficiente de los sistemas de información y servicios de las Universidades
- Mecanismos de control internos efectivos y eficientes
- Conformidad con las leyes y reglamentos vigentes según normativa
- Fortalecer y mejorar las salvaguardas existentes
- Implementar nuevos mecanismos de seguridad

Con base en el resultado del análisis de riesgos y con el fin de gestionar el riesgo residual, se proponen acciones de mejora las cuales pueden estar en marcha por medio de planes de acción o de tratamiento del riesgo, con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, Para que sea efectivo, es necesario que "la empresa adopte determinadas medidas y acciones encaminadas a modificar, reducir o eliminar el riesgo, que tienen un costo y debes ser asumido por la misma. Igualmente, si no se toma medidas contra el riesgo la empresa debe enfrentarse a pérdidas importantes que pueden afectar el correr del negocio y su credibilidad con los usuarios"[30].

Primero se realizará un análisis tomado en cuenta, el costo para las universidades de las diferentes medidas que se pudiesen tomar de forma muy efectiva; frente al de evaluar y cuantificar probables pérdidas que originaría de la no aceptación de medidas contra el riesgo. Gracias a las diferentes identificaciones de riesgos, amenazas, vulnerabilidades y criticidad, fue posible seleccionar controles para disminuir el nivel de riesgo desde un enfoque administrativo o que no requiera una inversión alta en tiempo y recursos para que realmente sean implementados, al comparar los resultados; podremos saber si debemos actuar o no ante el riesgo, y en caso de decidir actuar, buscar la medida más adecuada para el tratamiento del riesgo que debe ser el más apropiado de acuerdo a su importancia y relevancia en la actividad de la empresa.

Para esto se puede definir:

- Los riesgos de bajo nivel, pueden ser aceptados por la organización, esto significa que su probabilidad es baja y su impacto es leve lo cual permite a la entidad asumirlo, pudiendo no ser necesaria una acción

[30] Excellence, I. (21 de 05 de 2015). *ISOTools Excellence*. Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

adicional, es decir se encuentra en un nivel que puede aceptarlo sin necesidad de tomar medidas de control y seguimiento.

- Los riesgos de nivel significativo deben ser tratados y controlados siempre, mediante un análisis de costo y beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo y su aceptación o no, responderá a la estrategia de la compañía y a la oportunidad que el riesgo pueda generar.
- Los niveles altos de riesgo y de impacto catastrófico, es aconsejable generar más controles en la actividad que genera el riesgo en la medida que sea posible, con el fin de disminuir el impacto, con ayuda de una cuidadosa administración y gestión, así como de la preparación de planes específicos para administrar y corregir posibles consecuencias.

Con las nuevas generaciones de tecnología las salvaguardas se ven en la obligación de variar con el avance tecnológico:

- Porque surgen nuevas tecnologías
- Porque desaparecen tecnologías antiguas
- Porque se generan nuevos activos informáticos que se deben considerar
- Porque se forman más posibilidades de los atacantes
- Porque se desarrollan nuevos catálogos de salvaguardas disponibles

El catálogo de salvaguardas utilizado por la metodología Magerit, interesa a las empresas que trabajan con sistemas de información, con el fin de tratar información y prestar servicios de los cuales no entra en la selección de paquetes o productos a instalar, pero brindan o establecen protecciones taxonómicas para ordenar y clasificar los diferentes materiales, tecnológicas, organizativas y procedimentales que sean de aplicación en cada momento.

Tabla 9. Protecciones generales u horizontales

Protecciones Generales
IA Identificación y autenticación
AC Control de acceso lógico
ST Segregación de tareas
IR Gestión de incidencias
tools Herramientas de seguridad
tools.AV Herramienta contra código dañino

tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión
.tools.CC Herramienta de chequeo de configuración
Continuación Tabla 9
tools.VA Herramienta de análisis de vulnerabilidades
tools.TM Herramienta de monitorización de tráfico
tools.DLP DLP Herramienta de monitorización de contenidos
tools.LA Herramienta para análisis de logs
tools.HP Honey net / honey pot
tools.SFV Verificación de las funciones de seguridad
VM Gestión de vulnerabilidades H.AU Registro y auditoría

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 10. Protección de los datos / información

Protección de la Información
A Copias de seguridad de los datos (backup)
I Aseguramiento de la integridad
C Cifrado de la información
DS Uso de firmas electrónicas
TS Uso de servicios de fechado electrónico (time stamping)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 11. Protección de las claves criptográficas

Gestión de claves criptográficas
C Gestión de claves de cifra de información
DS Gestión de claves de firma de información
disk Gestión de claves para contenedores criptográficos

:omms Gestión de claves de comunicaciones
509 Gestión de certificados

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 12. Protección de los servicios

Protección de los Servicios
Continuación Tabla12
A Aseguramiento de la disponibilidad
start Aceptación y puesta en operación
SC Se aplican perfiles de seguridad
op Explotación S.CM Gestión de cambios (mejoras y sustituciones)
end Terminación
www Protección de servicios y aplicaciones web
email Protección del correo electrónico
dir Protección del directorio
Continuación Tabla 12
dns Protección del servidor de nombres de dominio (DNS) S.TW Teletrabajo
voip Voz sobre IP

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 13. Protección de las aplicaciones (software)

V Protección de las Aplicaciones Informáticas
V.A Copias de seguridad (backup)
V.start Puesta en producción
V.SC Se aplican perfiles de seguridad
V.op Explotación / Producción
V.CM Cambios (actualizaciones y mantenimiento)
V.end Terminación

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 14. Protección de los equipos (hardware)

HW Protección de los Equipos Informáticos
HW.start Puesta en producción
HW.SC Se aplican perfiles de seguridad
HW.A Aseguramiento de la disponibilidad
HW.op Operación
HW.CM Cambios (actualizaciones y mantenimiento)
HW.end Terminación HW.PCD Informática móvil
HW.print Reproducción de documentos
HW.pabx Protección de la centralita telefónica (PABX)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 15. Protección de las comunicaciones

COM Protección de las Comunicaciones
COM.start Entrada en servicio
COM.SC Se aplican perfiles de seguridad
COM.A Aseguramiento de la disponibilidad
COM.aut Autenticación del canal
COM.I Protección de la integridad de los datos intercambiados
COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op Operación
Continuación Tabla 15
COM.CM Cambios (actualizaciones y mantenimiento)
COM.end Terminación
COM.internet Internet: uso de ? acceso a
COM.wifi Seguridad Wireless (WiFi)
COM.mobile Telefonía móvil COM.DS Segregación de las redes en dominios

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 16. Protección en los puntos de interconexión con otros sistemas

IP Puntos de interconexión conexiones entre zonas de confianza
IP.SPP Sistema de protección perimetral
IP.BS Protección de los equipos de frontera

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 17. Protección de los soportes de información

MP Protección de los Soportes de Información
MP.A Aseguramiento de la disponibilidad

MP.IC Protección criptográfica del contenido

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 18. Protección de los elementos auxiliares

AUX Elementos Auxiliares
AUX.A Aseguramiento de la disponibilidad
AUX.start Instalación
AUX.power Suministro eléctrico
AUX.AC Climatización
AUX.wires Protección del cableado

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 19. Seguridad física – Protección de las instalaciones

L Protección de las Instalaciones
L.design Diseño
L.depth Defensa en profundidad
L.AC Control de los accesos físicos
L.A Aseguramiento de la disponibilidad
L.end Terminación

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 20. Salvaguardas relativas al personal

PS Gestión del Personal
PS.AT Formación y concienciación
PS.A Aseguramiento de la disponibilidad

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Las salvaguardas relativas a las personas, son todas aquellas que hacen referencia al personal que tienen relación con el sistema de información.

