Elva Gioconda Lara Guijarro
Edgar Fermín Castañeda Guijarro
José Luis Medina Balseca

Modelo de seguridad de la información, basado en OSSTMMv3, NIST SP 800-30 E ISO 27001, para centros de educación

compAS
Grupo de capacitación e investigación pedagógica
UNIVERSIDAD DE ORIENTE

Modelo de seguridad de la información, basado en OSSTMMv3, NIST SP 800-30 E ISO 27001, para centros de educación

Autores:

Elva Gioconda Lara Guijarro
Edgar Fermín Castañeda Guijarro
José Luis Medina Balseca

Universidad Internacional SEK

Modelo de seguridad de la información,
basado en OSSTMMv3, NIST SP 800-30 E ISO 27001,
para centros de educación

Autores.

Elva Gioconda Lara Guijarro
Edgar Fermín Castañeda Guijarro
José Luis Medina Balseca

Primera edición: junio 2019

ISBN: 978-9942-33-126-7
Diseño de portada y diagramación: Grupo Compás

Este texto ha sido sometido a un proceso de evaluación por pares externos con base en la normativa del editorial.

Guayaquil-Ecuador 2019

Cita.
E. Lara, E. Castañeda, J. Medina (2019) Modelo de seguridad de la información, basado en OSSTMMv3, NIST SP 800-30 E ISO 27001, para centros de educación, Editorial Grupo Compás, Guayaquil Ecuador, 92 pag

Contenido

PRÓLOGO

En la actualidad existen diferentes modelos de seguridad de la información que pueden ser utilizados por instituciones o empresas, éstos sirven para precautelar la información delicada de personas ajenas que quieran apoderarse de estos datos y hacer un uso indebido o sacar ganancia de los mismos. El objetivo del presente trabajo es determinar las mejores políticas de seguridad que serán utilizadas de acuerdo a la necesidad de la institución, tomando en cuenta que no todas tienen las mismas necesidades para el envío de la información dentro de su red de datos.

La falta de un modelo de seguridad de la información en las instituciones de educación superior, implica que actualmente la gestión de los datos esté expuesta a diferentes incidentes o vulnerabilidades. Por ello requiere de un modelo de gestión de tecnología que adopte a la seguridad de la información como componente principal, a fin de controlar todos los procesos de la institución.

Este libro trata de proporcionar un modelo de seguridad de la información para instituciones, basado en los modelos de seguridad de la información, como son: OSSTMMv3 (Open Source Security Testing Methodology Manual versión 3), NIST 800-30 (National Institute of Standards and Technology) y el estándar ISO 27001. Consta de varios protocolos, estándares o normas que son utilizados en redes de datos para dar seguridad acorde a las necesidades de las instituciones, tomando en cuenta que no todos los institutos superiores tienen los mismos dispositivos de red en sus instalaciones. El modelo cubre las políticas de seguridad e implementación de controles, identificación de activos y evaluación del plan de seguridad.

El estudio realizado demostró que un modelo de seguridad es la presentación formal de un estándar, que conlleva un conjunto de reglas y prácticas que regulan cómo se maneja, protege y distribuye la información de una institución, especialmente los datos delicados. Se extrajo las mejores prácticas de implementación de seguridad de los modelos tradicionales.

Del trabajo realizado se pudo concluir que por lo general existe un manejo inadecuado en las instituciones en: dar restricciones en sitios web que son utilizados por los diferentes usuarios, las contraseñas no son actualizadas periódicamente, incidentes con la información académica de los estudiantes. Estos parámetros hacen que una red sea insegura y no resista a un ataque planificado. El libro se encuentra estructurado en tres partes:

- **Capítulo I: Introducción,** incluye temas abordados para la seguridad de una red como son vulnerabilidades o riesgos de la información, gestión de la información, seguridad de la información, entre otros.
- **Capítulo II: Modelos y gestores de seguridad,** trata sobre los gestores de seguridad, explicando en cada uno de ellos sus partes principales y los estándares que utilizan para dar seguridad a las diferentes partes de una red de información. Se hace énfasis en los 3 modelos que son base de este libro.
- **Capítulo III: Modelo de seguridad de la información, basado en OSSTMMv3, NIST SP 800-30 E ISO 27001, para Centros de Educación,** aquí se explica cada uno de los estándares que son utilizados en los diferentes puntos de la red de datos, acorde a la matriz de riesgo obtenida de la institución.

CAPÍTULO 1
INTRODUCCIÓN A LA SEGURIDAD DE LOS DATOS

1.1. Introducción

Toda organización que disponga de una infraestructura tecnológica adoptada, producto del constante cambio tecnológico en el desarrollo de sus actividades, debe estar consciente de los riesgos que implica no contar con procesos adecuados de seguridad. Esto conlleva una mayor responsabilidad en los centros educativos, ya que la información manejada por ellos, son de propiedad de los estudiantes, según el principio de habeas corpus contemplado en la legislación ecuatoriana, es decir, la Universidad es responsable del acceso no autorizado a los datos de los estudiantes, con todos los posibles usos indebidos que se hagan de ellos. Además, está el aspecto de la incomodidad que se genera en los usuarios de un sistema informático que ha sido objeto de un ciber ataque, pues deben lidiar con problemas como retraso en el acceso a la red, pérdida o alteración de datos, proliferación de virus informáticos y malware.

En la tabla 1 se puede visualizar el porcentaje de ataques por usuario conectado, en algunos países de América Latina y Centroamérica según el estudio realizado por la BBC en el año 2016.

Tabla 1: Porcentaje de ataques por usuario conectado

Intentos de ataque por usuarios conectados	
País	**Porcentaje**
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

Fuente: (BBC, 2016)

En un entorno real, la BBC ha publicado un reporte en el que informa

que América Latina y Centroamérica registraron un promedio de 12 ataques informáticos por segundo en septiembre de 2016. De acuerdo a esta información Ecuador ocupa el octavo lugar con el 36,1% de intentos de ataque por usuario conectado.

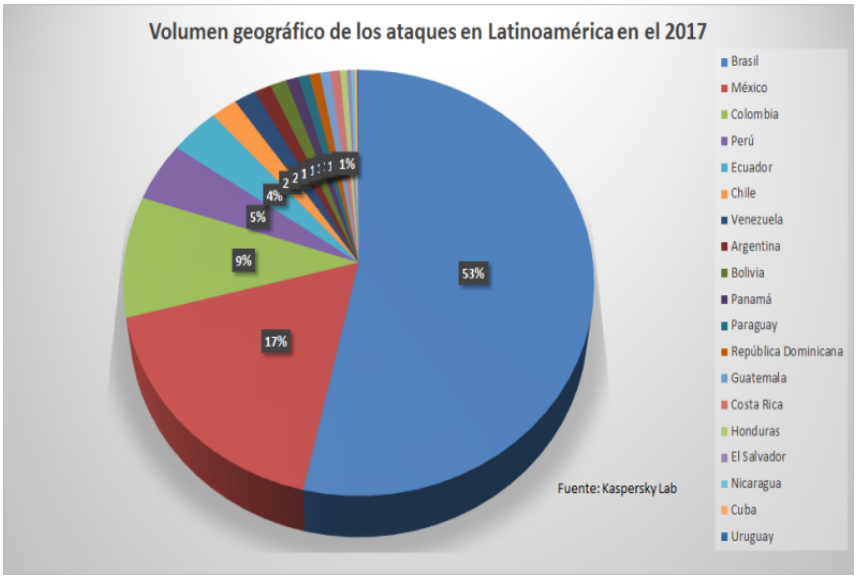


Figura 1: Países de Latinoamérica vs ataques informáticos
Fuente: (Kaspersky, 2018)

Según Kaspersky Lab., en septiembre de 2017 la misma región registró un promedio de 33 ataques por segundo, ubicándose el Ecuador en el quinto lugar entre los países que más ataques han sufrido, como puede apreciar en la Figura 1.

Se puede decir, que las redes de información del país se encuentran permanentemente expuestas a diversos ataques informáticos, lo que supone un riesgo para la seguridad de los datos que se encuentran almacenados en dispositivos conectados a dicha red, con todos los problemas relacionados con el envío y manipulación de los datos en una red de información.

Según datos proporcionados por el Centro de respuestas a incidentes informáticos del Ecuador (EcuCERT), la pérdida de información u otros casos de delitos cibernéticos se ocasionan principalmente porque algún dispositivo (computador, router, servidores) o sistemas informáticos

presentan algún tipo de vulnerabilidad que puede ser aprovechada por el atacante.

De acuerdo a otros datos proporcionados por el EcuCERT, los mayores niveles de vulnerabilidades se encuentran a nivel institucional, incluidas las universidades del país, por ello es sumamente necesario tomar medidas de prevención y mantener asegurados los diferentes dispositivos de red con los cuales opere cualquier institución. (CSIRT, 2016)

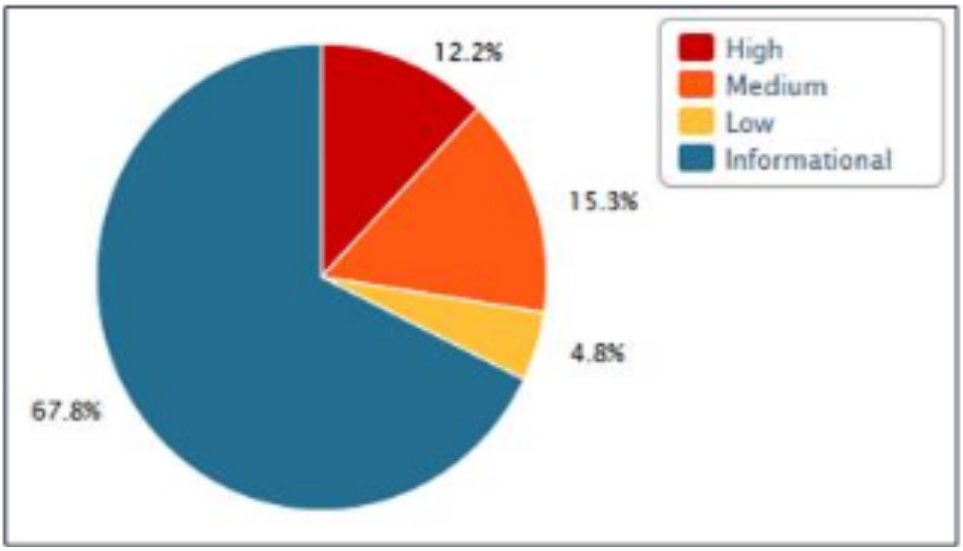


Figura 2: Índice de vulnerabilidades a nivel institucional en el Ecuador
Fuente: (Lindao & Alexander, 2017)

1.2. Seguridad de datos en establecimientos de educación

De manera general, un riesgo de seguridad de información, es la exposición de una organización, a sufrir un ataque a su sistema de gestión de la información. El tema de la seguridad de la información ha sido afrontado seriamente en el ámbito empresarial, teniéndose abundante bibliografía acerca de las diferentes técnicas para proporcionar seguridad a las redes de información. (Molina, Meneses, & Silgado, 2009)

En el ámbito académico, específicamente en el universitario, se ha extendido el uso de redes de datos para la gestión de las actividades docentes y administrativas. Desde un punto de vista general, la universidad puede verse como una empresa que utiliza redes de información para el

desarrollo de sus actividades, por lo que está expuesta a las mismas amenazas que cualquier otra organización. Sin embargo, existe poca bibliografía que aborde el tema de la seguridad de la información, específicamente enfocado a universidades. La mayoría de trabajo al respecto, en el Ecuador, son a nivel de proyectos de grado de tercer nivel, como por ejemplo el trabajo de (Guagalango Vega & Moscoso Montalvo, 2011) que trata sobre la evaluación de la seguridad en el data center de una recinto universitario.

En Ecuador desde el 2012 se implementó el Centro de Respuestas a Incidentes Informáticos del Ecuador (CERT - Computer Emergency Response 29 Team o CSIRT - Computer Security Incident Response Team), para proteger a los ecuatorianos cuando navegan por internet. El objetivo del mismo es proveer servicios y apoyo a una circunscripción definida para prevenir, manejar y responder a incidentes de seguridad informática. (CERT, 2007). En la Figura 3 se puede ver el informe de vulnerabilidades en redes de información desde 1995 hasta el 2007, según CERT.

Figura 3: Informe de vulnerabilidades reportadas por CERT
Fuente: (CERT, 2007)

Según CSIT, en el 2017 se ha mantenido estable el número de alertas procesadas, a pesar de haber incrementado los tipos de alertas que se procesa se ha bajado el total de alertas de 991162 en el 2016 a 39097 en 2017.

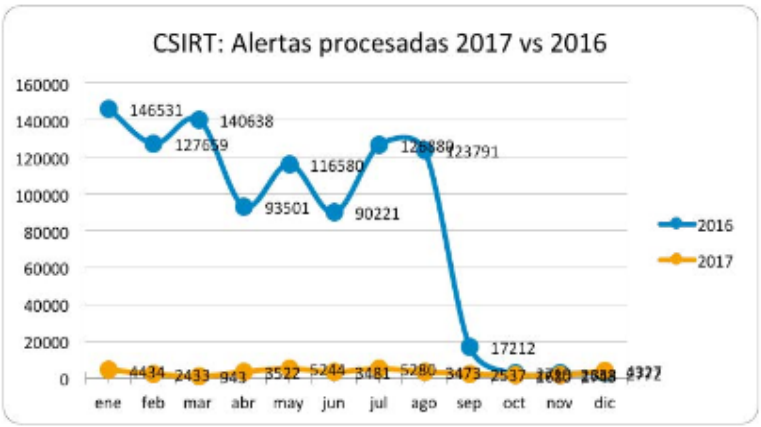


Figura 4: Alertas procesadas en CSIRT
Fuente: (CEDIA, 2017)

Otro centro responsable de la ciberseguridad en Ecuador es el EcuCERT: Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (EcuCERT). Actualmente, este es el organismo encargado de la seguridad de las redes de telecomunicaciones de todo el país, así como del uso de la red de internet. También, coopera con otros equipos CSIRT dentro y fuera del Ecuador. Actualmente EcuCERT maneja 4 redes: una red es ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), otra red que es para uso interno de EcuCERT en la cual se gestionan y se da seguimiento a los incidentes; la tercera es una red de laboratorio, para analizar los incidentes por medio de un Sandbox, y por último una red forense que usan para análisis. En la figura 5, se puede ver varios incidentes a nivel nacional que fueron reportados por el Centro de Respuestas a Incidentes Informáticos del Ecuador EcuCERT en el 2017.

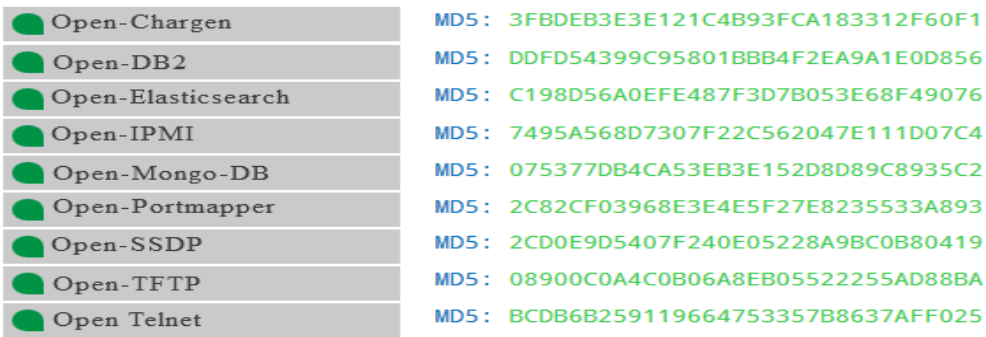


Figura 5: Incidentes reportados por EcuCERT
Fuente: (EcuCERT, 2017)

En lengua inglesa, se tienen varios artículos de investigación que tratan el tema desde una perspectiva más general, llegándose a proponer la implementación de un sistema de seguridad de la información, exclusivo para universidades, programando módulos multiagente (Faris et al., 2014). Aquí se hace un estudio de las herramientas y frameworks utilizados para la gestión de riesgos de redes de información. Según los autores, la gestión del riesgo de la organización es un elemento clave en el programa de seguridad de la información y provee un marco de referencia efectivo para seleccionar los controles de seguridad apropiados para un sistema de información. Ponen énfasis en el análisis comparativo de los diferentes frameworks de gestión de riesgos aceptados por la industria, recalcando que ninguno de ellos tiene un enfoque multiagente. También analizan los estándares ISO 27001, 27002 y 27005 destacando sus características relevantes, así como al framework ITIL V3, del cual dicen que es el más aceptado en el mundo. El estudio concluye determinando que las técnicas actuales de gestión de riesgos son inadecuadas porque tienen un enfoque reactivo, es decir, actúan después de producirse un ataque por lo que se recomienda cambiar a un enfoque proactivo, para prevenir los riesgos y amenazas, sin comprometer la integridad de los sistemas de información.

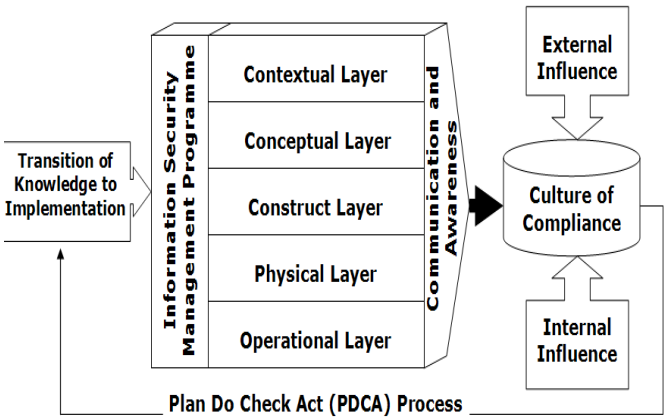


Figura 6: Modelo de gestión de los profesionales de la seguridad
Autor: (May & Lane, 2006)

El estudio "A Model for Improving e-Security in Australian Universities" realizado en Queensland University of Technology, (May & Lane, 2006), propone un modelo basado en capas, que tenga a la cultura de

conformidad con las políticas y procesos de seguridad, como principal componente, esto debido a que la universidad constituye un entorno pluricultural, en el que no todos los integrantes miran del mismo modo al tema de la seguridad de datos. En la figura 6 se puede ver el modelo de gestión de los profesionales que está basado en 5 capas.

Este modelo da más importancia al cómo implementar, antes que al qué implementar. Actualmente este modelo está siendo aplicado en la Universidad Cruz del Sur, para validar su aplicabilidad y utilidad.

Un estudio acerca de la relación entre las políticas de seguridad de la información y la efectividad de los sistemas de gestión de información, se ha llevado a cabo en las principales universidades palestinas de la franja de Gaza además, se investiga la relación entre la implementación de políticas de seguridad, con la efectividad de los sistemas de seguridad de la información empleados (Abdelwahed, Mahmoud, & Bdair, 2016). Realizan un análisis de los diferentes métodos de desarrollo y ciclo de vida de las políticas de seguridad, así como de los sistemas de gestión de la información. Los principales resultados obtenidos de dicho estudio son:

- Las universidades palestinas se enfocan en la creación e implementación de políticas de seguridad de la información.
- Examinan y renuevan dichas políticas, cada cierto tiempo.
- Los sistemas de gestión de la información utilizada por estas universidades dieron resultados idóneos.
- Existe una relación entre la implementación de políticas de seguridad de información y la efectividad de los sistemas de gestión de seguridad de la información.

Según la empresa Digiware, Ecuador es el cuarto país que más ataques cibernéticos soporta en Latinoamérica, con un 11,22% del total de ataques recibidos por la región. Los sectores más atacados son el financiero y el gubernamental.

En el ámbito educativo, en el Ecuador, se han elaborado proyectos de grado que abordan el tema de seguridad en redes de información. Se analizan las diferentes metodologías existente para el análisis de riesgos y vulnerabilidades de las redes de información, como son: Diseño de un Plan para el Tratamiento de riesgos Tecnológicos utilizando la metodología NIST SP 800-30 (Beltran & Yesabeth, 2015), Análisis de los riesgos y vulnerabilidades de la red de datos de Escuela Politécnica Nacional (Pazmiño Naranjo, 2007), Propuesta metodológica para la implementación de buenas prácticas y procedimientos de verificación de seguridad de datos (Yanchapaxi & Marcelo, 2017); para proponer soluciones puntuales a los problemas detectados en redes de datos.

En otros trabajos del mismo tipo, se observa que el interés de los autores no está en determinar el número de ataques, sino en demostrar que la red ya está siendo atacada, y en determinar los factores que provocan, así, en un estudio desarrollado por la Universidad de Babahoyo, (G. Vega & Ramos, 2017) se llega a las siguientes conclusiones:

- La Universidad no cuenta con políticas de seguridad de la información.
- Los virus informáticos siempre están presentes.
- Existe software malicioso en las computadoras de la Universidad.
- Sólo el 50% del personal a cargo de la red de datos utiliza algún software de seguridad de redes.
- El 55% de administradores utiliza algún software de monitorización de red, por lo que se deduce que la red no está siendo protegida de manera adecuada.

También, se hace un estudio profundo de una metodología específica (Pazmiño, 2007). En otros casos, se plantean soluciones más generales, tales como modelos de seguridad basados en diferentes técnicas relacionadas con la seguridad de las redes de datos.

Otros trabajos se enfocan en el acceso a la red y las restricciones de navegación que deberían implementarse en una red universitaria. En este aspecto, se destaca la tesis de maestría de la Universidad de Los Andes, extensión Puyo (Guallpa, 2017), quien obtiene los siguientes resultados:

- Los estudiantes aceden a los servicios web de la Universidad sin credenciales de autenticación.
- Los estudiantes si tienen credenciales de acceso, proporcionada por el departamento de TI de la universidad. (pero no son necesarias para el acceso)
- Los estudiantes pueden conectarse a cualquier computador de la universidad, esto evidencia que no hay segmentación de red ni de servicios.
- Las credenciales de acceso no se cambian con frecuencia.
- Los estudiantes pueden ingresar anónimamente a la red de la Universidad, lo que sin duda es un indicador importante de la vulnerabilidad de la red de la Universidad.
- No hay restricciones en cuanto al contenido de la información que los estudiantes pueden descargarse.

En todos los trabajos mencionados, como parte del proceso investigativo, los autores determinan estadísticamente las vulnerabilidades que tiene cada red estudiada. Tomando en cuenta los aspectos comunes a todas ellas, se ha procedido a elaborar un resumen, graficado en la figura 9, en el que se sintetiza los resultados estadísticos obtenidos por los autores citados anteriormente.

Puede apreciarse que la ausencia, o desconocimiento por parte de los interesados, de una política de seguridad de la información es alta, lo que desencadena la ocurrencia de las demás fallas en seguridad, tales como restricciones de accesos y contenidos, deficiente manejo de contraseñas de acceso, exposición a virus y malware, ausencia de software de monitoreo y análisis de red. Es evidente la importancia que el tema de

la seguridad de la información tiene en los ámbitos académico, empresarial, y también social, puesto que actualmente casi no hay actividad que no se realice por medio de una red de datos.

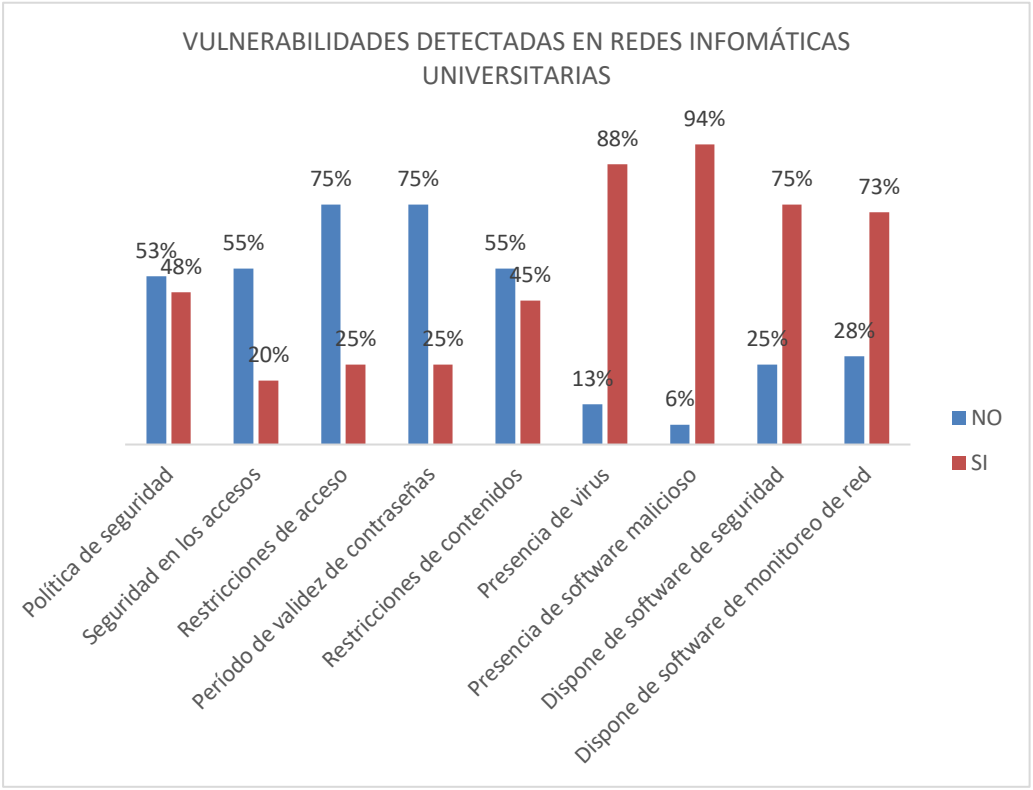


Figura 7: Vulnerabilidades generales de las redes de datos en las universidades del Ecuador

Fuente: El Autor

De lo expuesto, se puede determinar que el primer paso para decidir la implementación de un sistema de gestión de la información, es el establecimiento de políticas de seguridad, que deben ser evaluadas y actualizadas permanentemente. Deben ser valorados los distintos frameworks de seguridad de información, así como las diferentes metodologías de análisis de riesgos, dominantes en el mercado, para realizar una adecuada elección y desarrollo del modelo de seguridad que se va a proponer.

El establecimiento de políticas de seguridad de la información, y el desarrollo de un modelo adecuado a las necesidades de la Institución, garantizan la efectividad de los sistemas de gestión de seguridad que se

implementen. En nuestro país los miembros del CSIRT-CEDIA son toda institución miembro del CEDIA (por ejemplo Universidad Técnica de Ambato, la UNIANDES, la Escuela Politécnica del Chimborazo, Universidad Nacional del Chimborazo, Universidad Técnica Indoamérica, Universidad de las Fuerzas Armas-ESPE, entre otras), los directores de TI de estas instituciones son los encargados de reunirse con los miembros de CSIRT a nivel de país o en grupos zonales, para plantear un modelo de seguridad a seguir, con miras a mejorar la seguridad de la información a nivel de las universidades del país.

1.3. Gestión de la información

El término gestión se utiliza para indicar un conjunto de trabajos o actividades que permiten la realización de cualquier proyecto, también se puede decir que se refiere a todos aquellos trámites que se realizan con la finalidad de resolver un determinado proyecto. Esto puede realizarse en el ámbito empresarial o institucional, la gestión es asociada con la administración y manejo de un negocio. (Tápies, 2010)

La gestión de la información es la explotación de la información para la consecución de los objetivos de la entidad. Su creación, adquisición, procesamiento y difusión. (Alonso-Arévalo, 2007)

Las características que priman en el entorno de cualquier entidad moderna, que incorpore a su gestión las tecnologías de información, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, el envío de información y la seguridad de los datos, demanda transformaciones en la práctica de seguridad que va a ejercer el control de las redes de información.

En el contenido de las organizaciones o instituciones, la gestión de la

información se puede identificar como el método que se encarga de todo lo relacionado con el proceso de obtener la información acorde a las necesidades, libre de errores, para la persona indicada, a un coste conveniente, en el tiempo determinado y articulando todas estas operaciones para el desarrollo de una tarea correcta.

La gestión de la información incluye todos los pasos adecuados que cumplen con las necesidades de una organización. En términos de gestión de riesgos de seguridad de los datos, en una empresa se debe proteger la documentación digital al igual que aquella contenida en cualquier otro soporte como por ejemplo el papel. Los documentos de una empresa o institución tienen un ciclo de utilización, luego del mismo éstos deben ser destruidos de una forma segura. En Ecuador una información digital se debe resguardar 7 años en el sector público. (INEN 2015)

En la sociedad actual, la revolución digital ha transformado las relaciones con usuarios, proveedores e instituciones, donde el Internet es utilizado como medio de comunicación. Éste por su naturaleza libre y de bajo coste, ha permitido interconectar a las personas con las empresas entre sí, rompiendo las barreras geográficas y habilitando en gran medida la llamada globalización de la economía y la sociedad

1.4. Vulnerabilidades o riesgos de la información

Las vulnerabilidades son puntos débiles en la seguridad de un sistema informático o de un proceso, a través de estos se pueden presentar cierto tipo de amenazas que pueden poner en peligro la confidencialidad, integridad y autenticación de la información (Milagros & Steven, 2017). Es importante tener en cuenta que parte de la red de datos es la que debería estar más resguardada en nuestra institución, tomando en cuenta que una red puede tener dispositivos físicos, documentos, infraestructura, entre otros.

Pueden existir riesgos físicos, naturales, de las comunicaciones, software e incluso humanas. Los físicos se refieren a la posibilidad de

acceder al sistema directamente desde el equipo para extraer datos, alterarlos o destruirlos. Los naturales, es cuando la información sufre daños imprevistas como incendios, inundaciones, terremotos. Las vulnerabilidades de las comunicaciones, son eventos en el que varios usuarios pueden acceder a un sistema informático que se encuentra conectado a una red global y sustraerse la información. Los riesgos de software en cuando hay la posibilidad de que el sistema sea sensible por la forma de diseño del programa. También se puede decir que las personas o usuarios que tiene acceso al sistema pueden cometer errores involuntarios que afecten a los datos. (Mieres, 2009)

Un aspecto que se debe tomar en cuenta es que la información debe estar disponible, para el usuario autorizado en cualquier momento. La validación de identificación, que generalmente no es tomada en cuenta por sistemas comerciales, se refiere a que sólo usuarios autorizados y con los privilegios adecuados, tengan acceso al sistema de información. Todos los ataques a las redes de información, se encajan en la integridad, confiabilidad, confidencialidad y disponibilidad de los datos.

Varias circunstancias pueden amenazar los sistemas de seguridad de una empresa o institución. Entre ellos se puede mencionar insiders, o personal interno, virus, malware, gusanos o hackers en general. Las amenazas detonan posibles vulnerabilidades a la infraestructura de la red de datos.

1.4.1. Clasificación de las vulnerabilidades

Según Pazmiño (2007), en su investigación "Análisis de los riesgos y vulnerabilidades de la red de datos de la Escuela Politécnica Nacional" dice que, las vulnerabilidades de acuerdo a su naturaleza pueden ser:

- **Vulnerabilidades de diseño:** es una debilidad que se puede encontrar dentro de las especificaciones de hardware o software. Éstas representan el mal esquema de aplicaciones de software,

arquitecturas de red, infraestructura física, sistemas de seguridad, entre otros. Los riesgos asociados a esta vulnerabilidad son los siguientes: por vandalismo, de mal uso o mala configuración de equipos, de pérdida de la información.

- **Vulnerabilidades de configuración:** resultan de un error en la configuración y administración de un componente de sistema, también pueden aparecer como consecuencia de un error humano. Éstas hacen que una institución sea propensa a los siguientes riesgos asociados: pérdida de información, caídas de sistema, pérdida de confidencialidad de la información, de autenticación y de violación de la integridad.
- **Vulnerabilidades de implementación:** están asociadas a actividades de programación errónea de sistemas. Los riesgos que están asociados son: de mal uso o configuración de equipos, pérdida de información, caída de sistemas, pérdida de confidencialidad de la información, violación de integridad, riesgos económicos, entre otros.
- **Vulnerabilidades organizacionales:** aparecen cuando no existe la documentación adecuada a las políticas y prácticas de seguridad dentro de la institución, o estas no son debidamente explicadas y fundamentadas para su correcta aplicación.
- **Vulnerabilidades tecnológicas:** están presentes en aplicaciones a servicios de red, arquitectura, sistemas operativos y sus aplicaciones, éstos incluyen debilidades de diseño, implementación y configuración.
- **Vulnerabilidades físicas:** son asociadas a la infraestructura física con la que cuenta la institución para asegurar un desempeño aceptable de todos los procesos que maneje, dentro de éstos se puede los siguientes aspectos: falta de sistemas de control de acceso, carencia de protección antisísmica, no contar con sistemas de acondicionamiento para los servidores, entre otros.
- **Vulnerabilidades de control:** se formulan como parte de un control mal desarrollado o implementado dentro de una institución. Estos

pueden ser riesgos de pérdida de la información, de caídas de sistema o económicos. (Pazmiño Naranjo, 2007)

1.5. Seguridad de la información

La información es lo más valioso que tiene una empresa o institución y si llega a mano de personas ajenas a ella, puede causar daño tanto material como económico. Por ello, es de gran importancia la seguridad de la información y la utilización de un modelo adecuado que pueda precautelar todos los datos y la utilización de los mismos. El término seguridad de la información se refiere a la confianza de que la misma no sea accedida por usuarios no autorizados, que siempre esté disponible, que los canales de transmisión no estén comprometidos. Es decir, la seguridad de la información implica que se requiere proporcionar protección a los recursos físicos, así como a los recursos abstractos.

La seguridad es una forma de protección contra los riesgos, es un conjunto de pasos o procedimientos en el que se toma en cuenta elementos como aspectos tecnológicos, de gestión organizacionales, de negocios, de tipo legal, de cumplimiento, entre otros. (Bertolín, 2008). La seguridad de la información, es un método de la informática que se encarga de proteger los objetivos básicos de la seguridad de una empresa a través de políticas, métodos o estándares que deberían ser implementados. Además de los conocimientos para proteger nuestras redes de datos y hacerlas más seguros, con el fin de evitar que personas ajenas a la institución ingresen o manipulen datos confidenciales.

Un modelo de seguridad es la presentación formal de una estrategia de seguridad y que debe identificar el conjunto de reglas y prácticas que regulan como un sistema maneja, protege y distribuye la información delicada. Se recomienda la utilización de ellos, de acuerdo al tipo de datos con los que se esté trabajando. En la figura 1 se puede ver las categorías de la clasificación de la información que son: integridad, disponibilidad y

confidencialidad.

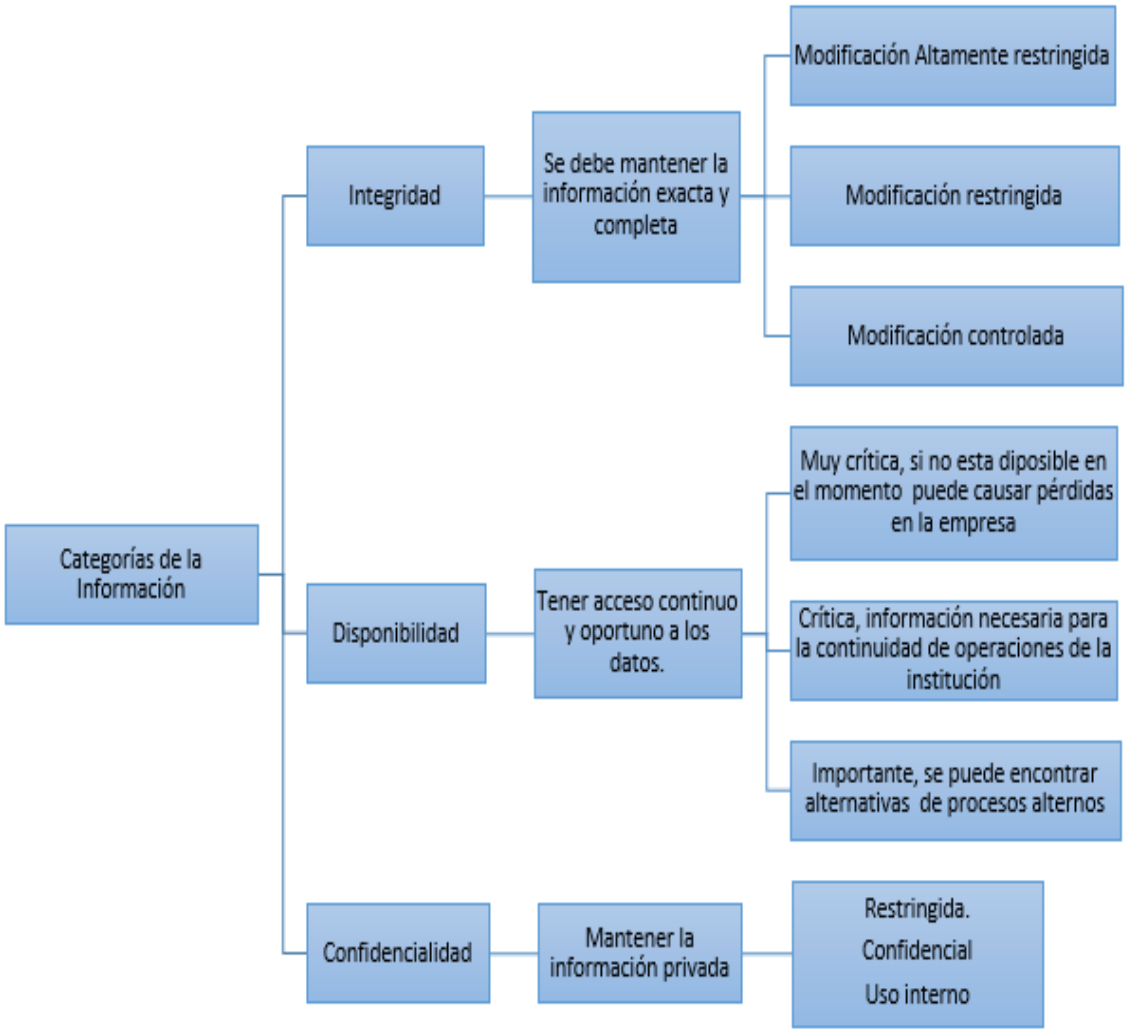


Figura 1 Categorías de la clasificación de la información

Fuente: El Autor

Los recursos físicos contemplan toda la infraestructura de la red (equipos de cómputo, dispositivos de almacenamiento, cableado, racks, host). En tanto que los recursos abstractos se refieren a la confianza de que información no sea accedida por usuarios no autorizados, que siempre esté disponible o que los canales de transmisión no estén comprometidos. Es decir, la seguridad de la información implica que se requiere proporcionar protección a los recursos físicos y recursos abstractos, incluido el software de aplicación. (Comer, 2015)

De manera general, un modelo de seguridad de información es el

conjunto de políticas, procedimientos, procesos y controles que una empresa adopta para promover la implementación de un sistema de gestión de la información.