Tabla 21. Salvaguardas de tipo organizativo

G Organización
G.RM Gestión de riesgos
G.plan Planificación de la seguridad
G.exam Inspecciones de seguridad

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Las Salvaguardas de tipo organizativo, son aquellas que se refieren al buen gobierno de la seguridad.

Continuidad de operaciones

Tabla 22. Prevención y reacción frente a desastres.

BC Continuidad del negocio
BC.BIA Análisis de impacto (BIA)
BC.DRP Plan de Recuperación de Desastres (DRP)

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Externalización

La frontera entre los servicios ofrecidos en las diferentes empresas es cada vez más flexible entre los servicios de seguridad prestados internamente y los servicios contratados a terceros. Es fundamental que en estos casos se cierren aspectos de relación contractual:

- SLA: nivel de servicio, si la disponibilidad es un valor
- NDA: compromiso de secreto, si la confidencialidad es un valor
- Identificación y calificación del personal encargado
- Procedimientos de escalado y resolución de incidencias
- Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
- Asunción de responsabilidades y penalizaciones por incumplimiento

Tabla 23. Externalización

E Relaciones Externas
E.1 Acuerdos para intercambio de información y software
E.2 Acceso externo
E.3 Servicios proporcionados por otras organizaciones
E.4 Personal subcontratado

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Tabla 24. Adquisición y desarrollo

NEW Adquisición / desarrollo
NEW.S Servicios Adquisición o desarrollo

NEW.SW Aplicaciones: Adquisición o desarrollo
NEW.HW Equipos: Adquisición o desarrollo
NEW.COM Comunicaciones: Adquisición o contratación
NEW.MP Soportes de Información: Adquisición
NEW.C Productos certificados o acreditados

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

9. MECANISMOS DE CONTROL

Dentro de las herramientas a proponer para garantizar un mejor acceso a la información, y que los usuarios en general especialmente la parte académica tengan acceso exclusivo a servicios de índole formativos, propongo las siguientes herramientas que servirán de aporte como diversos mecanismos de acceso seguro y gestión adecuada de redes de datos[31].

Tabla 25. Alternativa 1

Nombre de la Alternativa 1	**Autenticar los usuarios en a la red Wifi ante un servidor de dominio**
Justificación	Las Universidades del Tolima deben implementar controles que permitan el uso adecuado de la red Wifi de las comunidades académicas, para esto debe propender a centralizar la prestación del servicio a sus usuarios misionales los cuales son los estudiantes. Por lo cual la información de estudiantes está almacenada en sistemas de autenticación de distintas plataformas, haciendo necesario la implementación de un servidor de Directorio Activo, el cual permita el agrupamiento de usuarios, dependiendo de sus perfiles, para así poder aplicar políticas de red adecuadas. El servidor de Directorio Activo se puede configurar para que pueda administrar la autenticación de usuarios en los sistemas operativos, y por ende los usuarios de redes Wifi, y que estos usuarios se autentiquen a la red Wifi de forma transparente a la hora de iniciar sección del sistema operativo del cliente (pc del usuario). Directorio Activo tiene múltiples servicio de seguridad y administración de recurso de red, entre ellos, administración de certificados de servidor, autenticación por medio de certificados de usuario, creación de políticas de red, autenticación de equipos, autenticación de usuarios, agrupamiento de usuario y equipos dependiendo de sus perfiles.

[31] **GUTIERREZ, Manuel Suarez.** www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.

Continuación Tabla 25	
Nombre de la Alternativa 2	**Reserva de Direcciones IP**
Justificación	Uno de los problemas que más acrecienta a las Universidades del Tolima es la proliferación dispositivos móviles, en los cuales un solo usuario puede representar hasta tres o más conexiones de red, contando como conexión cada dispositivo con el que el usuario pueda contar, entre ellos PC Portátil, Smartphone, Tablet, entre otros. Causando agotamiento del direccionamiento IP y saturando los puntos de acceso (AP). La reserva de direcciones IP puede ayudar a solventar este inconveniente, pues se puede realizar controles de la cantidad de dispositivos que pueda conectar un usuario a la red, realizando un inventario de dispositivos con su dirección física (MAC) y configurar el servidor dhcp para que asigne siempre la mismas direcciones IP de acuerdo a la dirección MAC, por lo cual solo permitirá conectar la cantidad de dispositivos que se encuentren en el inventario evitando el agotamiento de las direcciones IP, lo cual también se verá reflejado en la disminución de la cantidad de dispositivos conectados en los puntos de acceso (AP).

Fuente: El autor

Tabla 27. Alternativa 3

Nombre de la Alternativa 3	**Servidor RADIUS**
Justificación	Para realizar un control en la seguridad de la red WI-FI de las instituciones, se hace necesario la implementación de un servidor RADIUS que permitirá gestionar el acceso controlado a los servicios de red garantizando la seguridad de la información, para ello se realiza una descripción de dicha herramienta.

Fuente: El autor

Descripción General: Descripción general Instalación y configuración de un servidor RADIUS

Es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una biblioteca BSD para clientes, módulos para soporte de apache, este servidor es modular, para facilitar su administración, y es muy escalable, se resumen con las siglas “AAA” que significan Autenticación, Autorización y Anotación.

Autenticación: Se realiza mediante el servidor de acceso remoto NAS, que sirve como negociador entre el usuario y el servidor RADIUS realizando unas validaciones con las credenciales del usuario para asegurar que sean correctas, incluyendo la comprobación de la dirección de red.

Autorización: el servidor RADIUS mantiene una lista de direcciones de protocolo en Internet e instruye al RAS para asignar al cliente como parte del proceso de autorización, esto con el fin de llevar un control en el intercambio de información, pero para RADIUS el cliente no tiene la necesidad de tener una misma dirección IP se realiza mediante la validación de credenciales y el servidor asigna los recursos de red como dirección IP y otros parámetros y se realiza el control mediante la duración de la sesión.