En la actualidad la gran mayoría de las empresas usan tecnologías de la información para la gestión de sus operaciones, es por ello que se han creado diversos estándares o modelos y su implantación se ha convertido en los últimos años en una necesidad, para aquellas instituciones que deseen tener sus datos e información segura.

De acuerdo a cada circunstancia que se presente en una institución o empresa se puede acoplar los métodos o estándares que existen hoy en día. Se debe recalcar que para cada uno de los inconvenientes que se presenten, hay más de un modelo aplicable para gestionar dichas problemáticas.

CAPÍTULO 2
MODELOS Y GESTORES DE SEGURIDAD

2.1 Gestores de Seguridad

2.1.1 Gestión de proyectos con PMBOk (Proyect Management Institute PMI)

Es la guía de fundamentos de la gestión de proyectos. Es un libro donde se presenta estándares y normas que se deben seguir para la manipulación de un proyecto, fue realizado por PMI (Project Management Institute) que es una asociación profesional sin fines de lucro más importante y de mayor crecimiento a nivel mundial que tiene como misión convertir a la gerencia de proyectos como la actividad indispensable para obtener resultados en cualquier actividad de negocios. En la práctica es un grupo de profesionales de la gerencia de proyectos que se dedican a promover el desarrollo del conocimiento y competencia básicos para el ejercicio profesional.

Conocer qué es el PMBOK es el paso inicial para poder comprender la amplitud de la gestión de proyectos y su importancia para una organización, ya que el compendio de información contenida en el PMBOK provee a todo profesional que desee realizarse en esta área de los fundamentos de la administración de proyectos para poder aplicarlos en campos tan diversos como son la electrónica, el desarrollo de software, proyectos web y muchos otros más. Se basa en un conjunto de buenas prácticas divididas en 10 áreas de conocimiento subdivididas en actividades que van desde la gestión del alcance hasta gestión de las adquisiciones.

Figura 8: Grupos de procesos del PMBOK

Fuente: (PMBOK, 2018)

PMBOK está compuesta de 47 procesos de dirección de proyectos, agrupadas en 10 áreas de conocimientos. En el ciclo de vida de la dirección del proyecto se describe lo que se tiene que hacer para dirigir un proyecto, se divide en 5 grupos de procesos (Iniciación, Planificación, Ejecución, Seguimiento y Control, Cierre), pueden ser separados por cada fase del ciclo de vida del proyecto y los grupos de procesos no son fases del proyecto. Las partes del marco de trabajo de PMBOK son aplicables de acuerdo a la necesidad de la empresa. (Snyder & Dionisio, 2017).

Figura 9: Procesos del PMBOK

Fuente: (PMBOK, 2018)

2.1.2. ITIL (Information Technology and Infrastructure Library)

Es un estándar para la gestión de los servicios TI, centrado en brindar servicios de alta calidad para lograr la máximo satisfacción del cliente a un costo manejable. Para ello, parte de un enfoque El núcleo de ITIL comprende seis procesos de soporte de servicio y cinco procesos de entrega de servicios. Los procesos de soporte de servicio son utilizados por el nivel operacional de la organización, mientras que los procesos de prestación de servicios son tácticos por naturaleza. (Cater-Steel & Tan, 2005)

La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) es un marco desarrollado por el Reino Unido, Oficina de Comercio Gubernamental (OGC), que describe las mejores prácticas en gestión de servicios de Tecnología de Información y Comunicación (TIC). Hasta la fecha, ITIL es el único completo, no propietario,

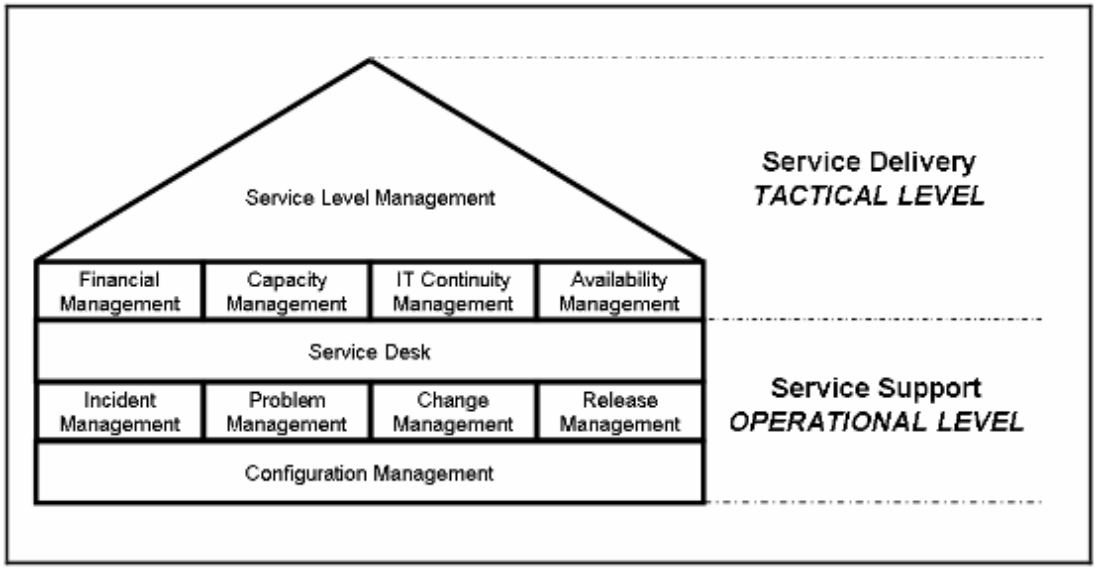


Figura 10: Funciones y procesos de gestión del servicio central de ITIL
Fuente: (Cater-Steel & Tan, 2005)

La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) es el marco de trabajo de "mejores prácticas" más popular para administrar los servicios de Tecnología de la Información (TI). Sin embargo, implementar ITIL no solo es muy difícil, sino que tampoco hay mejores prácticas para implementar ITIL. Como resultado, las implementaciones de ITIL suelen ser largas, caras y riesgosas.

2.1.2. CMMI (Capacity Maturity Model Integrated)

El modelo CMMI es utilizado para medir el grado de madurez de las empresas o instituciones respecto a la aplicación de las mejores prácticas de desarrollo y gestión del software. Este modelo tiene cinco niveles de madurez: inicial, repetible, definido, administrado, optimizado. Por lo general las empresas llegan solo hasta el nivel 3.

CMMI integra procesos que son esenciales para el desarrollo de productos,

que se han abordado por separado en el pasado, como ingeniería de software, ingeniería de sistemas y adquisición. Para usar los modelos CMMI publicados se necesita conocer el contenido de cada modelo y el área que desea mejorar. (Chrissis, Konrad, & Shrum, 2003)

El CMMI comienza con un proceso de evaluación que evalúa tres áreas específicas: desarrollo de procesos y servicios, establecimiento y gestión de servicios, y adquisición de productos y servicios. Está diseñado para ayudar a mejorar el rendimiento al proporcionar a las empresas todo lo que necesitan para desarrollar constantemente mejores productos y servicios.

Pero el CMMI es más que un modelo de proceso, también es un modelo de comportamiento. Las empresas pueden usar el CMMI para abordar la logística de mejorar el rendimiento mediante el desarrollo de puntos de referencia medibles, pero también pueden crear una estructura para alentar un comportamiento productivo y eficiente en toda la organización.

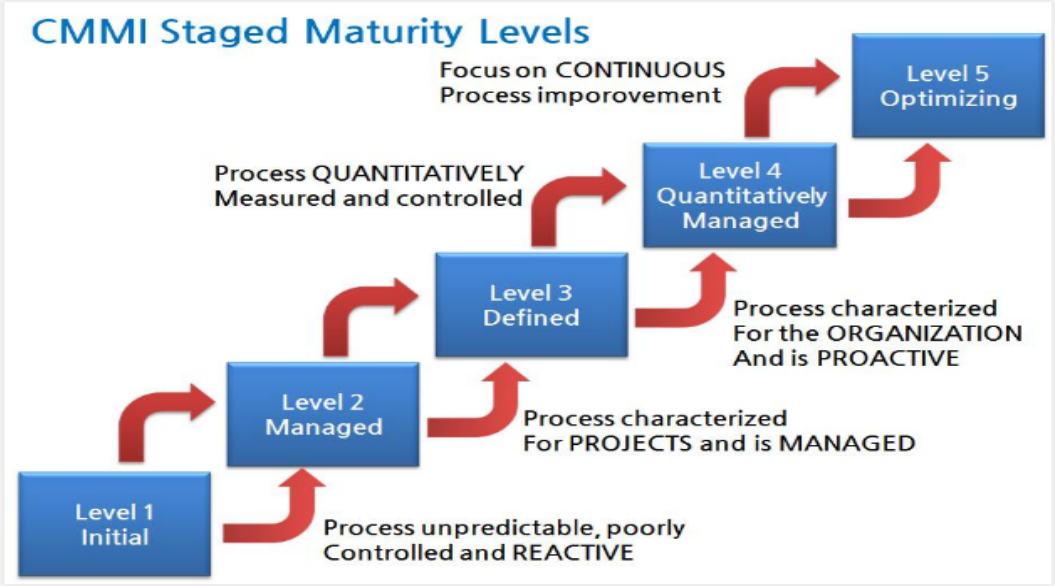


Figura 11: Niveles de CMMI

Fuente: (CMMI, 2003)

El modelo describe procedimientos, principios y prácticas que subyacen en la madurez del proceso de desarrollo de software. También proporciona las mejores prácticas para permitir que una organización desarrolle un enfoque estandarizado para el desarrollo de software que se pueda utilizar en muchos grupos diferentes. Los cinco niveles de madurez del modelo CMMI son:

- **Inicial:** la empresa no utiliza procedimientos y planes de gestión efectivos. No hay garantía de consistencia y la calidad es impredecible.
- **Repetible:** se cuenta con una estructura de gestión formal, control de cambios y garantía de calidad. La empresa no tiene modelos formales de proceso definidos.
- **Definido:** Existen procedimientos formales que delinean y definen los procesos llevados a cabo en cada proyecto. La organización tiene una manera de permitir la mejora cuantitativa del proceso.
- **Gestionado:** la empresa cuenta con procesos formales para recopilar y analizar datos cuantitativos, y las métricas se definen y se incorporan al programa de mejora de procesos.
- **Optimización:** la compañía evalúa los planes para la mejora continua de los procesos.

2.1.3. COBIT (Control Objectives for Information and related Technology)

Estándar utilizado para gestión y control de TI. Está conformado por cuatro dominios organizados en procesos que se subdividen en actividades y objetivos de control.

COBIT se ha diseñado como un sistema metodológico que consiste en un conjunto de objetivos de control de TI de alto nivel y una estructura global para su clasificación y funcionamiento. Su misión es: investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información. Está diseñado como un estándar aplicable y aceptable, para

una buena práctica de la auditoría de las tecnologías de la información en todo el mundo. (De Haes, Van Grembergen, & Debreceny, 2013)

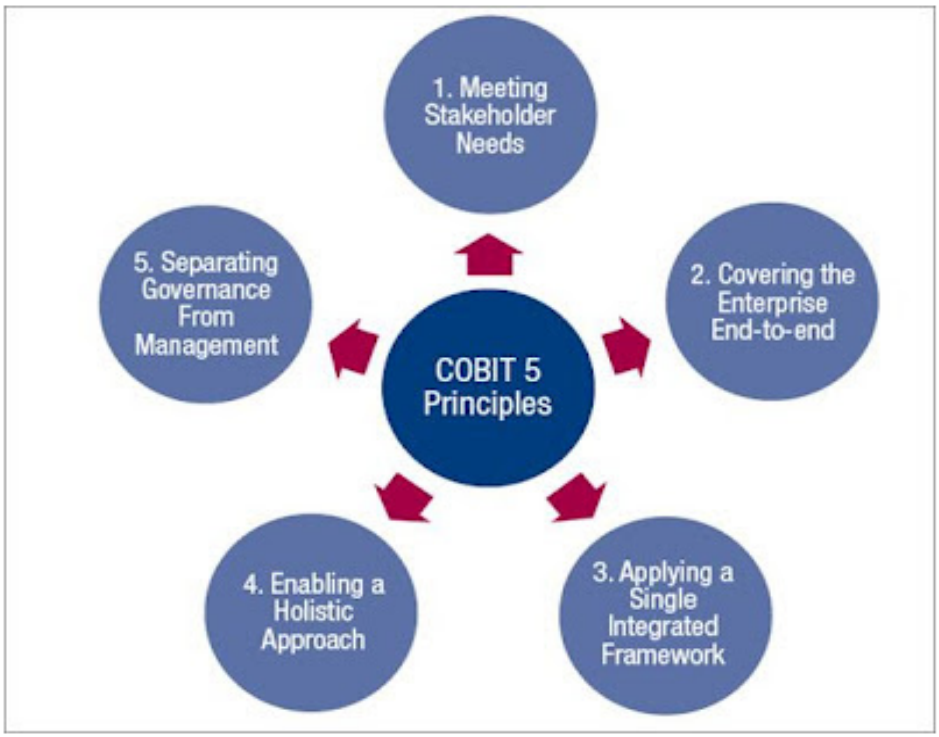


Figura 12: Principios de COBIT
Fuente: (COBIT, 2012)

De todos los modelos o estándares de seguridad de la información disponibles se han elegido: OSSTMMv3, NIST SP 800-30, ISO 27001, por su presencia y aceptación en el mundo de la informática, se consideran que marcan la pauta a seguir en los distintos aspectos que conforman un sistema de gestión de la seguridad de la información.

2.1. Modelos y estándares de Seguridad de datos

2.1.1. OSSTMMv3

El OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad, fue creado en 2001 por Pete Herzog Director Ejecutivo de ISECOM (Instituto para la Seguridad y Metodologías Abiertas) y más de 150 colaboradores directos. Es uno de los estándares profesionales más completos y manejados a la hora de revisar la Seguridad de los Sistemas

desde Internet.

Éste manual contempla el cumplimiento de estándares y buenas prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL, entre otras, lo que le hace uno de los manuales más completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones. (Valdez Alvarado, 2013). Más que un modelo de seguridad, es una herramienta de análisis de seguridad en las redes. Se la toma en cuenta debido a que provee directrices de pruebas de seguridad, en todos los ámbitos que conciernen a una red de información, desde el nivel físico (incluyendo al elemento humano), hasta el nivel de aplicación. (Herzog, 2017)

Según Herzog (2017), la metodología OSSTMM está alineada a la norma ISO 27001, está generalizada a la seguridad como una función de separación; es decir, separa un activo de información de posibles amenazas, estableciendo controles que permitan gestionar la confidencialidad, integridad y disponibilidad de la información, es un manual que permite la elaboración de pruebas de seguridad la información de una manera estable y repetible, el objetivo es proporcionar una metodología científica en donde se busca la mejora de la seguridad operacional (OpSec).

A esto ISECOM (2012) manifiesta que la metodología OSSTMMv3 se centra en detalles netamente técnicos de los elementos que necesitan ser auditados, buscando el mejoramiento de la seguridad de la información, en donde, las diferentes pruebas a aplicarse deben tratar de recopilar información de todos los canales que intervienen en la operación (factores humanos, factores físicos, redes inalámbricas, servicios, aplicaciones, telecomunicaciones y redes de datos).

Su propósito es proveer una metodología científica para examinar la organización, realizando pruebas de seguridad desde adentro hacia

afuera. (Vásquez Alvarado, 2014)

En la actualidad los entornos son significativamente más complejos que en los últimos años, debido a la evolución de la tecnología, tales como, operaciones remotas, virtualización, computación en la nube y otros tipos de infraestructura nuevas, ya no se puede pensar en simples pruebas sólo para ordenadores de sobremesa, servidores, o equipo de enrutamiento. OSSTMMv3, abarca pruebas de todos los canales. Esto también hace que sea adecuado para las pruebas de infraestructuras de computación en la nube, infraestructuras de comunicación móvil, lugares de alta seguridad, recursos humanos y computación confiable. Posee un tablero de instrumentos para la gestión y es beneficioso para pruebas internas y externas, permitiendo una comparación o combinación de los dos. El OSSTMMv3 incluye información para la planificación del proyecto, cuantificación de resultados y las reglas de contratación para realizar auditorías de seguridad. La metodología se puede integrar fácilmente con las leyes vigentes y las políticas para asegurar una seguridad exhaustiva que auditan por todos los canales.

Tabla 2: Clase y canales OSSTMMv3

Clase	Canal	Descripción
Seguridad física (PHYSSEC	Humano	Comprende el elemento humano de comunicación donde la interacción es físico o psicológico.
	Física	Seguridad física pruebas donde el canal es físico y no electrónico. Comprende lo tangible.
Seguridad de espectro (SPECSEC)	Wireless	Comprende todas las comunicaciones electrónicas, señales y emanaciones que llevará a cabo en el espectro

Seguridad de comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas.
	Redes de datos	Compromete todo sistema electrónico y redes de datos.

Fuente: (OSSTMMv3, 2010)

Utiliza 7 pasos que le llevará al inicio de una prueba de seguridad bien definida, estos son los siguientes:

1. Definir lo que desea proteger. Estos son los activos. Los mecanismos de protección para estos activos son los controles que pondrá a prueba para identificar limitaciones.
2. Identifique el área alrededor de los activos que incluye los mecanismos de protección y los de procesos o servicios en torno a los activos.
3. Definir todo fuera de la zona que usted necesita para mantener sus activos operacionales. Esto puede incluir cosas que no influye directamente en electricidad, aire, suelo estable, información, entre otras. Contar aquello que mantiene la infraestructura operacional como procesos, protocolos y recursos continuos. Este es el alcance de la prueba.
4. Definir cómo su alcance interactúa dentro de sí mismo y con el exterior. Lógicamente segmentar los activos dentro del ámbito a través de la dirección de las interacciones tales como: interior a exterior, exterior a interior, interior a interior, Departamento A Departamento B, entre otras. Se trata de sus vectores. Cada vector idealmente debería ser una prueba separada para mantener la duración de la ella, compartimentado lo que puede suceder en el entorno.
5. Identificar qué equipos se necesitan para cada prueba. Dentro de cada vector, pueden producirse interacciones en varios niveles. Estos

niveles pueden ser clasificados de muchas maneras, sin embargo aquí han sido clasificado por función como cinco canales: Humanos, Física, Wireless, telecomunicaciones y redes de datos. Cada canal debe analizarse por separado para cada vector.

6. Determine qué información desea obtener de la prueba. ¿Va estar probando interacciones con el patrimonio o también en la respuesta de las medidas de seguridad activa?
7. Asegurar la prueba de seguridad definidos en conformidad a las reglas de contratación, una pauta para asegurar el proceso, con una prueba adecuada de seguridad, sin creación de malentendidos, falsas ideas o falsas expectativas.

El resultado final será una medida de la superficie de ataque, que es la parte desprotegida, el alcance de un Vector definido.

Tabla 2: Términos que se utilizan en el modelo de seguridad OSSTMMv3

Término	Definición
Superficie de ataque	La falta de separaciones específicas y controles funcionales que existen para ese vector.
Vector de ataque	Un sub-ámbito de un vector creado para abordar las pruebas de seguridad de un ámbito complejo de manera organizada. Se basa en el paradigma de diseño de algoritmo de dividir y conquistar, que consiste en dividir un problema de forma recursiva en dos o más sub problemas del mismo tipo (o relacionado), hasta que se vuelvan lo suficientemente simples como para resolverlos directamente.
Controles	Controles de reducción de impacto y pérdida. La garantía de que los activos físicos y de información, así como los propios canales, están protegidos contra diversos tipos de interacciones no válidas, según lo define el canal. Por ejemplo, asegurar la tienda en caso de incendio es un control que no evita que el inventario se dañe o sea robado, pero que pagará un valor equivalente por la pérdida. Se han definido diez controles. Los primeros cinco controles son Clase A e interacciones de control. Los cinco controles de

	Clase B son relevantes para los procedimientos de control. Consulte la sección 1.2 a continuación para obtener más información sobre los controles.
Limitaciones	Este es el estado actual de los límites percibidos y conocidos para los canales, las operaciones y los controles según lo verificado dentro de la auditoría. Los tipos de limitaciones se clasifican por la forma en que interactúan con la seguridad y la seguridad en un nivel operativo. Por lo tanto, las opiniones en cuanto al impacto, la disponibilidad en la naturaleza, la dificultad de realizar y la complejidad no se utilizan para clasificarlas.
Operaciones	Las operaciones son la falta de seguridad que uno debe tener para ser interactivo, útil, público, abierto o disponible. Por ejemplo, limitar la forma en que una persona compra bienes o servicios de una tienda a través de un canal en particular, como una puerta para entrar y salir, es un método de seguridad dentro de las operaciones de la tienda.
Perfecta seguridad	El balance exacto de seguridad y controles con operaciones y limitaciones.
Porosidad	Todos los puntos interactivos, operaciones, que se clasifican como una visibilidad, acceso o confianza.

Fuente: (OSSTMMv3, 2010)

OSSTMM contempla seis tipos de pruebas, que van desde la intrusión hasta la auditoría guiada, estas son: blindaje o hacking ético, doble blindaje, auditoría de caja negra o pruebas de penetración, de caja gris, de doble caja gris, test tándem o secuencial y prueba inversa.

El Manual de la Metodología Abierta de Testeo de Seguridad tiene diferentes controles, uno de ellos son los controles de operación. Éstos están compuestos de 2 tipos: controles clase A y clase B. La clase A son los controles interactivos, éstos constituyen exactamente la mitad de todos los controles de operación e influyen directamente en la visibilidad, el acceso o las interacciones de confianza. En la Figura 13 se puede ver los tipos de categorías de controles de Clase A. La clase B son también conocidos como los controles de proceso que se utilizan para crear procesos de defensa.

Estos controles no influyen directamente en las interacciones, sino que protegen los activos una vez que se encuentran amenazados. En la Figura 14 se puede ver los controles de Clase B.

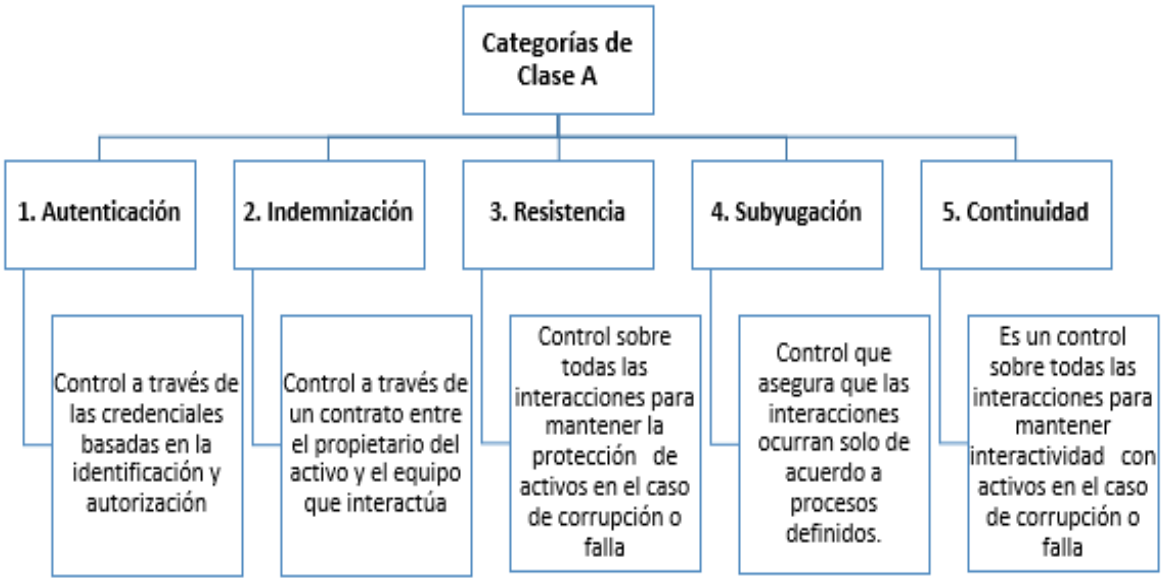


Figura 13: Tipos de categorías de controles de Clase A

Fuente: El Autor

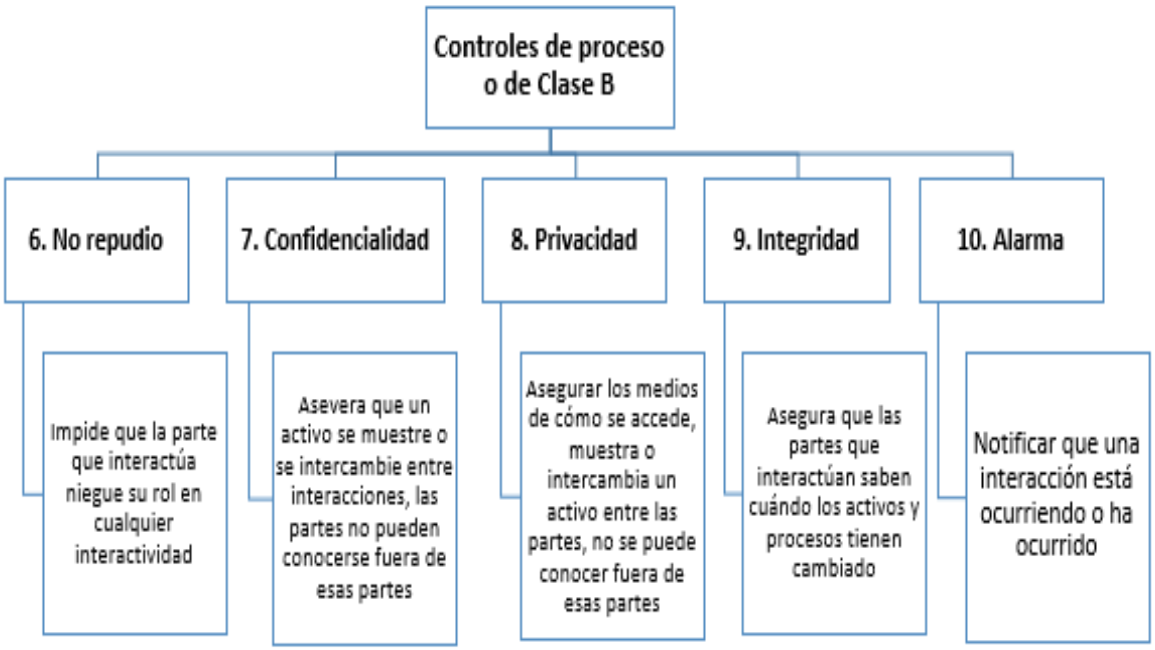


Figura 14: Tipos de categorías de controles de Clase B

Fuente: El Autor

De acuerdo a la necesidad de las instituciones o empresas se pueden aplicar los diferentes controles que tiene el modelo OSSTMMv3. El uso de controles debe garantizar que no se presenten nuevos ataques. Para facilitar la comprensión de los controles de operación, OSSTMMv3 tiene los siguientes objetivos de aseguramiento de la información: confidencialidad, integridad y disponibilidad.

Tabla 3: Objetivos de aseguramiento de la información

Objetivos de aseguramiento de la información	Controles de operación
Confidencialidad	Confidencialidad Privacidad Autenticación Resistencia de
Integridad	Integridad No repudio Subyugación
Disponibilidad	Continuidad Indemnización de Alarma

Fuente: (OSSTMMv3, 2010)

La metodología OSSTMMv3 se centra en dos canales que ayudarán a una obtención eficaz de datos. El canal de seguridad físico con la sección humano y el canal de seguridad de las telecomunicaciones con la sección redes de datos que tienen sus correspondientes tareas y procedimientos, de acuerdo al 4canal que está siendo evaluado.

Tabla 4: Mapeo con limitaciones efecto seguridad y cómo se determinan los valores

Categorías		OpSec	Limitaciones
Operaciones		Visibilidad	Exposición
		Acceso confianza	Vulnerabilidad
		Autenticación	
Controles	Clase A – Interactivo	Indemnización	Debilidad
		Resistencia	
		Subyugación	
		No continuidad	
		Repudio	
	Clase B – Proceso	Confidencialidad	preocupación
		Privacidad	
		Integridad	
		Alarma	
			Anomalías

Fuente: (Valdez Alvarado, 2013)

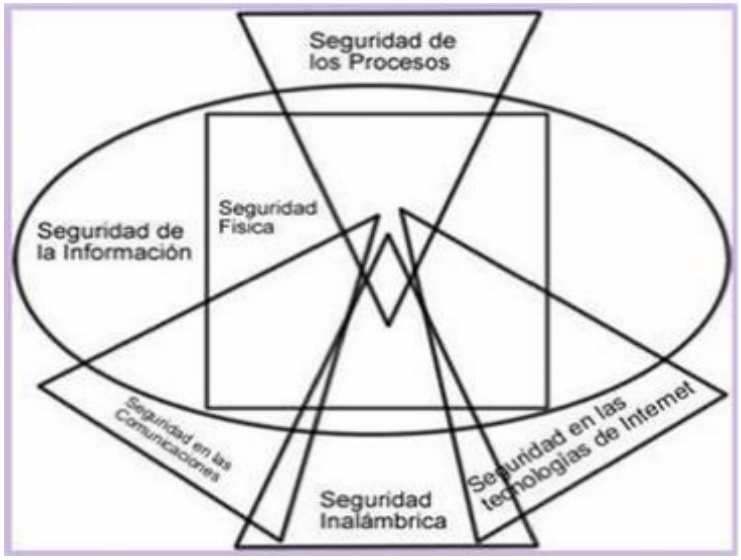


Figura 15: Esquema de la metodología OSSTMMv3

Fuente: (Gavilánez & de la Nube, 2016)

En la figura 15 se puede visualizar los esquemas de la metodología OSSTMMv3. Se puede utilizar la metodología OSSTMMv3 para evaluar la

seguridad de los sistemas operativos, sus vulnerabilidades y estimaciones de ataques que puedan afectar el equipo de cómputo.

2.1.2. NIST SP 800-30

Es una metodología de gestión de riesgo, proporcionada en forma de guía, desarrollada por el departamento de comercio del gobierno de los Estados Unidos. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) implemento la guía: Seguridad de la información para pequeñas empresas, que tiene como objetivo proporcionar recomendaciones de seguridad cibernética básicas para empresas a través de un proceso de evaluación de riesgos. (NIST, 2012)

Al proporcionar liderazgo técnico para la infraestructura nacional de medición y estándares, NIST SP 800-30 desarrolla técnicas de prueba, datos de referencia, pruebas de implementaciones conceptuales y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. NIST contiene el desarrollo de normas y directrices técnicas, físicas, administrativas y de gestión para la seguridad y privacidad adecuada de la información delicada no clasificada en sistemas informáticos federales.

La publicación especial 800-series informa sobre los esfuerzos de investigación, orientación y divulgación de NIST en seguridad de datos, y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas. La guía está conformada por cinco secciones que en conjunto son un proceso iterativo de tareas que se ejecutan de manera secuencial. (Stoneburner, Goguen, & Feringa, 2015)

El modelo NIST-300 tiene entradas, actividades y salidas. Las actividades constan de 9 pasos, pero no siempre se deben realizar todos los pasos presentados, estos se utilizan acorde a las necesidades de la institución. Por lo general, se utiliza en la seguridad de la red de datos

cuando se envía mediante el internet.

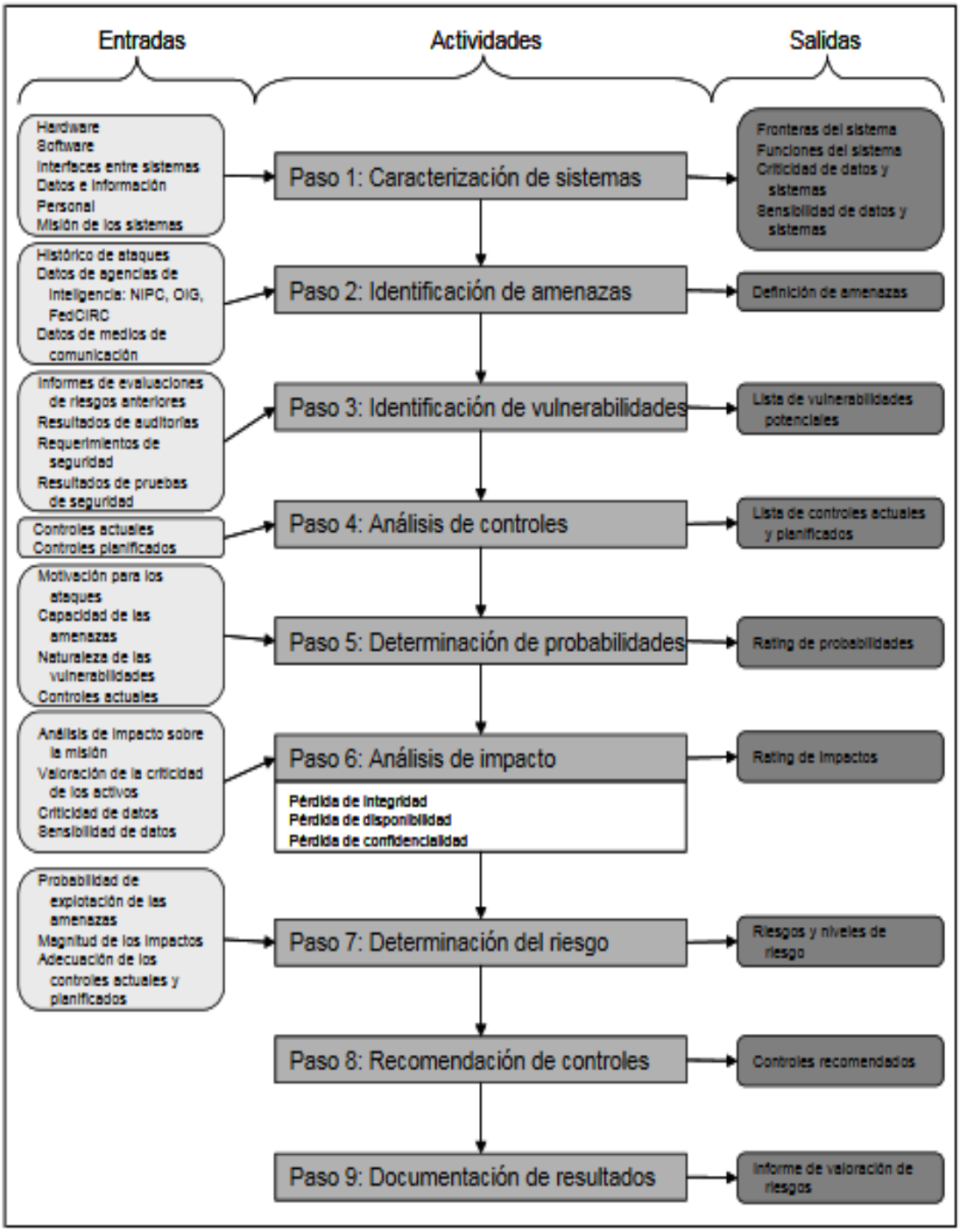


Figura 16: Procesos de análisis de riesgos de NIST SP 800-30

Fuente: (Matalobos Veiga, 2009)

En la figura 17 se puede ver las entradas, actividades y salidas de los procesos de gestión de riesgos de NIST SP 800-30.

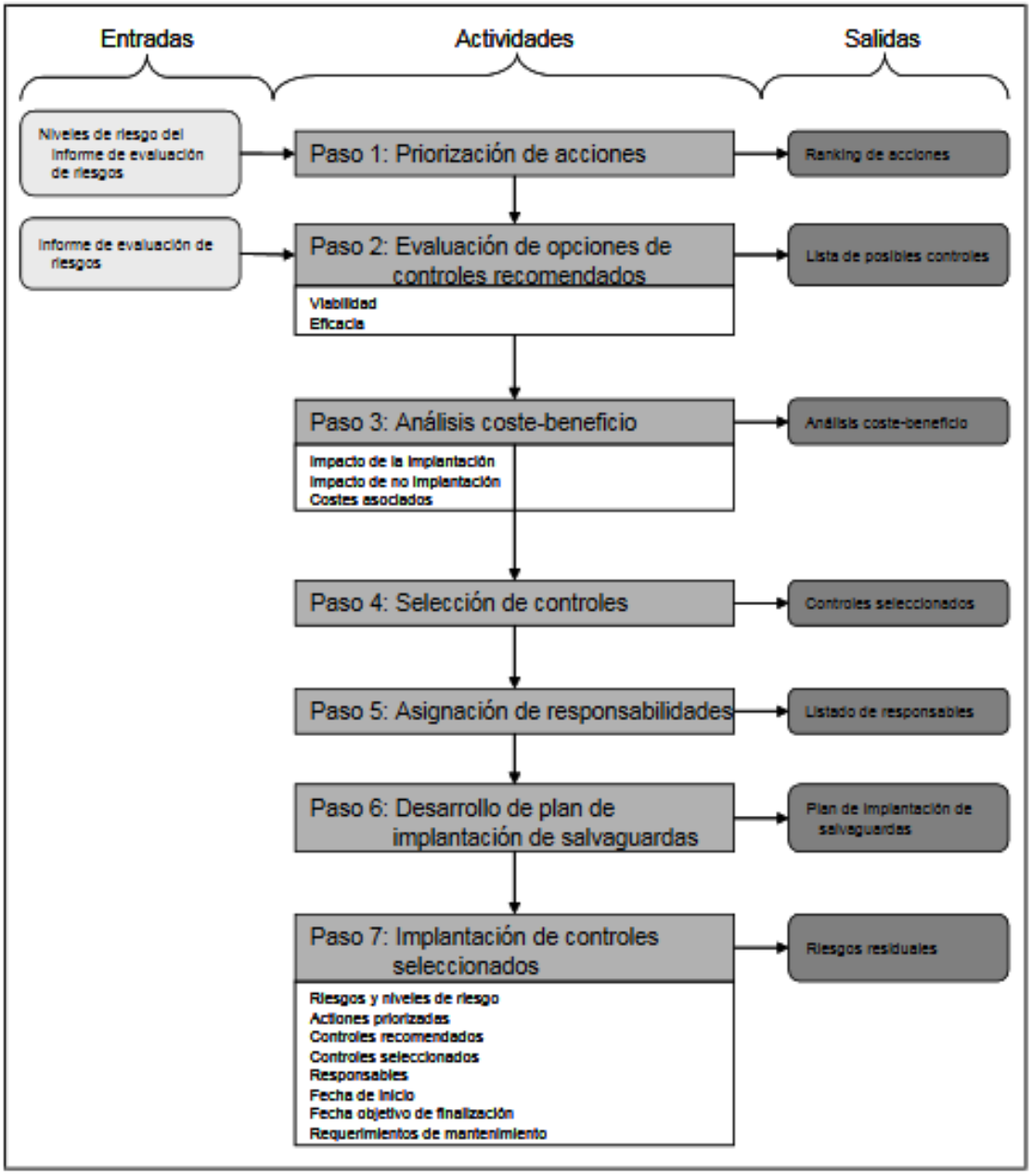


Figura 17: Procesos de gestión de riesgos de NIST SP 800-30

Fuente: (Matalobos Veiga, 2009)

2.1.3. ISO 27001

Es la norma para seguridad informática de la Organización Internacional de Normalización que describe la manera de gestionar la seguridad de la información de una empresa. Está basado en el ciclo de mejora continua propuesto por Deming (planificar, hacer, verificar, actuar), lo cual implica que un sistema de gestión de información basado en esta norma es dinámico, puesto que se está revisando continuamente (Calder & Watkins, 2008). Para conseguir la mejora continua, la norma pone énfasis en

buscar los potenciales problemas de seguridad que pueden comprometer la información, y proponer formas de evitarlos. Pone énfasis en la documentación adecuada de cada proceso, y en la revisión continua de todos ellos, para adaptar el sistema de gestión a los cambios que se producen al expandirse la empresa. (Disterer, 2013)

El estándar ISO/IEC 27001 determina los requisitos para analizar, establecer, implementar, monitorear, proteger y optimizar un SGSI, además especifica lo que se necesita para la

Implementación de controles de seguridad de acuerdo a las necesidades de la institución, frente a un proceso específico o un servicio. Esta normativa comprende dos secciones, en la primera se especifican cinco cláusulas enfocadas a características metodológicas del SGSI y en la segunda se definen los controles para la gestión de la seguridad de la información. (Calder & Watkins, 2008).