Anotación: Una vez completado los procesos de autenticación y autorización, el servidor de acceso envía un mensaje de inicio de sesión al servidor RADIUS. Cuando el usuario cierra la sesión, el servidor de acceso envía un mensaje de detención, determinando así el tiempo de cesión y deteniendo los mensajes para cada sesión de usuario. [32]

Tabla 28. Alternativa 4

[32] **CEJA GARCIA, Efrain. 2012.** tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

Nombre de la Alternativa 4	Portal Cautivo
Justificación	Es un sistema que permite la validación de usuarios en redes WI-FI, brindando conexiones reguladas, en dicho sistema se definen dos partes Zona pública y la privada, brindando la posibilidad de crear sistemas separados con el fin de brindar seguridad sobre los servicios siendo así solo accesible mediante la validación del usuario, este sistema se compone de una serie de herramientas colocadas estratégicamente con el fin de generar un sistema de seguridad confiable, por lo tanto en el momento que un usuario decide ingresar, el sistema comprueba que el usuario este autenticado mediante la posesión de tokens en el caso de que no sea válido se direcciona hacia un portal donde se solicitará usuario y contraseña válidos de este modo accedería a los servicios privados de una institución
Nombre de la Alternativa 5	**Sistemas y herramientas criptográficas**
Justificación	Son herramientas destinadas a la protección de la confidencialidad de la información tanto en tránsito como almacenada, permitiendo el cifrado y descifrado de la información mediante técnicas criptográficas, por tal motivo impiden el uso de las mismas por personas no autorizadas, garantizando el intercambio de la información de forma segura a través de medios o sistemas de comunicación inseguros, incorporando mecanismos para detectar modificaciones, cambios o manipulaciones durante su envío o almacenamiento

Fuente: El autor

9.1 CUADRO COMPARATIVO ALTERNATIVAS DE SOLUCION

En este cuadro se debe evidenciar características técnicas para encontrar la mejor solución alcanzable y efectiva para la red WI-FI de la Universidad del Tolima.

Tabla 30. Comparación de alternativas de soluciones

Alternativas de Solución	Características Técnicas	Ventajas	Desventajas
Servidores de Autenticación (Mena Ludeña, 2013)	Un servidor de autenticación es un host que controla quién puede acceder a una red inalámbrica. Los servidores de autenticación vienen en formas diferentes. El software de control de la autenticación puede residir en un servidor de acceso a la red, un router u otro tipo de hardware para controlar el acceso a la red, o algún otro AP de red. Se refiere a la combinación de hardware y software que cumple la función de autenticación.	Los objetivos son la autorización de autenticación, la privacidad y no repudio. La autorización: determina qué datos de un usuario puede tener acceso a la red, si los hubiere. Privacidad: mantiene la información se divulgue a persona no autorizadas. No repudio: es un requisito legal y se refiere al hecho de que el servidor de autenticación puede registrar todos los accesos a la red junto con los datos de identificación, de manera que un	Sus desventajas están relacionadas con el tiempo de respuesta de la operación debido al proceso que realiza. La autenticación se realiza sobre el usuario y contraseña no sobre la identificación real del mismo. Su eficiencia va de acorde a la parametrización y la información que se registra en cada servidor.

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
Servidores de Autenticación (Mena Ludeña, 2013)		usuario no puede repudiar o negar el hecho de que él ha tenido o modificado el dato es cuestión.	
Infraestructura de Clave Pública (PKI) (BOHORQUEZ, CASTILLO GUZMAN, & VARGAS NARANJO, 2013)	La PKI es una combinación de hardware y software, políticas y procedimientos de seguridad. Permite contar con sistemas de autenticación, controles de acceso, confidencialidad y no repudio para las aplicaciones en redes, usando tecnología avanzada, tal como firmas digitales, criptografía y certificados digitales. Existen diferentes herramientas de software PKI, que permiten la administración y generación de certificados digitales, generación de	Autenticación de usuarios, asegurando la identidad y garantizando el acceso a los servicios. Integridad de la información: Se está garantizando que los datos firmados no se van alterar bajo ninguna circunstancia. Integración con las aplicaciones y con el sistema de seguridad, lo que le permite un mejor manejo en toda su infraestructura. Mediante: Comunicaciones entre servidores e internet	A pesar de que es una buena solución, entre sus desventajas tenemos. Problemas relacionados con el Servicio de respuesta en línea. En esta categoría se incluyen problemas de solicitud y respuesta y la configuración del proveedor de revocación. Problemas relacionados con las herramientas del Servicio de respuesta en línea. En esta categoría se incluyen todos los problemas del complemento

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	claves privadas y públicas, firma digital para documentación electrónica, firma de correos electrónicos, servicio de sellado de tiempo, etc..	Correo electrónico Redes privadas virtuales (VPN) Cifrado de documentos Autenticación de documentos Claves seguras Recuperación segura de claves Validación de identidad	Servicio de respuesta en línea y los relacionados con la sincronización de la configuración de revocación
Implementación del Servicio EduRoam	Se basa en infraestructura jerárquica de servidores RADIUS, los cuales están conectados a través de las diferentes redes académicas de alta velocidad a nivel nacional e internacional permitiendo la autenticación con credenciales institucionales a	Permite la autenticación y autorización de usuarios, adicionalmente realiza conteo de sesiones lo cual facilita la elaboración de reportes de conexión. Promueve la visita de investigadores y comunidad académica internacional a	Todos los servidores del nivel jerárquico deben estar conectados para garantizar una conexión de clientes remotos Algunos Sistemas Operativos Windows no cuentan con el protocolo EAP-TTLS nativo por lo que se hace necesario

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	los diferentes miembros de las entidades participantes del proyecto. El software utilizado para proveer las credenciales de identidad a los diferentes usuarios es FreeRadius, gracias a este se gestionan las solicitudes de autenticación y autorización mediante el conjunto de protocolos de red 802.X permitiendo a su vez implementar seguridad mediante protocolo AAA. Finalmente, todos los puntos de acceso deben ser configurados para autenticación mediante servidor RADIUS local en	las instituciones nacionales agilizando el acceso a Internet mediante las credenciales institucionales asignadas en las entidades de origen a cada uno. Los usuarios registrados en las redes nacionales tendrán acceso a internet en las instituciones internacionales La conexión para un usuario será transparente, no requerirá de configuración especializada.	instalar software de terceros para poder autenticarse con el servidor mediante 802.11X La primera configuración de la red en el equipo debe realizarse de manera manual

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	cada institución y debe ser asignado un único identificador de red o SSID denominado “eduroam”		
Redefinición de las zonas Wi-Fi al interior de la Universidad	Concentración de Puntos de Acceso inalámbrico para facilitar el balanceo de carga (usuarios conectados a un mismo equipo). Se plantea un canal con acceso a Internet exclusivo para los usuarios inalámbricos	No requiere inversión adicional en equipos activos en el momento. Se controla la concurrencia de usuarios al ubicarlos en zonas especificas	Se limita la cobertura de las Zonas WiFi existentes. Se requiere la contratación de un canal de datos adicional
Autenticar los usuarios en a la red Wi-Fi ante un servidor de dominio	Administración centralizada desde Directorio activo. Fusiona mediante la organización y creación de departamentos.	Administración centralizada. Interfaz gráfica amigable para facilitar la administración.	Contar con licencia de Windows Server para poder implementar directorio activo. Altos requerimientos

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	Uso de protocolo Radius. Creación automática de certificados de usuario. Uso de protocolo de autenticación EAP, MD5, EAP-TLS, EAP-TTLS, LEAP y PEAP. Escalable, configurar varios servidores interconectados dependiendo de la cantidad de usuarios. Administración de puntos de Acceso	Clasificación de clientes por grupos. Asignación de políticas de red dependiendo del perfil del cliente. Cifrado de datos en el canal de transmisión. Autenticación en la WLAN con el mismo usuario de sistema operativo y de forma automática cuando el usuario inicia sección. Control de usuarios conectado en la red WLAN. Autenticación mediante protocolo Radius y por certificados.	de hardware de servidor. Adquirir licencia de Radius nativo de Windows server.
Reserva direcciones IP	El protocolo DHCP permite la configuración	Administración centralizada, el servido se encarga de la	Mayor carga administrativa para el

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	automática de los nodos de una red. Funciona en un esquema cliente servidor. El servidor realiza la reserva de dirección IP y distribuir al cliente los parámetros necesarios para configuración de su interfaz TCP/IP. El cliente se ejecuta en cada nodo que se desea configurar.	asignación y configuración de las direcciones IP. Se gana seguridad, pues solo asigna dirección IP a los clientes que se encuentre en la base de datos del servidor DHCP, si por cualquier circunstancia un intruso trata de acceder a la red, no se le asigna dirección IP. Permite controlar la cantidad de usuarios que pueden acceder a la red.	administrador de la red. No aplica seguridad de encriptación de datos, desde el cliente hasta el punto de acceso, pues solo se encarga de asignación y control de direcciones IP.
Servidor Radius	Entre las principales características encontramos: Es el responsable de recibir el requerimiento de	Nos permite tener un servicio centralizado en cualquier red. Permite la identificación de	Las plataformas donde Radius es implementado son frecuentemente ilimitadas para soportar

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	conexión del usuario Actúa como servidor proxy para otros sistemas de autenticación. El protocolo Radius tiene las siguientes características: Seguridad Flexibilidad Administración simple Capacidad extensiva de auditoría.	usuarios con facilidad. Fue diseñado para mantener y suplir las necesidades de autenticar, autorizar y mantener un registro de uso. Posibilidad de aplicar restricciones a un usuario/perfil en particular.	protocolos adicionales, esto quiere decir que si se realiza algún cambio al protocolo este debe ser compatible con clientes y servidores ya existentes. Este método no garantiza la confidencialidad de la información transmitida, ya que no cuanta con ningún mecanismo de cifrado.
Portal cautivo	Las interacciones entre el navegador web del usuario y el servidor de autenticación se cifran mediante https evitando la captura de credenciales. Permite el filtrado de paquetes	Control de conexiones a los servicios de red mediante el registro de direcciones físicas (MAC). Informes y estadísticas, registros de conexión, utilización del	Se debe editar las tablas de direcciones en todos los puntos de acceso para dar de baja a un equipo Ataques a direcciones MAC produciendo

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	mediante dirección MAC, IP o por URLs, especificando reglas de bloqueo. No requiere la instalación del lado del cliente, se realiza el enrutamiento de todos los clientes a la pantalla de inicio de sección. Control de información de los usuarios (Datos personales).	servicio, informe de estado de la red. Validación de usuarios, mediante credenciales. Seguridad basada en identidades. No hay lactancia por cifrado. Aplicación de políticas por usuario.	suplantación del usuario Este método no garantiza la confidencialidad de la información transmitida, ya que no cuanta con ningún mecanismo de cifrado Menos segura que otras soluciones siendo necesario la combinación con sistemas de cifrado
Herramientas criptográficas	Nos brindan herramientas para garantizar la seguridad de la información mediante la: Autenticación Integridad	Combinación de software, tecnologías de encriptación y servicios que ofrecen a las empresas u organismos mecanismos para sus comunicaciones	No hay protección contra el robo de claves No hay protección contra ataques de denegación del servicio No se puede evitar el estudio

Continuación Tabla 30			
Alternativas de Solución	**Características Técnicas**	**Ventajas**	**Desventajas**
	Confidencialidad No repudio	y transacciones por internet.	de análisis de tráfico

Fuente: El autor

10 LINEAMIENTOS DE SEGURIDAD MEDIANTE POLÍTICAS Y PROCEDIMIENTOS

Para poder implementar acciones que puedan contrarrestar las fallas de seguridad presentadas, se debe establecer el árbol de estructura organizativa de la empresa, establecer el nivel de importancia de aplicaciones de software dependiendo de su grado de criticidad para la empresa, todo esto para poder crear y establecer políticas que se ajusten a las necesidades de la empresa, para poder instalar y configurar infraestructuras tecnológicas basadas en estas políticas, permitiendo cumplir con los objetivos trazados.

Adquirir un sistema de Gestión de Unificada de Amenazas (UTM), un único equipo que incluye múltiples características de seguridad como: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus y anti spam y redes privadas virtuales; dicha adquisición es muy útil para centralizar las soluciones[33].

Con este cambio de configuración de la arquitectura las instituciones de educación superior del Tolima. Cambia y da soluciones a los problemas planteados

- Se configura el cortafuego segmentado los servicios de web (correo y página web) y la pasarela de antivirus y anti spam en la zona DMZ con política restrictiva.
- Configurar el sistema de detección y prevención de intrusos, tanto para el cliente remoto, la red interna y la zona DMZ, para detectar y prevenir posibles ataques.
- Colocar los servidores de base de datos y de aplicaciones en la red interna inaccesible de internet.
- El punto de acceso al servicio a través de la VLAN (Red de Área Local Virtual)

[33] CATALINA, R. M. (s.f.). *Redes de computadoras*. Obtenido de https://sites.google.com/site/605bredesdecomputadoras/home/7

- Un equipo UTM Firewall contiene diferentes funcionalidades, entre las más comunes están el módulo de Firewall, VPN, Antispam, Antiphishing, Antispyware, Email Security, Filtro de contenidos, detención y prevención de intrusos IDS/IPS.
- Establecer la zona DMZ donde encontraran los servidores publicados, aplicado reglas de acceso y servicios basados en las políticas de seguridad establecidas.
- Configuración adecuada de Routers, ya que son los que tienen contacto directo con una red externa, mediante el uso de reglas ACL (Listas de control de acceso), de tal forma de restringir el flujo de datos mejorando la seguridad en la red.
- Diseño e implementación de una red de datos estructurada segmentada física y lógica, donde se crearán redes virtuales (VLAN) por dependencia y / u oficina, lo cual permite tener administración adecuada, permitiendo la aplicación de reglas de seguridad de red por VLAN, encontrar problemas en la red rápidamente, aislamiento de problemas que se puedan presentar sin afectar la prestación del servicio de las otras VLAN.
- Configuración de servidores PROXY, definición de reglas ACL para controlar el uso que hacen los usuarios de los servicios de internet.
- Instalación y actualización constante de Antivirus, definiendo configuraciones adecuadas para que realmente proteja los equipos.
- Hardening y Tuning a los servidores, Realizar Hardening a los sistemas operativos de los servidores, eliminado aplicaciones y servicios innecesarios, eliminado huecos de seguridad, establecer controles de acceso, implementación de firewall local en cada uno de los servidores, implementación de actualizaciones y parches de seguridad.
- Realizar Tuning permite el afinamiento de los parámetros de comportamiento y configuración para mejorar el rendimiento de los servicios y aplicaciones.

- Implementación Directorio Activo que permite establecer grupos de usuario y grupos de equipos para ser administrados de acuerdo la estructura orgánica de la empresa, permite establecer reglas globales, reglas por grupos de usuario, reglas por grupo de equipos y reglas por usuario o equipo, permite desplegar la instalación de software remotamente en uno o muchos equipos al tiempo, controlar el acceso y uso de aplicaciones, acceso a recurso de red y también se puede usar como una base de datos para la autenticación de usuarios en diferentes aplicaciones compatibles con este servicio.