La ISO 27001 se utiliza en la alineación, requerimientos de seguridad, conocimiento de la administración de los riesgos, la disposición de las políticas y procedimientos de seguridad, y los mecanismos para la medición de efectividad del programa de seguridad de la información, las políticas, los controles y planes para el tratamiento del riesgo. (Solarte, Rosero, & del Carmen Benavides, 2015)

Estos tres modelos ayudarán en el desarrollo del Modelo de Seguridad de la Información de la Universidad, y también podrán ser implementados en otras instituciones de educación con modificaciones acorde a sus necesidades.

ISO 27001 proporcionará la metodología para desarrollar el modelo, OSSPMMv3 proveerá las directrices para realizar las pruebas que garanticen la seguridad de la red de información, y finalmente, NIST 800-30 servirá de guía para desarrollar medidas de gestión de riesgos en la red de

información.

Hay que tomar en cuenta que los estándares fueron creados para diferentes necesidades o propósitos, por lo que, no siempre pueden encajar el uno con el otro. El reto se encuentra en saber que partes de cada estándar o modelo se puede utilizar en determinada institución en particular, para ayudar a cumplir sus objetivos institucionales.

Según NTE INEN-ISO/EC 27001 (2018), los controles del estándar ISO 27001 se agrupan de la siguiente forma:

- **A.5 Política de seguridad de la información:** está constituido por dos controles. Aquí se puede ver la complejidad que representa el diseño, planteamiento, preparación, desarrollo y revisiones de una Política de Seguridad. Se recomienda seguir los siguientes pasos: Política de Seguridad (RFC1244) → Análisis de riesgo → Grado de exposición → Plan de Seguridad → Plan de contingencia.
- **A.6 Organización de seguridad de la información:** tiene 7 controles. Está dividido en dos grupos. Abarca roles y responsabilidades de seguridades de la información, separación de funciones, contacto con las autoridades, contacto con los grupos de interés especial, gestión de proyectos de seguridad de la información, política de dispositivo móvil y teletrabajo.
- **A.7 Seguridad en recursos humanos:** tiene 3 grupos, cubre 6 controles. Se encuentra subdividido en: antes del empleo, durante el empleo y finalización o cambio de empleo. Se inicia por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos, aquí se debe determinar los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información de ese puesto.
- **A.8 Gestión de activos:** dividido en 3 grupos, tiene 10 controles.
- **A.9 Controles de acceso:** 4 grupos, 14 controles.

- **A.10 Criptografía:** tiene 2 controles.
- **A.11 Seguridad física y del entorno:** este grupo cubre 15 controles y se divide en: áreas seguras y equipos.
- **A.12 Seguridad de las Operaciones:** tiene 7 grupos y 14 controles.
- **A.13 Seguridad en las comunicaciones:** tiene 2 grupos y 7 controles.
- **A.14 Adquisición, desarrollo y mantenimiento del sistema:** tiene 3 grupos y 13 controles.
- **A.15 Relaciones con los proveedores:** 2 grupos y 5 controles.
- **A.16 Gestión de incidentes de seguridad de la información:** tiene 7 controles.
- **A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio:** tiene 2 grupos y 4 controles.
- **A.18 Cumplimiento:** tiene 2 grupos y 8 controles.

Los requisitos de la Norma ISO 27001 aporta un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que se garantice en todo momento la continuidad de las actividades de la empresa. Los Objetivos del SGSI son preservar la:

- Confidencialidad
- Integridad
- y Disponibilidad de la Información

El Sistema de Gestión de la Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la siguiente figura.

Figura 11: El SGSI que propone la Norma ISO 27001

Fuente: (ISO 27001, 2018)

2.1.4. CONTROLES CIS

Los controles críticos de seguridad del Centro de Seguridad de Internet (Controles CIS) nacieron en el 2018 y se crearon en cooperación con representantes del gobierno de Estados Unidos y organizaciones de investigación de seguridad del sector privado. Son un conjunto de defensas prácticas de naturaleza técnica encaminadas a detener los ciberataques más comunes que comprometan los sistemas de información. (CERT-PY,

2017)

Los controles CIS están diseñados para dar prioridad y enfoque, para aprovechar el poder de una gran comunidad de expertos para identificar y apoyar prácticas de gran valor y pasos fundamentales, y para ayudar en la ciberseguridad de las empresas o instituciones. Éstos se centran en la acción técnica, los desarrolladores de los Controles reconocieron que muchas de estas recomendaciones obligarían a los equipos técnicos operacionales a cambiar las prácticas para mejorar tanto los controles operacionales como la seguridad, reevaluar sus estrategias básicas de defensa y ser más estructurados y disciplinado en sus actividades. Pero siempre hay que tomar en cuenta que los controles deben estar bien aplicados para que se obtenga el resultado esperado. (CIS, 2018)

La implementación exitosa de los controles requerirá que muchas organizaciones cambien su forma de pensar sobre la ciberseguridad, es decir que todos sus empleados y directivos se adopten a la nueva forma de gestionar la seguridad, a la forma en que abordan las operaciones y la defensa de TI.

Las organizaciones por lo general no implementan cada uno de los subcontroles descrito en los controles CIS (la versión 6.0, por ejemplo, tiene 149 subcontroles), solo adoptan los que están acorde a sus necesidades.

Muchas organizaciones se encuentran siguiendo una arquitectura de seguridad utilizando como base otras normas o regulaciones de seguridad, tales como, la Framework de ciberseguridad NIST, la alineación del NIST y la serie ISO 27000, entre otras. Buscar un estándar como NIST 800-30 no impide que las organizaciones usen los Controles CIS como la forma efectiva hacia el logro de estándares adicionales.

En las empresas o instituciones, es adecuado implementar por fases, esto ayuda a garantizar los beneficios importantes logrados mediante la

implementación de los controles de mayor prioridad.

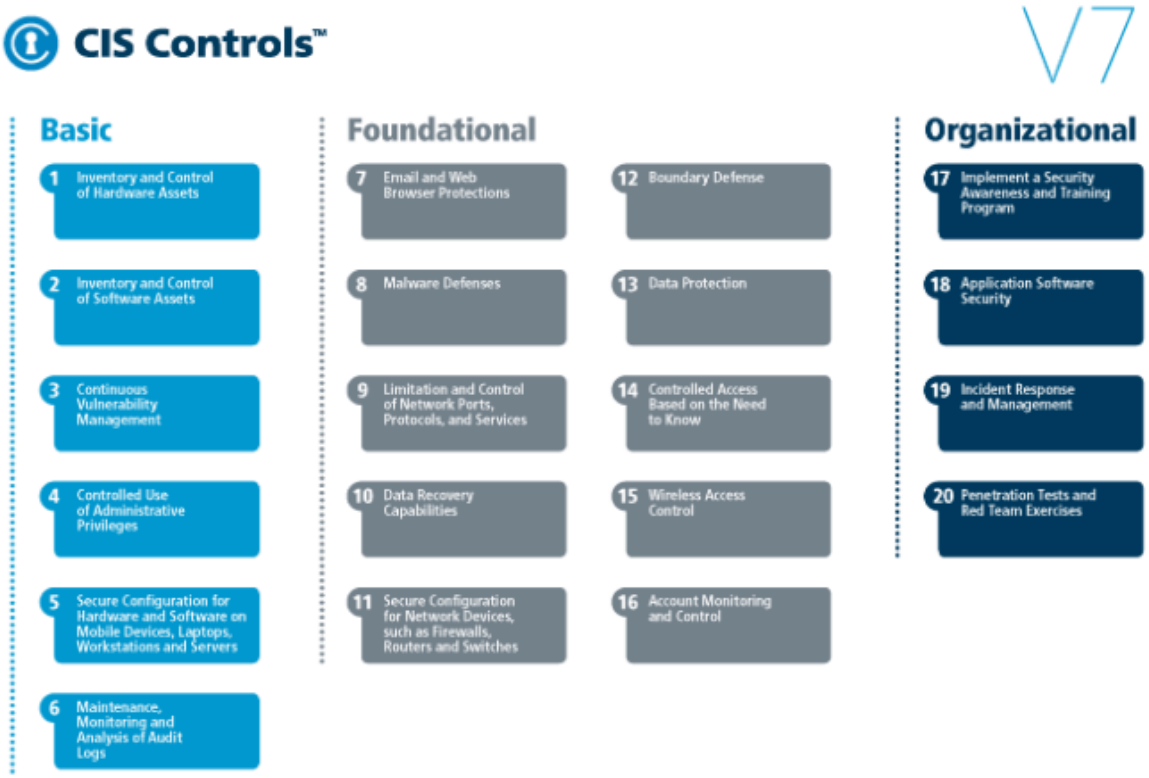


Figura 18: Tipos de Controles CIS
Fuente: (CIS, 2018)

Se dice que la ejecución del inventario de activos (Controles CIS 1 y 2) y las configuraciones estándar (Control 3), son para ahorros costes generales para la empresa, ya que se requieren menos sistemas y administradores de red para gestionar el entorno de ciberseguridad de la organización. El coste de implementación de los controles CIS será proporcional al tamaño de la organización y acorde a las necesidades de cada una de ellas.

- **CSC 1: Inventario de dispositivos autorizados y no autorizados**. El objetivo de este control es ayudar a las organizaciones a definir una línea de base de lo que se debe defender. Este proceso de inventario debe ser lo más completo posible. Después de que una organización haya inventariado con precisión sus sistemas, el siguiente paso es evitar que los dispositivos no autorizados se unan a una red, aquí es

donde se destaca la implementación de la autenticación a nivel de red.

- **CSC 2: Inventario de software autorizado y no autorizado.** El objetivo de este control es garantizar que solo se permite la ejecución de software autorizado en los sistemas de información de una organización, de esta forma se puede evitar que programas maliciosos sean cargado en nuestro sistema afectando al mismo. Este esfuerzo requerirá que una organización reconsidere sus modelos operativos: los usuarios ya no podrán instalar el software cuando y donde quieran.
- **CSC 3: Configuraciones seguras de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.** La mayoría de los sistemas tecnológicos se instalan con un enfoque en la facilidad de uso y no necesariamente en la seguridad. Los sistemas pueden tener la capacidad de ser protegidos, pero es probable que existan configuraciones que un sistema debe tener para garantizar una alta seguridad.
- **CSC 4: Evaluación continua de la vulnerabilidad y remediación.** El objetivo de este Control es comprender las debilidades técnicas del software que existen en los sistemas de información de una organización y eliminar o remediar esas debilidades, para esto se puede utilizar los parches de software que cubren vulnerabilidades tanto de sistemas operativos como de aplicaciones de terceros, también las organizaciones deben implementar un sistema comercial de administración de vulnerabilidades para darse la posibilidad de detectar dónde existen vulnerabilidades de software explotables actualmente para que puedan ser remediadas.
- **CSC 5: Uso controlado de privilegios administrativos.** El objetivo de este Control es garantizar que los miembros de la fuerza laboral solo tengan los derechos, privilegios y permisos del sistema que necesitan para realizar su trabajo, es decir no todos deben tener el dominio del

sistema completo incluyendo de administrador de dominio. El uso de este control elimina permisos o permisos innecesarios del sistema, dando privilegios de acorde al cargo.

CAPÍTULO 3
MODELO DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN OSSTMMv3, NIST SP 800-30 E ISO 27001 PARA CENTROS DE EDUCACIÓN SUPERIOR

En este capítulo se presenta el modelo obtenido acorde a las mejores prácticas de los modelos OSSTMMv3, NIST 800-30 y el estándar ISO 27001. Se plantea en base a resultados obtenidos del estudio de una universidad del país en donde se realizaron encuestas a los usuarios de la red de datos, también se hicieron visitas insitu para determinar las vulnerabilidades de la red y algunas entrevistas a los encargados del área de TIC`s. En la siguiente figura se puede ver el esquema del modelo propuesto para el desarrollo del Modelo de Seguridad de la Información.

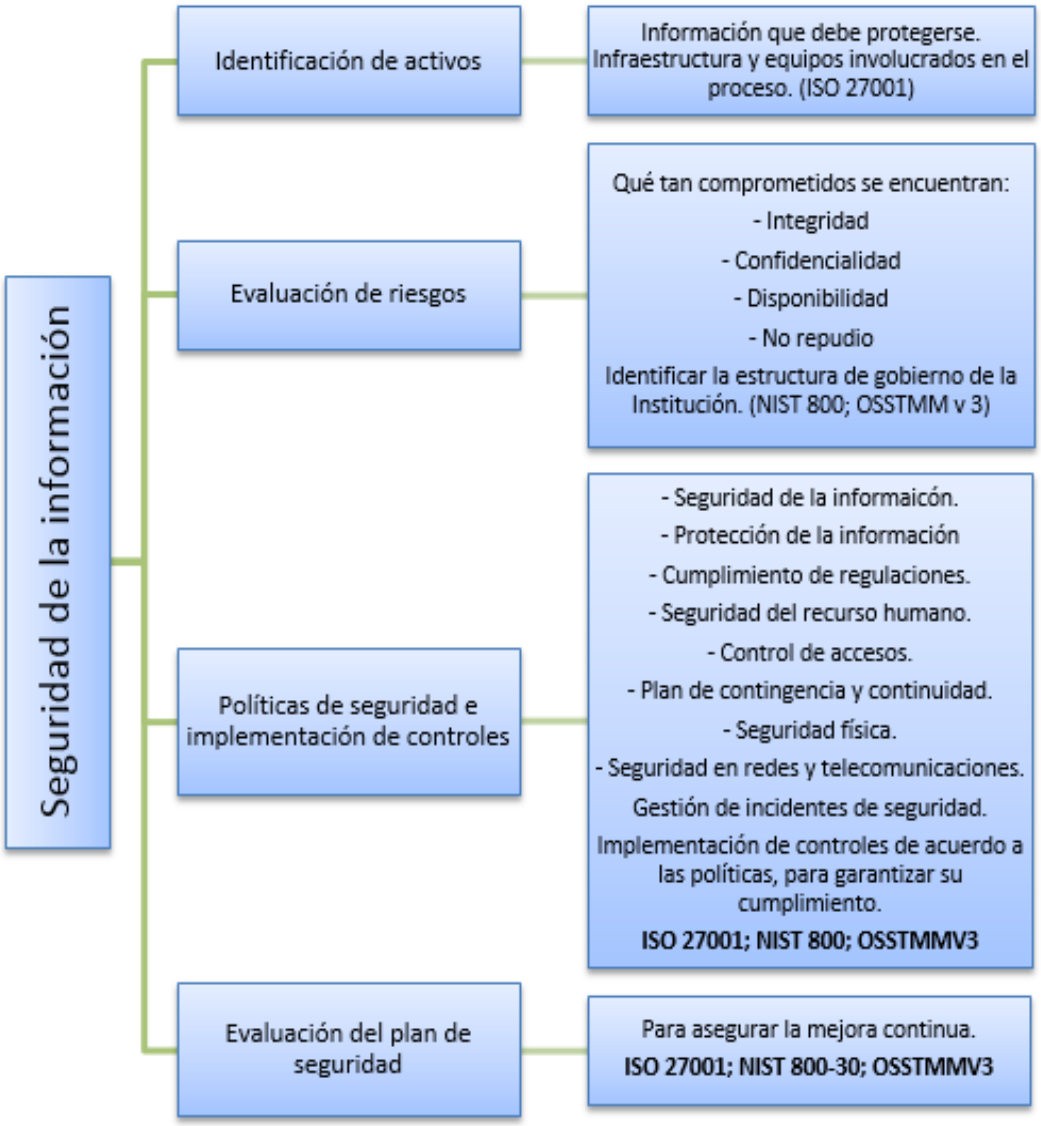


Figura 19: Esquema para el desarrollo del Modelo de Seguridad de la Información en un centro de educación superior

Fuente: El Autor

El desarrollo del plan de seguridad se fundamenta en los análisis del tratamiento del riesgo, basados en las amenazas y vulnerabilidades detectados en la fase del análisis situacional realizado en la Universidad.

Todas las políticas de seguridad se derivan de la norma ISO 27001, tomándose en cuenta, además, las recomendaciones de la norma NIST 800 y del manual OSSTMM versión 3.

El objetivo principal de la Política de Seguridad de la Información, es que la universidad disminuya las probabilidades de alteraciones de la información que maneja, sea que estas se realicen de manera intencional o accidental.

Los objetivos secundarios de la utilización del modelo de seguridad son:

- Salvaguardar la información que genera la institución, así como los recursos físicos de Tecnologías de la Información que se utilizan para su procesamiento, frente a amenazas de cualquier tipo, para de esta manera asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
- Instaurar las directrices, procedimientos y requisitos necesarios para controlar los accesos indebidos a la red de datos.

3.1. Identificación de activos

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y continuidad, éstos necesitan protección para asegurar las correctas operaciones y continuidad de la institución. La gestión apropiada de los activos es vital para poder mantener una adecuada protección de los activos de la empresa. (Peltier, 2010)

Cada activo debe estar identificado y valorado apropiadamente. Según la ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información), los activos se pueden clasificar en:

- Activos de información: bases de datos; archivos de estudiantes, docentes, personal administrativo; documentación del sistema; manuales de usuario, de redes, de revista indexada, de congresos; planes de continuidad, entre otros.
- Documentos impresos: contratos de docentes y personal administrativo, lineamientos, documentos de la institución, proyectos de grado de cada una de las carreras.
- Activos de software: Software de aplicación, software de sistema, herramientas de desarrollo.
- Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros servicios técnicos.
- Personas: Estudiantes, docentes y personal administrativo.
- Servicios: Servicios de computación y comunicación, otros servicios técnicos.