Aplicación y Control de Políticas: Establecer controles que permitan medir el grado de cumplimiento de la política de seguridad establecidas, para encontrar posibles fallas y así realizar mejoras oportunas que ayuden en el desarrollo de las actividades y procesos de la empresa. Entre las políticas que se pueden implementar están:

- Políticas de Correo Electrónico.
- Políticas de uso de las estaciones de trabajo.
- Políticas de Acceso a aplicaciones.
- Políticas de Instalación y Actualización de Software.
- Políticas de uso de las redes de datos.
- Políticas de uso de Internet.
- Políticas de Instalación y cambio de Equipos.
- Políticas de Cambio de Hardware.
- Políticas de Mantenimiento.
- Políticas de Manejo de Antivirus.

- Políticas Administración y Gestión de Procesos.
- Políticas de Soporte
- Políticas de Desarrollo.
- Políticas de Backups.
- Políticas de Servicios de Outsourcing.

a) Políticas de Seguridad, que se deberían implementar en la empresa para todo el personal que en ella labora.

Una política de seguridad deben ser las declaraciones formales de las reglas que debe mejorar e implementar en las instituciones de educación superior del Tolima. Y deben seguir las personas con acceso a los activos de tecnología e información dentro de la misma. Por otro lado, los procedimientos deben ser detallados de cómo se implantará cada política. El procedimiento incluye todas las actividades requeridas y los roles y responsabilidades de las personas encargadas de llevarlos a cabo y el compromiso de la Directiva en mantener y hacer cumplir dichas políticas. A continuación, se relacionan algunas.

Seguridad del personal vinculado a la empresa:

Orientación para los empleados y/o servicios de terceros nuevos: Cuando se contrate a un empleado nuevo y/o el servicio de algún tercero, se debe de entregar la política de seguridad, así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la empresa. Asimismo, se debe entregar un resumen escrito de las medidas básicas de seguridad de la información. El personal de terceros debe recibir una copia del acuerdo de no divulgación firmado por la empresa y por el proveedor de servicios de terceros, así como orientación con respecto a su responsabilidad en la confidencialidad de la información de la misma.

Capacitación de usuarios: Es responsabilidad del área de seguridad informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y buscar métodos que continuamente le recuerden al usuario su compromiso con la seguridad informática de la empresa. El usuario debe conocer los siguientes aspectos:

- Requerimientos de identificador de usuario y contraseña
- Seguridad de PC, incluyendo protección de virus
- Guías de acceso a Internet
- Guías de uso del correo electrónico, entre otros

b) Recomendaciones técnicas que usted por su experiencia o conocimiento acerca del tema estará dispuesto hacer al personal involucrado en el caso.

El administrador de red debe tener como prioridad la seguridad de su sistema por lo que debe estar continuó conociendo e informándose de las nuevas versiones de los productos instalados y de las nuevas amenazas.

- Los administradores de red deben periódicamente realizar actualización de parches en los productos instalados
- La seguridad informática no es solo del administrador de la red sino todo el usuario final de la empresa por lo tanto debe tener actualizado el antivirus, además existen programas imprescindibles dentro del PC y que deben actualizarse con regularidad. Y revisar su configuración para evitar fallas de seguridad.
- Capacitación continua sobre los delitos informáticos, los controles y el cumplimiento de la política de seguridad.
- Hacer copias de seguridad con frecuencia o backups de los sistemas de la organización
- Instalar software legal (se obtiene garantía y soporte).

- Usar contraseñas fuertes (evitar nombres, fechas, datos conocidos o deducibles, etc.), para hacer contraseñas fuertes se debe usar números, letras, símbolos y combinarlos ejemplo: GilBertJ@ir8314#
- No descargar o ejecutar ficheros desde sitios sospechosos o procedentes de correos que nos conozcamos

Se realiza el siguiente cronograma de actividades a realizar para la adecuada implementación de un SGSI con el cual se pretende realizar la normativa ISO 27001/2013 para el aseguramiento y mejora de sus actividades dividida en 4 fases para llevar a cabo dichos objetivos planteados[34].

Tabla 31. Cronograma actividades SGSI

FASES	DESCRIPCION	ACTIVIDADES	RESPONSABLE	SEMANAS
PRIMERA FASE	Creación del SGSI	Definición del alcance del sistema, revisión del estado inicial de la empresa	Director general Responsable de seguridad	2
		Elaboración, aprobación y distribución de una Política de Seguridad	Director general Responsable de seguridad	2
		Crear una estructura organizativa de la seguridad dentro de la empresa y un comité de seguridad	Director general Responsable de seguridad	1

[34] **EXCELLENCE, ISOTools.** ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

Continuación Tabla 31				
FASES	**DESCRIPCION**	**ACTIVIDADES**	**RESPONSABLE**	**SEMANAS**
PRIMERA FASE	Creación del SGSI	Análisis de riesgos, documentar una metodología de análisis, criterios para valoraciones y evaluaciones.	Director general Responsable de seguridad	2
		Inventario de activos, servicios, información, hardware, software, soporte, instalaciones, personal	Responsable de seguridad Director financiero Director comercial	1
		Identificación de amenazas para cada activo y descripción de vulnerabilidades asociadas a cada amenaza	Responsable de seguridad	1
		Evaluación de la probabilidad de ocurrencia de la amenaza	Responsable de seguridad	1
		Definir nivel de riesgo aceptable por la empresa	Director general Responsable de seguridad	1

Continuación Tabla 31				
FASES	**DESCRIPCION**	**ACTIVIDADES**	**RESPONSABLE**	**SEMANAS**
		Definir plan de tratamiento de los riesgos no aceptados por la empresa	Director general Responsable de seguridad	1
		Elabora primera versión de la declaración de aplicabilidad SOA (Statament of Aplicabilyty), posición de la empresa respecto a la ISO	Director general Responsable de seguridad Comité de seguridad	1
SEGUNDA FASE	HACER SGSI (PDCA)	Implantación plan de tratamiento de riesgos establecidos	Director general Responsable de seguridad Comité de seguridad	1
		Gestión de incidencias, registro de incidencias para facilitar seguimiento y resolución.	Responsable de seguridad	2
		Gestión de soportes, control de entrada y salidas de información en los dispositivos.	Responsable de seguridad	1
		Evaluar la eficiencia de esta implantación, realizar evaluación de la implantación, para monitorear eficiencia.	Responsable de seguridad	1
TERCERA FASE	HACER SGSI (PDCA)	Auditoría interna y revisión del SGSI,	Dirección de la organización	2

Continuación Tabla 31				
FASES	**DESCRIPCION**	**ACTIVIDADES**	**RESPONSABLE**	**SEMANAS**
		revisando puntos 4 y 8 de la norma ISO 27001	Responsable de seguridad	
		Revisión del SGSI, cambios y mejoras del PDCA, según puntos 7.2 de la ISO 27001.	Comité de seguridad	1
CUARTA FASE	MEJORA SGSI (PDCA)	Crear sistema de gestión de no conformidades, acciones correctivas y preventivas.	Responsable de seguridad	1
		Acciones correctivas de las no conformidades	Dirección de la organización Responsable de seguridad	2

Fuente: El autor

11 MECANISMOS DE SENSIBILIDAD PARA EL ACCESO A SERVICIOS DE RED WLAN DE LAS UNIVERSIDADES DEL TOLIMA

Para la elaboración del manual de políticas de seguridad para las universidades se tendrán en consideración los siguientes aspectos:

a. Seguridad del personal

Política: Todo usuario deberá firmar un documento que garantice la confidencialidad de la información manipulada en sus diferentes sistemas de información de las universidades.