Tabla 5: Activos de la universidad estudiada

Tipo de activo	Posee Universidad
Activos de información	• PEDI • POA
Documentos impresos	• Documentación de la institución. • Carpetas docentes. Contratos de personal docente. • Documentación de revista indexada.
Activos de software	• Software de aplicación y de sistema.
Activos físicos	• 5 laboratorios de informática con un total de 88 computadores personales. • 7 PC en la biblioteca. • Tienen red de VLAN con switch de capa 3. • Cada switch tiene 10 VLAN para dar un total de 120 PC. • Sólo utilizan un servidor para el área financiera-académica que se conecta con el troncal de Ambato. • Tiene 3 edificios en donde funcionan las diferentes carreras.

Personas/usuarios de red	• 837 estudiantes • 52 docentes • 25 personal administrativo
Servicios	• Plataforma Moodle • Correo institucional • Revista científica de la institución con publicación semestral.

Fuente: El Autor

Tabla 6: IP y switch con su ubicación en la Universidad

SWITCHS							
NUMERO	IP	SWITCH	NOMBRE	UBICACIÓN	SERIAL	PRODUCT No	MODEL
1	XXXX	HP-3COM	SW_TUL_DC_R1N_1	DATA CENTER	CN58GP41RM	JG924A	HPE 1920-24G Switch
2	XXXX	HP-3COM	SW_TUL_DC_R1P_2	DATA CENTER	CN56GP51ST	JG925A	HPE 1920-24G-PoE+ (180W)
3	XXXX	HP-3COM	SW_TUL_SP_N_1	LAB - DOCENTES	CN57GP315V	JG923A	HP 1920-16G Switch
4	XXXX	HP-3COM	SW_TUL_SP_N_2	LAB - CONTABILIDAD	CN62GP00L8	JG920A	HPE 1920-8G Switch
5	XXXX	HP-3COM	SW_TUL_SP_N_3	ADMINISTRATIVOS	CN57GP313Y	JG923A	HPE 1920-16G Switch
6	XXXX	HP-3COM	SW_TUL_SP_N_4	DIRECCION1	CN59GP00HT	JG920A	HPE 1920-8G Switch
7	XXXX	HP-3COM	SW_TUL_SP_N_5		CN56GP02MP	JG920A	HPE 1920-8G Switch
8	XXXX	HP-3COM	SW_TUL_SP_N_6	FINANCIERO 1	CN62GP00GF	JG920A	HPE 1920-8G Switch
9	XXXX	HP-3COM	SW_TUL_SP_N_6	FINANCIERO2	CN62GP00GF	JG920A	HPE 1920-8G Switch
10	XXXX	HP-3COM	SW_TUL_SP_N_6	BIBLIOTECA 1	CN62GP00GF	JG920A	HPE 1920-8G Switch
11	XXXX	HP-3COM	SW_TUL_SP_N_6	ED NUEVO	CN62GP00GF	JG920A	HPE 1920-8G Switch
12	XXXX	HP-3COM	SW_TUL_SP_N_6	BIBLIOTECA 2	CN62GP00GF	JG920A	HPE 1920-8G Switch

Fuente: Datos obtenidos del área de TIC de la universidad

Para los activos fijos se basará en la norma ISO 27001, anexo A, Tabla A.1, literal A.8 "Gestión de Activos"; aquí se especifican los requerimientos para establecer, monitorear, revisar, conservar y mejorar los activos de información de la universidad, también especifica los requerimientos para la implementación de controles de seguridad frente a las necesidades de toda la organización, de un proceso específico o un servicio.

3.2. Evaluación de riesgos

De acuerdo con los resultados de las encuestas realizadas a los estudiantes, personal docente y administradores de red de la Universidad; así como de la observación directa del entorno universitario, se han detectado algunas vulnerabilidades en la red de datos de la Universidad. Las vulnerabilidades encontradas se detallan en la siguiente tabla.

Tabla 7: Vulnerabilidades en la red de la información de la Universidad

Vulnerabilidad	Amenazas	Riesgos Potenciales
Hardware		
Falta de equipos reguladores de energía para contingencias con el suministro eléctrico.	Cortes de energía.	Daño en los equipos electrónicos, pérdida de información. Tiempo desperdiciado al repetir el trabajo ya realizado.
Software		
Software con problemas de seguridad	Ataques de inyección de código, errores de integridad de datos, información inconsistente.	Pérdida o modificación de la información, robo de credenciales de acceso (usuario y contraseña)
Actualización de los sistemas operativos en los computadores	Explotación de las debilidades de los sistemas operativos.	Acceso no autorizado a los computadores de los usuarios, con privilegios de administrador
Seguridad Física		
Acceso físico indiscriminado a las oficinas y equipos de cómputo por parte de personal ajeno a las áreas	Acceso directo a información sensible de la Universidad, ataques intencionados a los equipos informáticos	Robo, destrucción, modificación o eliminación de información. Destrucción o daño físico de los computadores.
Seguridad Lógica		
Deficiente control de acceso a los sistemas	Suplantación de identidad	Alteración y/o robo de datos, suplantación de identidad, robo de credenciales. Pérdida de información de interés para la empresa.
Redes de Comunicación		
Vulnerabilidad de navegadores de internet utilizados	Inyección de código SSI, ataques con código XSS	Alteración en el funcionamiento del código, programas y sitios.

Personal		
Usuarios sin capacitación adecuada	Ataques no intencionados, ingeniería social.	Borrado de información, daño al sistema operativo, robo de la información personal.
Falta de políticas claras de seguridad de la información	Ataque intencionados o no intencionados, evasión de responsabilidades	Alteración o pérdida de la información, daños físicos a los elementos constitutivos de la red.

Fuente: El Autor

Una vez identificadas las vulnerabilidades y amenazas, se procede a determinar el impacto de las mismas, y su probabilidad de ocurrencia, de acuerdo a la norma NIST 800 (Determinación de la Probabilidad). Para esto, las amenazas son clasificadas en: altas (son completamente capaces de vulnerar el sistema y los controles son inexistentes o defectuosos), medias (las amenazas son capaces de vulnerar el sistema, pero los controles son efectivos) y bajas (las amenazas no pueden vulnerar el sistema y los controles son efectivos). También se ha considerado el impacto que pueden causar en el sistema de información, estableciéndose la siguiente categorización: Leve (L), moderado (M) y catastrófico (C).

De acuerdo a lo expuesto anteriormente, se procedió a elaborar la tabla 31 con las vulnerabilidades de red de la información según la norma NIST 800.

Tabla 8: Vulnerabilidades de la red de la información, probabilidad e impacto según la norma NIST 800

Riesgo	Probabilidad			Impacto		
	A (altas)	**M** (medias)	**B** (bajas)	**L** (leve)	**M** (moderado)	**C** (catastrófico)
Hardware						
Falta de equipos reguladores de energía						
Software						
Sistemas sin restricción de acceso						
Falta de control de actualización de software						
Seguridad Física						
Pocos controles de restricción de acceso a los computadores						
Falta de seguridad en el entorno de trabajo						
Falta de control de acceso físico a las oficinas						
Seguridad Lógica						
Deficiente control de acceso de los usuarios						
Redes y Comunicaciones						
Vulnerabilidad de los navegadores de internet						
Uso de aplicaciones poco confiables para el intercambio de información						

Personal						
Usuarios no capacitados adecuadamente						
Falta de políticas de seguridad						

Fuente: El Autor

3.2.1. Construcción de la Matriz de Riesgos con flujo de calor para la Universidad en estudio.

Las consideraciones para la probabilidad de amenaza son las siguientes:

- Interés por parte de individuos externos.
- Nivel de vulnerabilidad.
- Frecuencia con que ocurren los incidentes.

La probabilidad de amenaza se valora así:

- Baja: Existen condiciones que hacen muy lejana la posibilidad de ataque.
- Media: Existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo a largo plazo.
- Alta: El ataque es inminente. No existen condiciones internas o externas que impidan el desarrollo del ataque.

Las consideraciones para valorar el impacto son las siguientes:

- ¿Quién sufrirá el daño?
- Incumplimiento de confidencialidad (interna y externa).
- Incumplimiento de obligaciones jurídicas (contratos, convenios).
- Coste de recuperación (imagen, emocional, recursos).

El impacto de un ataque se valora de la siguiente manera:

- **Leve:** Daño aislado, no perjudica a ningún componente de la organización.
- **Moderado:** Provoca la desarticulación de un componente de la organización. A largo plazo puede provocar la desarticulación de la organización. Este impacto puede ser tratado, mejorado y así no perjudica a la institución.
- **Severo:** En corto plazo inmoviliza o desarticula a la organización. Es causa de la banca rota de varias empresas.

De acuerdo con lo expuesto, se ha procedido a dar un valor numérico, tanto a los rangos de probabilidad, como al impacto, así:

PROBABILIDAD	IMPACTO
1 Baja	1 Leve
2 Media	2 Moderado
3 Alta	3 Severo

Se construye una matriz con estas ponderaciones, de tal manera que se pueda obtener el producto de probabilidad e impacto, y se procede a realizar un cruce de información de las dos variables.

Tabla 9: Cruce de información entre impacto y probabilidad

	PROBABILIDAD			
IMPACTO		Baja (1)	Media (2)	Alta (3)
	Leve (1)	Leve-Baja	Leve-Media	Leve-Alta
	Moderado (2)	Moderado-Baja	Moderado-Media	Moderado-Alta
	Severo (3)	Severo-Baja	Severo-Media	Severo-Alta

Fuente: El Autor

Dado que el producto más alto es 9 (combinación alta probabilidad, impacto severo), este valor se toma como 100% de riesgo.

Las ponderaciones de riesgo, en porcentaje, se realizan multiplicando los valores asignados de cada probabilidad, con los valores asignados a cada nivel de impacto y dividiendo este producto para 9.

Para la generación de un mapa de calor, se utilizan los colores del semáforo (utilizados internacionalmente, por lo que es fácilmente entendible), y se estratificas lo valores en tres categorías:

- Color verde (riesgo bajo), para lo valores menores a 33%.
- Color amarillo (riesgo mediano), para los valores entre 34% y 66%.
- Color rojo (riesgo alto), para los valores superiores a 66%

La ponderación de los parámetros utilizados para realizar la matriz de riesgos en la Universidad, así como los colores asignados a cada uno ellos, en la misma matriz, siguen los lineamientos expuestos anteriormente.

A más de las entrevistas y encuestas realizadas, también se tomaron en cuenta registros de percances anteriores al estudio, sufridos por la Universidad.

En la siguiente tabla se puede visualizar una parte de la Matriz de Riesgos para la institución. En el Anexo 1 se encuentra la tabla completa.

		PROBABILIDAD		
IMPACTO		B (1)	M (2)	A (3)
	L (1)	11%	22%	33%
	M (2)	22%	44%	66%
	S(3)	33%	66%	100%

L = Leve
M = Medio
S = Severo

B = Baja
M = Media
A = Alta

Tabla 10: Matriz de riesgo para la universidad en estudio

No.	IDENTIFICACIÓN DEL RIESGO								
	TIPO DE RIESGO (F=Funcional, O=Organizacional)	RIESGO	ORIGEN	Tipo		¿Qué afecta?			CONSECUENCIAS
				Interna	Externa	Confidencialidad	Integridad	Disponibilidad	
R1	F	Pérdida de Datos y/o daños en equipos de cómputo	Suministro Eléctrico	X				X	Por la forma abrupta que se va la energía se puede: 1. Dañar los dispositivos de la red, como: disco duro, memorias, servidores, entre otros. 2. Perder la información que no fue guardada.
R2	F O	Inestabilidad en la plataforma virtual	Funcionamiento inadecuado de la plataforma virtual	X			X	X	1. Pérdida de tiempo de los estudiantes. 2. Sobrecarga de servidor y capacidad de canal. 3. Malestar entre los usuarios.
R3	F	Pérdida del servicio	Saturación de la capacidad del canal. Ataque de negación de servicio. Actividad ilegal en la red.	X		X	X	X	1. Los datos no están disponibles a todo momento. 2. Mala imagen para los usuarios. 3. Pérdida de información.
R4	F O	Alteración y/o pérdida de la información por deficiencias en los controles de acceso físicos y lógicos a los servidores.	Accesos ilegales Políticas permisivas de acceso Falta de seguridad física (guardias, acceso restringidos, entre otros)			X	X	X	1. Accesos no autorizados. 2. Accesos autorizados concurrentes. 3. Vulnerabilidad del sistema informático.
R5	O	Fuga de información	Procesos internos no establecidos (ejemplo: gente va a comprar un derecho y no encuentra el proceso adecuado, no se puede hacer consulta a sus notas y prefiere preguntar verbalmente a su docente)		X	X			1. Inconformidad del usuario de la red 2. Publicidad negativa
R6	F	Pérdidas de datos	Falta de políticas y procedimientos de respaldo de información o backup	X			X	X	1. Información desactualizada ante incidentes de seguridad 3. Alteración de la información 2. Pérdida de datos 3. Descontento de los usuarios

Fuente: El Autor

3.3. Políticas de seguridad de la información de la institución superior

De acuerdo con los resultados del análisis de vulnerabilidades, se ha procedido a elaborar el siguiente esquema de políticas de seguridad de la información, que se sugiere que se implemente en la Universidad caso de estudio.

Figura 14: Políticas de seguridad para la Universidad estudiada
Fuente: El Autor

El establecimiento de políticas institucionales de seguridad de la información, es uno de las primeras recomendaciones de la norma ISO 27001, específicamente el anexo A.5.1 Dirección de gestión de seguridad información establece que el objetivo de la misma es "proporcionar dirección y soporte a la gestión de seguridad de la información, de acuerdo con los requisitos del negocio, las leyes, y reglamentos pertinentes."

En base a la mencionada norma se formulan las siguientes políticas institucionales:

Política 1: Organización de la seguridad de la información

Basada en el anexo A.5.1.1 de la norma ISO 27001. Se establece:

1.1 Creación de un comité de seguridad de la información.
1.2 Aprobación y revisión por parte de la Dirección.

Política 2: Protección de la información

Basada en el anexo A8 "Gestión de activos" de la norma ISO 27001

2.1 Levantamiento del inventario de activos de la empresa. (A.8.1.1 Inventario de activos)
2.2 Establecimiento de reglas de uso de los activos de la empresa. (A.8.1.2 Propiedad de los activos)
2.3 Designar responsables de la información.
2.4 Administración del riesgo en la seguridad de la información.
2.5 Definición de niveles de confidencialidad. (OSSTMM 8.15)
2.6 Destrucción segura de la información. (A.8.3.2 Eliminación de los medios)
2.7 Gestión del uso de medios removibles. (A.8.3.1 Gestión de medios extraíbles)

Política 3: Cumplimiento de regulaciones

Basada en el anexo A.18 "Cumplimiento" de la norma ISO 27001

3.1 Concordancia con leyes y reglamentos vigentes, sobre todos los aspectos relacionados con las redes de información. (A.18.1.1 Identificación de la legislación aplicable y de los registros contractuales)
3.2 Uso de software e información propietaria. (A.18.1.2 Derechos de propiedad intelectual)
3.3 Restricciones en el uso de datos personales. (A.18.1.4 Protección y privacidad de la información de carácter personal)

Política 4: Seguridad en el recurso humano

Basada en el anexo A.7 "Seguridad en recursos humanos" de la norma ISO 27001, y en el capítulo 7 del manual OSSTMM v3.

4.1 Capacitación y creación de una cultura de seguridad de la información. (A.7.2.2 Concienciación, educación y formación en seguridad de la información) (OSSTMM 7.1.3; 7.1.4; 7.1.5)
4.2 Acuerdos de confidencialidad. (A.7.3.1 Responsabilidades ante la finalización o cambio de empleo) (OSSTMM 7.1.1; 7.1.2)
4.3 Requisitos de seguridad en contratos con terceros. (OSSTMM3 7.10.1; 7.10.2; 7.10.3)

Política 5: Control de accesos

Basada en el anexo A.9 "Control de acceso" de la norma ISO 27001

5.1 Definición de perfiles de acceso, asignación y retiro de privilegios.(A.9.2.1)
5.2 Revisión periódica de privilegios de acceso.(A.9.2.2)

5.3 Identificación y autenticación de usuarios en recursos informáticos.(A.9.2.3)
5.4 Uso personalizado del identificador de usuario.(A.9.2.4)
5.5 Determinación de usuarios privilegiados y usuarios genéricos. (A.9.4.1)
5.6 Conexión segura de terceros a la red.(A.9.4.2)
5.7 Acceso restringido a servicios de Internet.
5.8 Las contraseñas deben ser interactivas, cambiar periódicamente y ser la combinación de letras, números y caracteres especiales. (A.9.4.3)

Política 6: Plan de contingencia y continuidad

Basada en el capítulo 7 del manual OSSTMM v3.

6.1 Seguridad del plan de contingencia y continuidad.
6.2 Usuarios de contingencia. (OSSTMM 7.4; 7.5)
6.3 Respaldo de información crítica. (OSSTMM 7.4; 7.5)
6.4 Pruebas sobre el plan de contingencia y continuidad. (OSSTMM 7.6

Política 7: Seguridad Física

Basada en el anexo A.11 "Seguridad física y del entorno" de la norma ISO 27001 y en el capítulo 8 del manual OSSTMM.

7.1 Control de acceso y perímetro de las instalaciones.(A.11.1.1 Perímetro de seguridad física)
7.2 Gestión de amenazas ambientales.(A.11.1.4; OSSTMM 8.2.1)
7.3 Manejo de áreas de carga y descarga.(A.11.1.6)
7.4 Protección física de equipos de cómputo.(A.11.1.3)
7.5 Seguridad en el cableado.(A.11.2.3)
7.6 Protección contra fallos del suministro eléctrico.(A.11.2.2)

Política 8: Seguridad en redes y telecomunicaciones

Basada en el anexo A.13 "Seguridad en las comunicaciones" de la norma

ISO 27001 y en el capítulo 10 del manual OSSTMM v3.

8.1 Segmentación de redes y control de enrutamiento en la red.(A.13.1.3; OSSTMM 10.1.6)
8.2 Intercambio de información con terceros.(A.13.1.2; OSSTMM 10.2.1)
8.3 Uso de barreras de comunicaciones.(A.13.1.1; OSSTMM 10.2.2)
8.4 Seguridad en el correo electrónico.(A.13.2.3)

Política 9: Gestión de incidentes en la seguridad de la información

Basada en el anexo A.16 "Gestión de incidentes de seguridad de la información" de la norma ISO 27001

9.1 Designación de responsables del sistema de seguridad de la información.(A.16.1.1)
9.2 Reporte de incidentes de seguridad de la información.(A.16.1.2)
9.3 Reporte de debilidades de la seguridad de la información.(A.16.1.3)
9.4 Recopilación de evidencias.(A.16.1.7)
9.5 Valoración de impacto en incidentes de Seguridad de la información.(A.16.1.4)

3.4. Implementación de controles

De acuerdo las políticas establecidas, se procede a establecer los controles respectivos, para asegurar el cumplimiento de las mismas.