Obligaciones: Es obligatorio para todo usuario cumplir con las políticas y normas establecidas por las universidades.

Acuerdos 'de uso y confidencialidad: Todo usuario debe firmar el convenio de aceptación de la confidencialidad y uso adecuado de los sistemas de información de las universidades.

Entrenamiento en seguridad informática: Todo usuario nuevo debe tener una inducción al buen uso de los diferentes sistemas de información, así como las políticas y estándares orientados por la oficina de sistemas donde se dan a conocer las respectivas obligaciones.

- Todos los usuarios serán capacitados en cuestiones de seguridad de la información según las funciones que desarrollen.

Medidas disciplinarias: Cuando el departamento de sistemas identifique el incumplimiento de las políticas de seguridad será reportado o denunciado a la dependencia interna de control para efectos de hacerlas cumplir.

b. Seguridad física

Política: Los mecanismos de control de acceso físico del personal a las diferentes áreas de infraestructura tecnológica deben ser permitidos únicamente a personal autorizado, salvaguardando la integridad de los equipos de cómputo y comunicaciones.

Resguardo y protección de la información: El usuario deberá reportar cualquier tipo de incidente que suceda dentro de la universidad evitando posibles daños tecnológicos y de infraestructura.

- El usuario debe proteger los diferentes medios de respaldo de información que contengan datos importantes o confidenciales personales
- Es responsabilidad del usuario evitar el plagio de información de uso personal que se encuentre en los equipos de cómputo asignado.

Controles de acceso físico: Las personas que pretendan ingresar con algún elemento físico, dispositivos móviles y portátiles, debe ser registrado.

- Se debe regular y controlar el acceso a las áreas de misión crítica de la empresa, data center, evitando el acceso no autorizado.
- Se debe contar con un sistema de credenciales que permita la identificación del personal de las universidades.

Seguridad en áreas de trabajo: las diferentes áreas de las universidades son restringidas y se ingresan a ellas solo personal autorizado.

Protección y ubicación de los equipos: Los usuarios no deben trasladar los equipos de cómputo, de telecomunicaciones, instalar o desinstalar dispositivos sin la autorización previa.

- El área de control de seguridad se encargará de generar el resguardo y recolectar la firma del usuario responsable de los activos informáticos que se le asignen.
- Se deberá realizar capacitaciones a los usuarios de las herramientas informáticas con el fin de evitar riesgos de mal uso.

c. Seguridad y administración de operaciones de cómputo

Política: Los usuarios deberán utilizar los mecanismos necesarios para realizar las copias de seguridad protegiendo la información y garantizando la confidencialidad, deben conocer y aplicar las medidas para la prevención de código malicioso como virus, troyanos y gusanos de red.

Instalación de software: Los usuarios que necesiten realizar instalación de software deben contar con aprobación previa del departamento de seguridad y director del área.

Identificación del incidente: Los usuarios que detecten cualquier situación sospechosa como información importante revelada, modificada, alterada o borrada sin la autorización se debe reportar al área correspondiente.

Administración de la configuración: Los usuarios de las diferentes áreas de la empresa no deben modificar las configuraciones de los equipos sin autorización previa por parte del área encargada.

Seguridad para la red: Será considerado un ataque a la seguridad informática cualquier actividad realizada por un usuario que realice la exploración de los recursos informáticos de la red de las universidades en busca de una posible vulnerabilidad.

Uso de correo electrónico: Los usuarios deben de contar con un correo institucional previamente asignado para el desarrollo de sus actividades y no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas diferentes al correo asignado.

- Los usuarios deben tratar la información enviada por los correos como confidencial y propiedad de las universidades.

- Los usuarios podrán enviar información reservada y confidencial vía correo electrónico siempre y cuando vaya encriptada y destinada exclusivamente a personas autorizadas.
- El usuario debe hacer uso del correo electrónico única y exclusivamente para los recursos que le hayan sido asignados y las facultades que se le hayan sido atribuidas para el desempeño de su empleo o cargo.

Controles contra código malicioso: Para prevenir infecciones por virus los usuarios no deben hacer uso de cualquier clase de software que no haya sido proporcionado por las universidades.

- Los usuarios deben verificar que la información almacenada en los diferentes medios de respaldo y en equipos de trabajo estén libres de código malicioso, ejecutando el antivirus de la organización.
- Todos los archivos provenientes de fuentes internas o externas deben ser verificados que estén libres de virus utilizando el antivirus autorizado.
- Cualquier usuario que tenga sospechas de virus deberá dejar de usar inmediatamente el equipo y llamar al área encargada para la eliminación del mismo.

Internet: el acceso a internet provisto por las universidades es de uso exclusivo a actividades académicas

- Todos los accesos a internet tienen que ser realizados a través de los canales de las redes de las universidades.
- Prohibición al acceso a páginas no autorizadas

d. Controles de acceso lógico

Política: El coordinador del área de sistemas proporcionará toda la documentación necesaria y accesoria para la utilización de los sistemas de información de las universidades, así como los roles y funcionalidades correspondientes, también

asignará identificador de usuario y contraseñas necesarios para acceder a la información y a la infraestructura tecnológica.

Administración de privilegios: Cualquier cambio de los roles y responsabilidades de los usuarios deben ser solicitados al área de seguridad de las universidades.

Administración y uso de contraseñas: La asignación de contraseña se debe realizar de forma individual y no se debe compartir.

- Cuando un usuario olvide, bloquee o extravíe su clave, deberá levantar una solicitud haciendo uso de los formatos de calidad de las universidades, para que sea generado y luego ser cambiado por el usuario.
- Se prohíbe dejar las contraseñas visibles o escritas en lugares que pueden ser descubiertos por personal no autorizado.
- Sin importar las circunstancias las claves no se deben compartir es responsabilidad del usuario mantener confidencialidad.

Para la asignación y construcción de contraseñas se deben de tener en cuenta las siguientes características:

- Las contraseñas deben de tener una longitud segura entre 6 a 10 caracteres, dichos caracteres deben de ser alfanuméricos
- Las contraseñas deben ser difíciles de adivinar y no estar asociadas a la vida personal o trabajo del usuario.
- Se debe cambiar periódicamente.
- Las contraseñas no se deben almacenar en ningún programa que facilite recordarlo.

12. CONCLUSIONES

Se recomienda la utilización de la metodología MAGERIT V.3, en el análisis de gestión de riesgos con el fin de generar una serie de mecanismos que permitan salvaguardar la información garantizando la disponibilidad, integridad y confidencialidad de la información.

Se recomienda que la administración tome en cuenta estándares como ISO/IEC 27002:005 código de buenas prácticas para la gestión de la seguridad de la información, COBIT e ITIL (mejores prácticas de prestación de servicios YI u auditoría) y cisco (estándares internacionales de redes y telecomunicaciones).

Se recomienda que este proceso de análisis y gestión de riesgos de las redes WLAN, se hagan por lo menos, una vez cada año, esto con el fin de conocer sus fortalezas o debilidades e implementar salvaguardas para reducir las debilidades encontradas, y que estén acordes al avance tecnológico.

Después de realizar este proyecto, las Universidades obtendrán un documento encaminado a la seguridad en la red WLAN que será un punto de partida para la creación de normativas de seguridad.

Implantación de un Sistema de Gestión de la Seguridad de la Información, aplicando la normativa ISO 27001, esta norma ayuda a gestionar y proteger los valiosos activos de información, garantizando la selección de controles de seguridad adecuados y proporcionales.

Las métricas de seguridad nos permiten tomar decisiones sobre la red de datos, con el fin de solucionar problemas de seguridad que pueden afectar el servicio

La importancia de implementar políticas de seguridad que permitan contrarrestar las diferentes situaciones que comprometen la integridad, disponibilidad y confidencialidad de la información

El compromiso de los trabajadores conservando una ética profesional que vaya acorde a las necesidades de la empresa con el fin de lograr los objetivos propuestos, misión y visión

Las Universidades del Tolima requiere mejorar los niveles de seguridad de su red WiFi, debido a que actualmente es de libre acceso, lo que posibilita la realización de ataques del tipo sniffer y spoofing por usuarios que se conectan a la red y

ejecutan herramientas de análisis de paquetes y escalamiento de privilegios mediante suplantación de identidad.

El problema de las Universidades del Tolima puede ser controlado con herramientas de aseguramiento y estandarización, como lo son los protocolos AAA (Authentication, Authorization and Accounting).

13. RECOMENDACIONES

Se recomienda que haya una revisión periódica de las amenazas y riesgos y que la tecnología está cambiando constantemente y deben ser controlados para futuros problemas.

Se recomienda que todas las conexiones deban pasar a través de los cortafuegos con el fin de prevenir el uso y el acceso de usuarios no autorizados.

Se recomiendan mecanismos de cifrado que permitan controlar los riesgos, para que las transacciones en la WLAN se realicen con total confianza y garantía.

Se recomienda realizar un proceso de auditoría interna para identificar las posibles vulnerabilidades

Se recomienda establecer un plan de recuperación ante posibles desastres

Se recomienda instalar un sistema de monitorización de ciberseguridad y alerta de servidores

BIBLIOGRAFÍA

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. (En línea) 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.

GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.

GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.

HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.

HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.

Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.

Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.
LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.

LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones.

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.

SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.

tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

ANEXOS

Anexo A Formato RAE

Fecha de Realización: 24/07/2021
Título: ANÁLISIS DE RIESGOS BASADO EN LA NORMA MAGERIT V3 DE LA RED WLAN DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL TOLIMA
Autor: ORTIZ ARISTIZABAL AMPARO
Palabras Claves: MAGERIT V3, Seguridad de la Información, Activos, amenazas, riesgo, análisis de riesgos, salvaguardas, controles,
Descripción: El presente trabajo de grado tiene como objetivo la implementación de la "Planificación de un sistema de Información" (PSI) ya que en el caso contrario las organizaciones pueden enfrentar problemas judiciales, desprestigio y falta de credibilidad, al no garantizar las condiciones para el correcto funcionamiento. Se debe optimizar el trabajo de los empleados y a su vez garantizar la seguridad e integridad de lo que circula en la red, pues se trata de información sensible y de vital importancia para las instituciones de educación superior del Tolima que serán el objeto de estudio de este proyecto. Las redes WLAN son sistemas de comunicaciones de datos inalámbricos, que se constituyen como una alternativa a las redes de área local por medio de cable, o también como complemento a estas, utilizando la radiofrecuencia para transmitir y recibir datos, mediante el uso de ondas electromagnéticas. Esto genera mayor movilidad a los usuarios" y su uso se puede realizar desde diferentes tipos de dispositivos. Para lograr óptimas condiciones de seguridad en las instituciones de educación superior del Tolima, el presente proyecto radica y hace importante la implementación de una auditoría de seguridad (análisis de riesgos) en las redes WLAN, puesto que: El inconveniente más importante que supone el uso de este tipo de redes es el tema de la seguridad. Al ser el aire el medio de propagación empleado por las ondas, hace que la información esté expuesta a sufrir ataques. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz de sus comienzos" Aplicando la tercera "versión de la metodología de análisis y gestión de riesgos de los sistemas de información (Magerit v.3)" , se busca trazar un protocolo que permita el uso más eficiente y seguro de esta red de información interna dentro de las instituciones de educación superior.
Fuentes:

ADMINISTRACIONES, MINISTERIO DE HACIENDA Y. 2012. https://www.ccn-cert.cni.es/. [En línea] 10 de 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

AUTOR, DIRECCION NACIONAL DE DERECHO DE. 2013. http://derechodeautor.gov.co/. [En línea] 14 de 02 de 2013. http://derechodeautor.gov.co:8080/gl/decretos1?p_p_id=110_INSTANCE_McZZQV5PKQZ8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_110_INSTANCE_McZZQV5PKQZ8_struts_action=%2Fdocument_library_display%2Fview_file_entry&_110_.

BLACUTT, Roberto Vargas. 2009. https://repositorio.umsa.bo/. [En línea] 2009. https://repositorio.umsa.bo/bitstream/handle/123456789/1256/T-1854.pdf?sequence=1&isAllowed=y.

CÁRDENAS HERNÁNDEZ, Andrés y CASTAÑEDA MONTES, Daniel Hernan. 2018. http://polux.unipiloto.edu.co/. [En línea] 2018. http://polux.unipiloto.edu.co:8080/00004467.pdf.

CARREÑO GARCIA, Nayibe y ALFONSO SARMIENTO, Maria Camila. 2020. https://repository.ucc.edu.co/. [En línea] 2020. https://repository.ucc.edu.co/bitstream/20.500.12494/33982/2/2020_Analisis_seguridad_red.pdf.

CEJA GARCIA, Efrain. 2012. tesis.ipn.mx. [En línea] 10 de 2012. https://tesis.ipn.mx/jspui/bitstream/123456789/16022/1/228%20-%20Fosf..pdf.

CERVERA, Rafael Calduch. https://www.ucm.es/. [En línea] https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf.

ESPAÑA, GOBIERNO DE. 2012. Portal administracion electronica. [En línea] 10 de 2012. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

EXCELLENCE, ISOTools. 2015. ISOTools Excellence. [En línea] 21 de 05 de 2015. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

—. ISOTools EXCELLENCE. [En línea] https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

GANTIVA HENAO, Luis Alexander. http://repository.unipiloto.edu.co/. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y.

GAONA VASQUEZ, Karina del rocio. 2013. https://dspace.ups.edu.ec/. [En línea] 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

GARCÍA HERNÁNDEZ, David Alejandro y RUIZ MURILLO Jeisson Herley. 2017. https://repository.udistrital.edu.co/. [En línea] 2017. https://repository.udistrital.edu.co/bitstream/handle/11349/6813/Documento%20Proyecto%20Grado.pdf?sequence=1.

GUTIERREZ, Manuel Suarez. www.uv.mx/. [En línea] https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf.

HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA Lucio Pilar. https://www.uv.mx/. [En línea] https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf.

HUMANAS, ESCUELA DE CIENCIAS. urosario.edu.co. [En línea] https://www.urosario.edu.co/urosario_files/PortalUrosario/94/94ea1ea8-a218-4702-aea7-bf6c4277fe45.pdf.

Informatica, Oficina de Seguridad para las Redes. instituciones.sld.cu. [En línea] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf?cv=1.