3.4.1. Controles de Seguridad Lógica

a) Identificación

Para que un usuario pueda tener acceso al sistema de información financiero o académico, debe establecerse un procedimiento formal y por escrito que normalice y exija el ingreso de los siguientes datos:

- ID de usuario, valor alfanumérico único.

- Contraseña, la cual debe ser personal e intransferible.
- Nombres y apellidos completos.
- Grupo de trabajo al que pertenece el usuario.
- Tiempo de expiración de la contraseña.
- Contador de intentos fallidos.
- Autorización de ingreso al área de usuarios.

Los permisos asignados deben ser los mínimos y necesarios para que el usuario realice de manera correcta su labor diaria dentro dela Universidad.

El acceso al sistema y el uso de recursos de la red de datos de la Universidad, deben tener horarios establecidos, considerando lo siguiente:

- No debe ser posible acceder a las cuentas de usuario en horarios no laborales, salvo previa autorización.
- Durante las vacaciones o licencias de los propietarios de las cuentas, estas deben desactivarse.

La contraseña asociada al ID de usuario para el acceso a un computador, es la primera verificación de su identidad, lo que permitirá, en primera instancia, acceder al computador y a la información. Para resguardar los recursos de la Universidad, la contraseña debe ser secreta, personal e intransferible.

El departamento de Talento Humano deberá comunicar cualquier cambio en la nómina de empleados, luego de esta notificación, el administrador del sistema debe revocar los permisos de la cuenta, o desactivarla.

Los computadores deben tener configurado su sistema operativo, el cierre de sesión luego de cinco minutos de inactividad. Se debe desactivar en los computadores, los usuarios genéricos.

Se prohíbe el uso de cuentas invitado; todos los usuarios deben acceder a las computadoras con su ID y contraseña.

Se debe minimizar el uso de perfiles de usuarios con privilegios de administrador. Estos privilegios sólo deben otorgarse a aquellos usuarios que son directamente responsables de la seguridad de los sistemas.

Los propietarios de las cuentas de usuario, deben dejar constancia por escrito, que conocen y acatan las políticas y procedimientos de seguridad, así como su responsabilidad en el uso de las mismas.

b) Contraseñas

De acuerdo con las buenas prácticas de seguridad, las contraseñas utilizadas deben reunir las siguientes características:

- Tener una longitud mínima de 8 caracteres.
- Contener una combinación de caracteres alfanuméricos y no alfanuméricos. (combinando mayúsculas y minúsculas)
- Sistemas y aplicaciones de la Universidad que contengan información crítica, requieren el cambio de contraseña al menos cada 90 días.
- La nueva contraseña debe ser distinta a por lo menos las últimas 3 utilizadas.
- Se debe bloquear el perfil de todo usuario que ha fallado en autenticarse por más de tres veces, de forma consecutiva.
- Todo usuario nuevo, debe cambiar la contraseña proporcionada por el administrador, en el primer inicio de sesión.
- El usuario es responsable del almacenamiento y manejo de su contraseña.
- Las contraseñas predefinidas que tienen los nuevos equipos de TI, deben ser cambiados antes de ponerlos en producción.

3.4.2. Controles para la Seguridad en la Red de datos

Topología de red

Se debe considerar una arquitectura de red que beneficie o que sea acorde a las necesidades de la institución. Esta puede ser cambiante dependiendo de la cantidad de dispositivos que posee la red. Se debe considerar lo siguiente:

- Deberá existir documentación detallada de todo lo relacionado con la implementación física de la red.
- Se debe implementar redundancia en las vías de comunicación, ante la eventualidad de un fallo en el medio principal de comunicación.

Red de datos

Se debe recopilar la siguiente información:

- Capacidad de canal, contratado y utilizado.
- Tráfico generado por las aplicaciones.
- Estado de cada aplicación.
- Intentos de intrusión.

Las actualizaciones y nuevas instalaciones de software que se realicen en los equipos de red, así como los cambios de direccionamiento IP y las reconfiguraciones de los equipos de ruteo, deben ser documentadas y aprobadas.

Propiedad de la información

Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, deben considerarse como propiedad de la Universidad.

Uso de los sistemas de comunicación

Los recursos de la red de información de la Universidad, sólo deben utilizarse para actividades de trabajo. El uso personal de los mismos no es permisible.

Conexiones Externas

- Se debe asegurar el tráfico entrante y saliente de la red interna, este debe ser filtrado y controlado por un firewall, prohibiendo el tráfico que no se encuentre expresamente autorizado.
- El uso de Internet debe ser monitoreado constantemente.

Configuración lógica de la red

Cuando sea necesario conectar a la red algún equipo ajeno a la misma, se debe considerar lo siguiente:

- No identificarse como un usuario de la red.
- No ejecutar programas de monitoreo de tráfico, sin la debida autorización explícita de la Dirección y la aprobación el administrador de la red.
- No agregar ningún dispositivo que amplíe la infraestructura de la red, sin previa autorización.
- Asegurar la confidencialidad del direccionamiento IP de la red de información de la Universidad.

Antivirus

Todos los computadores de la Universidad deben tener instalado y ejecutándose, un antivirus corporativo, debidamente actualizado. El antivirus seleccionado debe cumplir con lo siguiente:

- Detectar y controlar cualquier acción realizada por un software malicioso, en tiempo real.
- Ejecutar periódicamente una exploración de todas las unidades de almacenamiento de la estación de trabajo, para detectar software malicioso.
- Actualizar su base de datos diariamente.
- Debe ser un producto totalmente legal. (con licencia o software libre)

Los dispositivos externos no deben ser utilizados en las computadoras de la Universidad, a menos que sea absolutamente necesario y hayan sido previamente escaneados por un antivirus.

Firewall

Se debe instalar un firewall en la red de la Universidad, el cual debe presentar, de manera predeterminada, una política de negación total. De esta manera, se habilitarán únicamente los servicios y puertos que se vayan a utilizar.

El departamento de TIC´s debe controlar periódicamente la configuración del firewall y los servicios de red, documentando dicho proceso.

Ataques de red

Para minimizar los ataques por la red de información, se deben tomar las siguientes acciones:

- Toda la información que se transmita por la red deberá encriptarse, o viajar en formato no legible.
- La red debe ser monitoreada constantemente para detectar infiltraciones.
- Se debe segmentar la red, de manera física o lógica, para disminuir el riesgo de sniffing.

- Las reglas del firewall deben ser diseñadas cuidadosamente, para evitar infiltraciones.

3.4.3. Controles para la Seguridad de las Aplicaciones

a) **Software**

No deben utilizarse aplicaciones descargadas de Internet, a menos que estas sean aprobadas por el departamento de TIC´s, ya que estas pueden contener código malicioso que vulnere las seguridades de la red.

La Universidad debe contar con software legal, es decir, debe adquirir las licencias del todo el software que utilice en sus actividades diarias. Se prohíbe estrictamente la instalación de software no autorizado. Si se requiere la instalación de software libre, este debe ser analizad previamente por el departamento de TIC´s.

b) **Control de aplicaciones en las computadoras**

Para mantener la seguridad de las estaciones de trabajo, se deben seguir las recomendaciones siguientes:

- Debe generarse un procedimiento donde se especifique qué aplicaciones deben instalarse, de acuerdo con el perfil de cada usuario, así como la frecuencia de actualización de dichas aplicaciones.
- Se deben realizar respaldos periódicos de la información de los equipos.
- Se debe documentar los procesos de instalación, mantenimiento y reparación de todos los equipos.
- Se debe notificar a los nuevos usuarios, acerca de las restricciones en la instalación de software no autorizado por el departamento de TIC´s.

c) **Control de datos en las aplicaciones**

Los archivos de datos generados en el trabajo diario, deben ser almacenados en directorios protegidos mediante el establecimiento de controles de acceso, y sólo el administrador de sistemas tendrá acceso a ellos.

3.4.4. Controles para la Seguridad Física

Los recursos de TIC´s, tanto físicos como lógicos de la Universidad, sólo deben usarse en un entorno seguro, para conseguir esto se deben considerar los siguientes aspectos:

- No debe modificarse la configuración, hardware y software, de los equipos, establecida por el departamento de TIC´s.
- Está prohibido fumar o comer en las estaciones de trabajo.
- Se debe proteger a los equipos de los riesgos de entorno. (polvo, incendios, agua)
- Los equipos no pueden ser reubicados o movidos sin permiso. Para llevar un equipo fuera del campus universitario, se requiere una autorización escrita.
- La pérdida o robo de cualquier componente de hardware o software, debe ser reportada inmediatamente.

Cualquier inconveniente en las computadoras o en la red debe reportarse rápidamente, para evitar problemas serios como pérdida de la información o indisponibilidad de los servicios.

3.4.4.1 Control de acceso físico a los equipos

Tanto las estaciones de trabajo, como el back bone de la red deben tener acceso restringido, para minimizar los riesgos de ataques internos. Se deben seguir las siguientes recomendaciones:

- Todo el personal que ingrese a las áreas restringidas, debe estar debidamente identificado y tener la respectiva autorización.

- Sólo los administradores deben tener acceso al back bone de la red.

3.4.4.2 Control de acceso a los equipos

Los siguientes controles de seguridad deben ser activados en todas las estaciones de trabajo, con el fin de protegerlas contra el robo de la información.

- Configurar el uso de contraseñas para proteger el teclado y la pantalla, cuando el equipo entre en modo de ahorro de energía, este debe activarse luego de un período de inactividad de 5 minutos.

3.4.4.3 Dispositivos de soporte

La Universidad debe contar con los siguientes dispositivos de soporte:

- Aire acondicionado en el back bone de la red para que el ambiente se mantenga a una temperatura entre 19° C y 20° C.
- Extintor de incendios, preferentemente de polvo químico, que cumpla las especificaciones para equipamiento eléctrico y de computación. En el centro de datos debe existir un extintor para uso exclusivo del centro.
- Alarmas contra intrusos: Deben ser activadas en horarios no laborables y deben permitir la activación manual en horarios laborables.
- UPS: Deberá existir al menos una UPS en el centro de datos, que atienda a los equipos de misión crítica, con la capacidad suficiente para permitir un apagado seguro de los equipos.
- Luz de emergencia: Deberá existir una luz de emergencia que se active automáticamente ante una contingencia.

3.4.4.4 Cableado estructurado

Se recomienda que el cableado actual de la red, cumpla los

estándares de cableado estructurado, para lo cual:

- Se deberá documentar en planos, los canales de tendido de cables y los puntos de red existentes.
- Deberá medirse periódicamente la capacidad de canal ocupado. Si esta excede el mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- Ante un corte del suministro de energía eléctrica, deberán apagarse los equipos del centro de datos de manera segura, como medida de prevención.

3.4.5 Controles de Seguridad Física y del Entorno

Las vulnerabilidades con respecto a la seguridad física tienen relación con la destrucción física, intrusos, problemas del entorno, que ocasionen daños inesperados a los equipos.

Instalaciones

Sólo la persona administradora de la red debe poseer la llave para abrir la puerta de acceso al back bone de la red, de esta manera se llevará el control y registro de lo que va hacer cada persona que entra ahí. La seguridad física deberá ser complementada con la seguridad contra fuego.

Perímetro de seguridad

Se debe implementar una arquitectura de seguridad basada en el uso de firewalls para establecer una zona de seguridad perimetral, como primera defensa en caso de ataques informáticos.

Controles físicos de entradas: Es importante contar con controles de acceso físico para resguardar todos los activos de la Universidad, estos deben:

- Supervisar a los visitantes de la Universidad y registrar la hora de su ingreso y salida.

Mantenimiento de equipos: Se debe realizar un mantenimiento periódico de los equipos informáticos de la Universidad. Para ello se debe considerar:

- El responsable del departamento de TIC´s de la Universidad debe realizar un cronograma de mantenimiento de los equipos, y llevar un registro de la frecuencia con que debe realizarse dicho mantenimiento, así como del detalle de los mismos.
- Establecer que sólo personal autorizado puede dar mantenimiento a los equipos y realizar tareas de reparación, si estas son necesarias.

3.4.6 Controles de Protección contra Software Malicioso

Controles contra software malicioso

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado.
- Instalar y actualizar periódicamente software de eliminación de virus, examinando computadoras y medios de almacenamiento.
- Mantener los sistemas operativos de las computadoras con las últimas actualizaciones de seguridad disponibles.
- Revisar periódicamente el contenido de software y datos de los equipos que procesan sustentan las actividades críticas de la Universidad, investigando formalmente la presencia de archivos no aprobados, o modificaciones no autorizadas.
- Explorar con antivirus, antes de su uso, cualquier medo removible de datos, o archivos recibidos a través de medos no confiables.
- Concientizar al personal, acerca de los riesgos provocados por virus y malware, y sus posibles consecuencias.

3.4.7 Controles de Gestión de la Seguridad de Red

Controles de red

El responsable del departamento de TIC´s definirá controles para garantizar la seguridad de los datos contra el acceso no autorizado, considerando los siguientes parámetros:

- Salvaguardar la confidencialidad e integridad del procesamiento de los datos.
- Mantener la disponibilidad de los servicios de red y computadoras conectadas.
- Garantizar mediante actividades de supervisión, que los controles se aplican en toda la infraestructura de procesamiento de información.

Gestión de medios removibles

Se deberán considerar las siguientes acciones para la administración de los medios informáticos removibles:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Universidad.
- Almacenar todos los medios en un entorno seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Intercambio de información. Mensajería electrónica

Se debe redactar normas claras con respecto al uso del correo electrónico:

- Todo empleado de la Universidad puede solicitar y disponer de una cuenta de correo electrónico institucional.
- El personal de TIC´s hará la configuración de la cuenta de correo electrónico, en la computadora del empleado solicitante.

- La activación de las cuentas de correo electrónico institucional debe ser centralizada.
- Para activar una cuenta de correo electrónico institucional, se deberá enviar una solicitud por escrito, misma que debe ser debidamente aprobada.
- Cuando un usuario reciba una nueva cuenta de correo electrónico institucional, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación de esa cuenta.
- Cuando un empleado de la Universidad renuncia o es separado de la institución, debe desactivarse la correspondiente cuenta de correo electrónico, para lo cual se requerirá la notificación respectiva por parte del área administrativa.

Dependiendo del software de correo electrónico utilizado por la Universidad, el contenido de los mensajes cursados por los usuarios, pueden ser monitoreados por el administrador. La Universidad debe dejar este aspecto en claro a los estudiantes y empleados, informando así mismo las condiciones que deben cumplirse para que una cuenta de correo electrónico institucional sea monitoreada.

3.4.8 Controles en el uso de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar la seguridad de toda la Universidad, por lo tanto, se controlará el acceso a los servicios de red, tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El administrador de la red es el responsable de otorgar los permisos, tanto a los servicios como a los recursos de la red, únicamente de acuerdo al pedido formal del solicitante. Para ello se desarrollarán procedimientos

para la activación y desactivación de derechos de acceso a las redes, los cuales comprenden:

- Identificar los servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y servicios de red, a los cuales se les otorgará el acceso.

3.4.9. Monitoreo de los Controles de Acceso

Se debe implementar un sistema de monitoreo de red, que proporcione información completa de la actividad de cada usuario conectado a la misma.

Conformidad con la política de seguridad

El responsable de TIC´s realizará revisiones periódicas de todas las áreas de la Universidad, a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, este período como mínimo debe ser cada 6 meses.

3.4.10. Controles de Seguridad de la Red Inalámbrica

Debido a su naturaleza, los enlaces inalámbricos están más expuestos a sufrir ataques informáticos, y constituyen el medio más vulnerable a los mismos. Es por esto que se deben considerar los siguientes aspectos:

- Restringir el tráfico permitido en estos enlaces.
- Forzar el uso de contraseñas seguras.
- Utilizar herramientas (hardware y software) para confinar el alcance inalámbrico al campus universitario.
- Colocar los puntos de acceso únicamente en zonas definidas tras un estudio minucioso.
- Evitar el uso de repetidores por parte del personal ajeno a TIC´s.

- Privilegiar el acceso a la red inalámbrica mediante el registro de direcciones físicas en el router, o mediante software específico.

3.5. Conclusiones

El modelo de seguridad propuesto, pone en evidencia serios factores de riesgo para la seguridad de la información y de la gestión de servicios en la Universidad, haciéndose necesario implementar los correctivos necesarios.

Se han determinado los procesos críticos de la gestión de información en la Universidad. El hallazgo más significativo está relacionado con la falta de políticas de seguridad y documentación de procesos internos.

Las políticas que se utilizaron en el modelo de seguridad están comprometidas con la privacidad y protección de los datos de los usuarios ante acciones ilegales o perjudiciales.

Para identificar las vulnerabilidades internas de la institución se aplicaron procesos técnicos como el mapeo de la red, revisión de puertos que están abiertos, acceso a la red wifi sin claves, no existen VPN's, no hay documentación de la red empresarial; adicionalmente se aplicaron encuestas a los usuarios de la red.

Es importante la utilización del presente modelo de seguridad con el fin de puntualizar el uso adecuado de los activos de la institución, en los que se debe incluir parámetros de seguridad acorde a las necesidades del establecimiento. Adicionalmente, estas deben ser difundidas con el fin de lograr una mayor eficiencia en la mitigación de riesgos dentro de la infraestructura de la red de información.

El aspecto más importante, y que afecta a cualquier modelo de seguridad, es que la Universidad no tiene interiorizado una cultura de seguridad de la información. El desarrollo de este tipo de cultura, es un proceso que se desarrollará de manera continua, aplicando rígidamente las

políticas de seguridad propuestas.

Los incidentes de seguridad se pueden presentar, ya sea por desconocimiento o negligencia de los usuarios de la red, de manera accidental o incluso de forma deliberada (mediante un ataque cibernético), por lo que, el uso del modelo basado en OSSTMMv3, NIST 800-30 e ISO 27001 considera la aplicación de distintas perspectivas para aumentar y mejorar la seguridad de la información, a través de la utilización de estándares y mejores prácticas de los modelos utilizados.

La utilización de los modelos de seguridad OSSTMMv3 y NIST 800-30 son aconsejables por ser más flexibles y se pueden acoplar a las necesidades de una institución, lo que no sucede con el estándar ISO 27001 que es más estricto debiendo llegar a la certificación de la misma, por ello se aconseja que esto se realice desde la matriz y no solo desde una extensión.

ANEXOS

ANEXOS

ANEXOS 1: Matriz de Riesgo obtenida acorde a los resultados de las metodologías aplicadas para obtener información sobre la seguridad actual que tiene la universidad.

No.	IDENTIFICACIÓN DEL RIESGO								
	TIPO DE RIESGO (F=Funcional, O=Organizacional)	RIESGO	ORIGEN	Tipo		¿Qué afecta?			CONSECUENCIAS
				Interna	Externa	Confidencialidad	Integridad	Disponibilidad	
R1	F	Pérdida de Datos y/o daños en equipos de cómputo	Suministro Eléctrico	X				X	Por la forma abrupta que se va la energía se puede: 1. Dañar los dispositivos de la red, como: disco duro, memorias, servidores, entre otros. 2. Perder la información que no fue guardada.
R2	F O	Inestabilidad en la plataforma virtual	Funcionamiento inadecuado de la plataforma virtual	X			X	X	1. Pérdida de tiempo de los estudiantes. 2. Sobrecarga de servidor y capacidad de canal. 3. Malestar entre los usuarios.
R3	F	Pérdida del servicio	Saturación de la capacidad del canal. Ataque de negación de servicio. Actividad ilegal en la red.	X		X	X	X	1. Los datos no están disponibles a todo momento. 2. Mala imagen para los usuarios. 3. Pérdida de información.
R4	F O	Alteración y/o pérdida de la información por deficiencias en los controles de acceso físicos y lógicos a los servidores.	Accesos ilegales Políticas permisivas de acceso Falta de seguridad física (guardias, acceso restringidos, entre otros)			X	X	X	1. Accesos no autorizados. 2. Accesos autorizados concurrentes. 3. Vulnerabilidad del sistema informático.