Informatica, Oficina de Sistemas e. 2020. esap.edu.co. [En línea] 2020. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf.

LÓPEZ, Gustavo. IMF Blog de Tecnologia. [En línea] https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/.

LUACES NOVOA, Jose Manuel. 2018. http://openaccess.uoc.edu/. [En línea] 16 de 10 de 2018. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf.

LUGO LUNA, John Freddy. 2017. repository.unad.edu.co. [En línea] 2017. https://repository.unad.edu.co/bitstream/handle/10596/17497/93237039.pdf?sequence=1&isAllowed=y.

MinEducacion. 2019. https://www.mineducacion.gov.co/. [En línea] 15 de 07 de 2019. https://www.mineducacion.gov.co/1759/w3-article-231240.html?_noredirect=1.

MINTIC. https://www.mintic.gov.co/. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

OJEDA-PÉREZ, Jorge Eliécer, RINCÓN-RODRÍGUEZ, Fernando y ARIAS-FLÓREZ, Miguel Eugenio y DAZA-MARTÍNEZ Libardo Alberto. 2010. SciELO. [En línea] 12 de 2010. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003#:~:text=La%20Ley%201273%20de%202009%20complementa%20el%20C%C3%B3digo%20Penal%20y,la%20informaci%C3%B3n%20y%20las%20comunicaciones..

OTOYA VERÁSTEGUI, Melitón Ricardo. 2018. Universidad cesar vallejo. [En línea] 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/16120.

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMbA, Mildred. 2014. repositorio unad.edu.co. [En línea] 2014. https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf;jsessionid=005E50D48087FD77F9480882DA5053AC.jvm1?sequence=3.

PIZARRO, Rodrigo Herrero. 2010. core.ac.uk. [En línea] 05 de 2010. https://core.ac.uk/download/pdf/30043589.pdf.

RAMÍREZ, Manuel y POLANCO, Carlos y FARÍAS, Bernardo. http://profesores.elo.utfsm.cl/. [En línea] http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf.

SALINAS, Adriana Paredes. 2018. https://repository.unad.edu.co/. [En línea] 2018. https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y.
SOLARTE, Francisco Nicolás. 2003. SCRIBD. [En línea] 17 de 04 de 2003. https://es.scribd.com/presentation/411834642/Presentacion-Metodologia-de-La-Investigacion.
tdx.cat. www.tdx.cat. [En línea] https://www.tdx.cat/bitstream/handle/10803/6219/05Capitulo3.PDF?sequence=5&isAllowed=y.

Contenido del documento:

El desarrollo de este trabajo consta de:

Formulación del problema

Se plantea un interrogante ¿Cómo el análisis de riesgos basado en la norma MAGERIT V3, ayudará a mejorar la seguridad y control de acceso a la red WLAN en las instituciones de educación superior del Tolima?

Objetivo general
Analizar los riesgos y salvaguardas que se presentan en el control de acceso a las redes WLAN de las instituciones de educación superior del Tolima

Objetivos específicos

● Identificar los activos informáticos, las vulnerabilidades, amenazas y riesgos de la red WLAN de las instituciones de educación superior del Tolima

● Sugerir los respectivos controles o salvaguardas necesarios para la seguridad y el control de acceso a las redes WLAN en las instituciones de educación superior del Tolima.

● Proveer lineamientos de seguridad mediante políticas y procedimientos que incluyen los controles de acceso a la red WLAN en las instituciones de educación superior del Tolima.

● Establecer mecanismos de sensibilización para el personal sobre temas de seguridad de la información

Marco Referencial: se divide en: Marco Conceptual, Marco teórico, Marco Histórico y Marco legal.
Diseño Metodológico: Es la fase donde se encuentra los ítems del desarrollo del proyecto, Se plantea un proceso de revisión, que pretende determinar las falencias de las redes WLAN de las instituciones de educación superior del

Tolima, realizando una auditoría y pensando en la seguridad y protección de los datos como un componente fundamental dentro de un plan de administración y gestión importante, lo que conlleva en un futuro a tener más cuidado y seguimiento con la seguridad de sus redes. Realizando la implementación a mediano y largo plazo de cualquiera de los aspectos adicionales exigidos en el modelo MAGERIT para alcanzar un mayor nivel de seguridad.

Desarrollo del proyecto: En esta fase se muestra la implementación a mediano y largo plazo de cualquiera de los aspectos adicionales exigidos en el modelo MAGERIT para alcanzar un mayor nivel de seguridad.

Resultados: En esta fase se mostrará los resultados obtenidos con desarrollo del proyecto.

Conclusiones

Bibliografía

Anexos

Metodología:

El desarrollo de este proyecto se llevó a cabo de acuerdo a las siguientes fases:

1. Identificar los activos a la fecha de las instituciones de educación superior del Tolima mediante inventarios físicos y lógicos.
2. Comprobar el rendimiento del hardware de redes mediante test.
3. Comprobar las garantías actuales que ofrece el hardware utilizado para almacenaje y procesamiento de información.
4. Analizar la disposición de los anchos de banda y comprobarlos en las redes tanto de uso externo como interno en las universidades.
5. Caracterizar los aplicativos de software actuales utilizados en las universidades y que interactúan con las redes.
6. Identificar los niveles actuales de seguridad de acceso a las redes, la disposición de permisos y privilegios de aplicativos.
7. Hacer pruebas a las salvaguardas actuales del sistema de procesamiento de información.
8. Realizar pruebas mediante software especializado a los controles propuestos según los resultados de las pruebas anteriores.
9. Seguir de cerca el rendimiento de los procedimientos manuales efectuados tanto por el personal como por la comunidad estudiantil.
10. Establecer la aplicación de medidas que mejoren el rendimiento manual sin afectar la productividad.
11. Implementación a mediano y largo plazo de cualquiera de los aspectos adicionales exigidos en el modelo MAGERIT para alcanzar un mayor nivel de seguridad.
12. Preparación y capacitación del personal en seguridad informática y disposiciones derivadas del resultado del presente análisis.
13. Organización y ejecución de controles para realizar auditorías constantes que garanticen seguridad en las redes a largo plazo.

Conceptos nuevos: AAA (Authentication, Authorization and Accounting). sniffer y spoofing.

Conclusiones: Se recomienda la utilización de la metodología MAGERIT V.3, en el análisis de gestión de riesgos con el fin de generar una serie de mecanismos que permitan salvaguardar la información garantizando la disponibilidad, integridad y confidencialidad de la información.

Se recomienda que la administración tome en cuenta estándares como ISO/IEC 27002:005 código de buenas prácticas para la gestión de la seguridad de la información, COBIT e ITIL (mejores prácticas de prestación de servicios YI u auditoría) y cisco (estándares internacionales de redes y telecomunicaciones).

Se recomienda que este proceso de análisis y gestión de riesgos de las redes WLAN, se hagan por lo menos, una vez cada año, esto con el fin de conocer sus fortalezas o debilidades e implementar salvaguardas para reducir las debilidades encontradas, y que estén acordes al avance tecnológico.

Después de realizar este proyecto, las Universidades obtendrán un documento encaminado a la seguridad en la red WLAN que será un punto de partida para la creación de normativas de seguridad.

AUTOR: AMPARO ORTIZ ARISTIZABAL