R5	O	Fuga de información	Procesos internos no establecidos (ejemplo: gente va a comprar un derecho y no encuentra el proceso adecuado, no se puede hacer consulta a sus notas y prefiere preguntar verbalmente a su docente)		X	X			1. Inconformidad del usuario de la red 2. Publicidad negativa
R6	F	Pérdidas de datos	Falta de políticas y procedimientos de respaldo de información o backup	X			X	X	1. Información desactualizada ante incidentes de seguridad 3. Alteración de la información 2. Pérdida de datos 3. Descontento de los usuarios
R7	F O	Afectación a los servicios de tecnología	Mala gestión de la red inalámbrica. falta de controles en la gestión de red inalámbrica.	X		X	X	X	1. Pérdida de datos 2. Alteración de la información 3. Fácil detección de las vulnerabilidades de la red.
R8	O	Suplantación de seguridad	Mala gestión de claves de acceso.	X		X	X		1. Alteración de datos.
R9	O	Acceso físico a los servidores	Falta de controles de seguridad para el acceso al centro de datos	X				X	1. Paralización de la red. 2. Pérdida de datos no respaldados 3. Pérdida de equipos 4. Impacto negativo en la imagen institucional
R10	F	Inestabilidad en la red de datos	Navegación abierta en internet sin restricciones.		X	X	X	X	Descarga de SW malicioso que sature la red. Cuellos de botella en el flujo de trabajo.
R11	F	Fácil escaneo de red	No tener segmentada la red	X		X	X	X	1. Vulnerabilidad general de la red con posible paralización de la misma. 2. Pérdida de información. 3. Formación de cuellos de botella en el flujo de trabajo.

No.	ANÁLISIS DEL RIESGO								PLAN DE TRATAMIENTO DEL RIESGO		
	Probabilidad			Impacto			Resultado	Categoría	Identificación del Control (OSSTMMv3, NIST 800-30, ISO 27001)	Descripción del Plan de Acción	Responsable
	A (3)	M (2)	B (1)	S (3)	M (2)	L (1)					
R1			1	3			33%	BS	Seguridad física del OSSTMMv3	Gestión de niveles de servicio Monitoreo y evaluación de procesos y servicios	Jefe de TI, Rector de la extensión UNIANDES Tulcán
R2		2			2		44%	MM	Nivel físico del OSSTMMv3 NIST 800-30	Una política del sistema de gestión de seguridad de la información. Manual de normas, estándares y políticas de seguridad (gestión de incidentes, acuerdos de confidencialidad, gestión de activos, entre otros). Gestión de la red.	Administradores de la red. Docentes de UNIANDES, extensión Tulcán.
R3		2		3			67%	MS	Seguridad física del OSSTMMv3 Seguridad dela Comunicación ISO 27001, A.9, Control de Accesos	Mecanismos de autenticación. Monitoreo de la red. Mejora de los controles de acceso.	Administradores de la red
R4	3			3			100%	AS	Clase: Seguridad física del OSSTMM3, canal: humano y físico. Clase: Seguridad de las comunicaciones, canal: red de datos	Delimitar áreas restringidas. Contratar personal de seguridad. Monitoreo y gestión de red, incluyendo SW y equipo especializado	Decanos de las diferentes facultades de la Uniandes extensión Tulcán. Administradores de red.
R5		2		3			67%	MS	Seguridad de la información de la ISO 27001, A.16. Clase: Seguridad en las comunicaciones, canal: telecomunicaciones y redes de datos	Mejorar la capacidad de canal entre la Matriz de Ambato y su extensión en Tulcán. Controles de acceso.	Administradores de la red. Rector de la UNIANDES extensión Tulcán. Secretaria

R6		2			2		44%	MM	Seguridad de la información de la ISO 27001, A.16. Definición de políticas de seguridad ISO 27001, A.5.1.1 NIST 800-30	Definir políticas de seguridad institucional Definir un proceso de respaldo de la información Adquisición y mantenimiento de equipos de respaldo de información. Asegurar de que los respaldos se realicen con periodicidad adecuada.	Administradores de red. Consejo Directivo y Rector de la UNIANDES, extensión Tulcán
R7	3			3			100%	AS	Clase: Seguridad inalámbrica, canal: inalámbrico de la OSSTMMv3 Seguridad de la información de la ISO 27001, A.16	Aplicar técnicas de seguridad inalámbrica (acceso por dirección MAC, deshabilitación SSID, restricción de los acceso a los recursos de las conexiones inalámbricas).	Administradores de red.
R8			1	3			33%	BS	Seguridad de la Información ISO 27001, A.16 Control de accesos ISO 27001, A.9	Uso permanente de herramientas de análisis de red. Determinar sanciones para el incumplimiento de los procedimientos de seguridad establecidos	Consejo Directivo, Rector de la UNIANDES extensión Tulcán. Administradores de Red.
R9			1	3			33%	BS	Clase: Seguridad física del OSSTMM3, canal: humano y físico.	Definir áreas de acceso restringido Implementación de seguridad física	Rector de UNIANDES, extensión Tulcán. Administrador de Red
R10		2		3			67%	MS	Clase: seguridad de las comunicaciones, canal: redes de datos según OSSTMM3	Uso de SW especializado en detección y eliminación de SW malicioso.	Administradores de redes, Docentes de la universidad
R11		2		3			67%	MS	Seguridad de la información 27001, A.16 NIST 800-30 Clase: Seguridad de las comunicaciones, canal: redes de datos según el OSSTMMv3	Uso adecuado de SW de análisis y gestión de red (Wireshark, Netcut, Kali Linux, entre otros)	Rector de la institución. Personal de TIC

Fuente: El Autor

ANEXO 2: Datos obtenidos de la Universidad que sirvieron para determinar las mejores prácticas para el modelo de seguridad que puede ser utilizado en las instituciones.

Pregunta	Respuesta		Porcentaje		Total de encuestados
	SI	NO	SI	NO	
¿Alguna vez ha tenido que repetir un proceso porque su información se perdió en la red?	194	88	69%	31%	282
¿Alguna vez no pudo acceder al sistema, aunque proporcione el usuario y contraseña correctos?	198	84%	70%	30%	282
¿Alguna vez han tenido problemas de consistencia con sus calificaciones?	158	124	56%	44%	282
¿La Universidad utiliza "identidades federadas"?	27	255	10%	90%	282
¿Su departamento cuenta con procedimientos a seguir en caso de detectarse una falla en el sistema informático?	16	16	50%	50%	32
¿Comparte con alguien sus credenciales de acceso a la red de datos de la Universidad?	8	24	25%	75%	32
¿Alguna vez ha tenido algún problema con el sistema informático?	18	14	56%	44%	32
¿Cambian con frecuencia sus credenciales de acceso a la red de la Universidad?	11	21	34%	66%	32
Cuando navega en internet ¿Tiene alguna restricción en las páginas, o contenido que explora?	91	191	33%	67%	282

De toda la metodología aplicada para obtener información de las vulnerabilidades de la universidad se tienen las siguientes conclusiones:

- No tienen restricciones al momento de utilizar el internet.
- Manejo inapropiado de usuarios y contraseñas de la red de datos.
- Uso inadecuado de las plataformas de la institución, tanto de docentes como de estudiantes.

- Los datos que genera la red no tienen sus debidos respaldos en tiempos adecuados.
- La mayor parte de los computadores son usados por varias personas, incluyendo los de uso exclusivo de docentes.
- Acceso inadecuado al cuarto de servidores.
- Inconformidad de los usuarios de la red con el sistema académico y plataforma.
- No existe una cultura de seguridad en el manejo de la red de información por parte de sus usuarios.
- No hay herramientas adecuadas para el análisis de seguridad de la red de información.

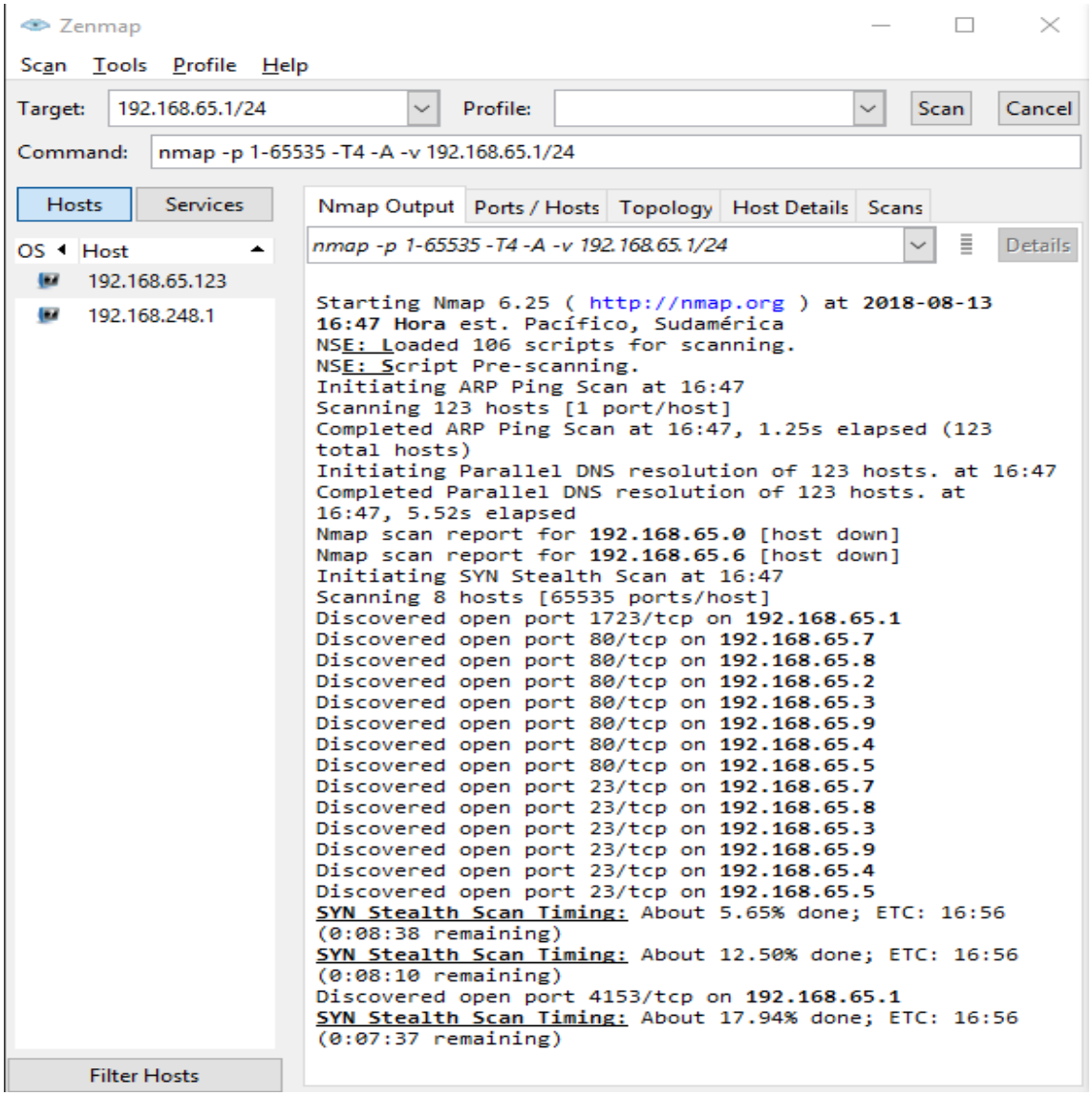
ANEXO 3: Estado actual del cableado estructurado de datos de la universidad.

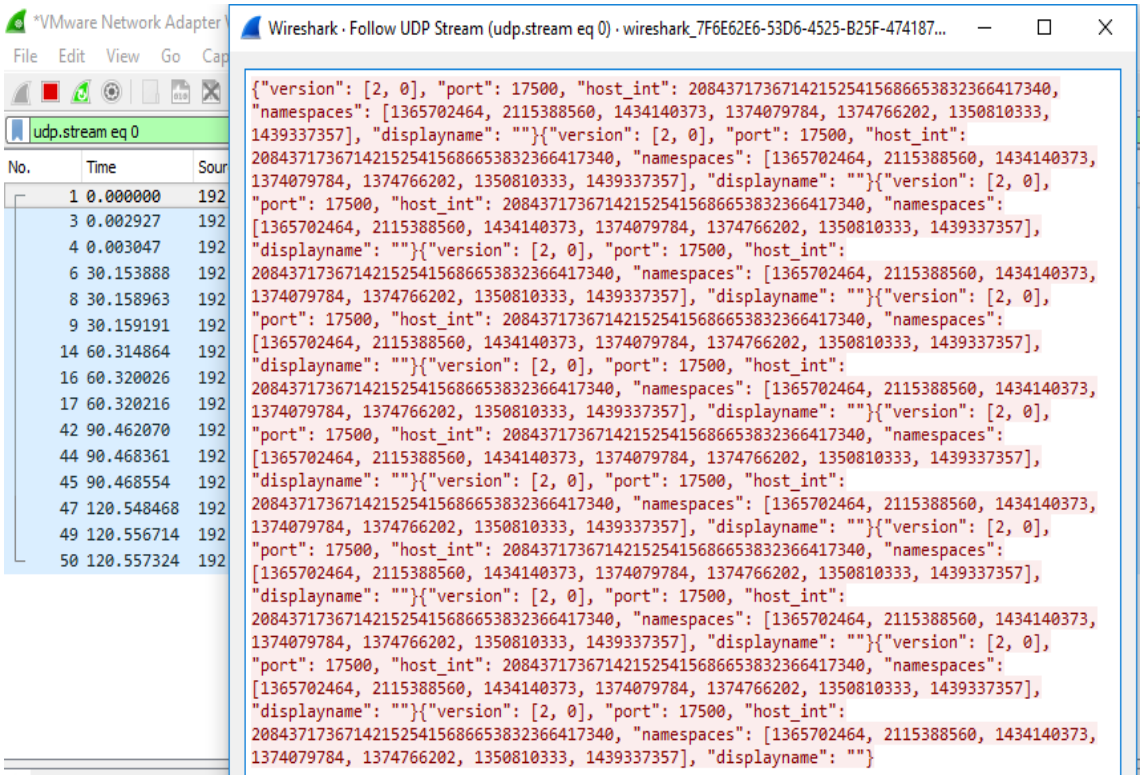
ANEXO 4: Mapeo de red, revisión de puertos abiertos en la red de datos de la universidad, para determinar posibles vulnerabilidades.

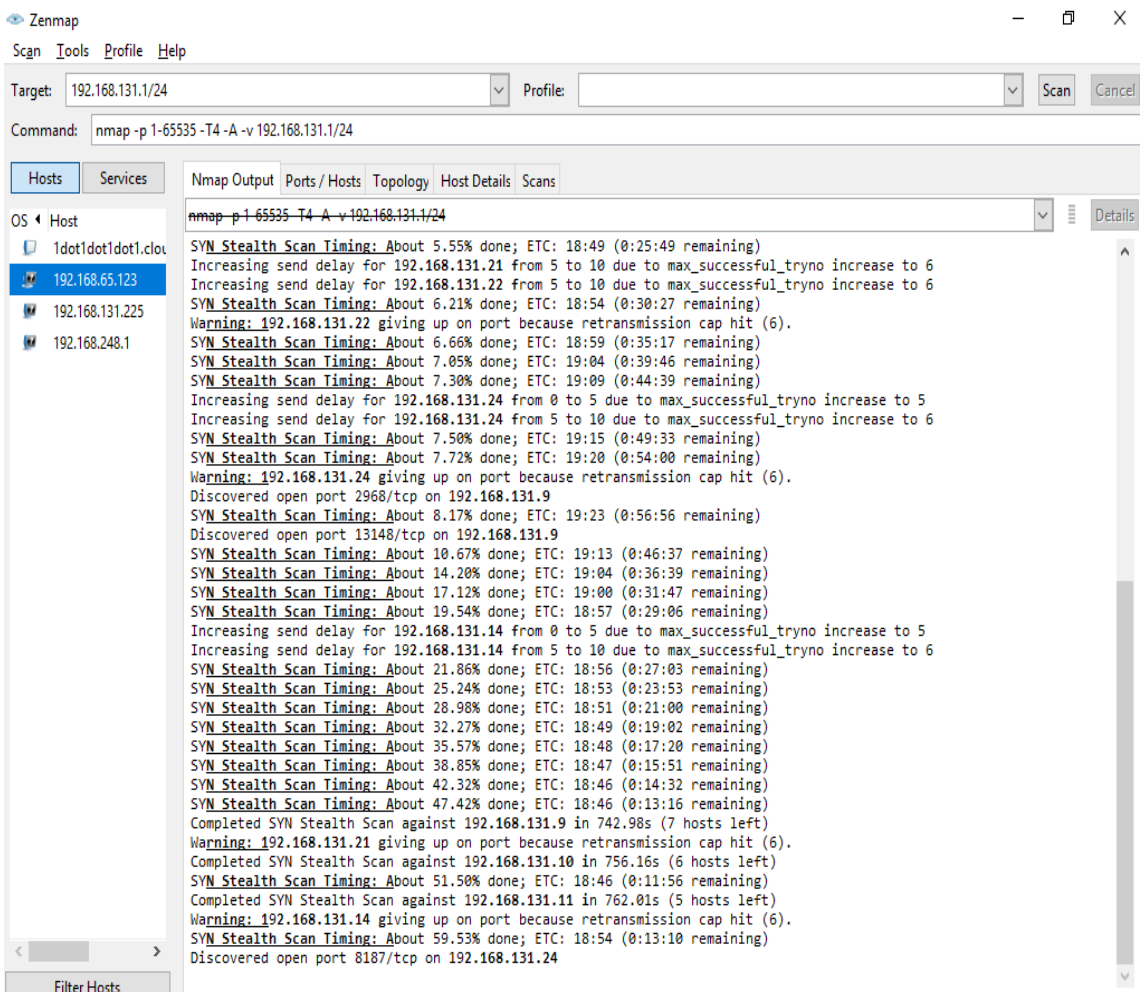
```
C:\Users\Elva>nmap -PN 192.168.65.1

Starting Nmap 6.25 ( http://nmap.org ) at 2018-08-13 16:05 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.65.1
Host is up (0.016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
1723/tcp open  pptp
2000/tcp open  cisco-sccp
8291/tcp open  unknown
MAC Address: 00:0C:42:FF:65:DE (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 9.87 seconds
```




*VMware Network Adapter
File Edit View Go Cap
udp.stream eq 0
No. Time Sour
1 0.000000 192
3 0.002927 192
4 0.003047 192
6 30.153888 192
8 30.158963 192
9 30.159191 192
14 60.314864 192
16 60.320026 192
17 60.320216 192
42 90.462070 192
44 90.468361 192
45 90.468554 192
47 120.548468 192
49 120.556714 192
50 120.557324 192
Wireshark · Follow UDP Stream (udp.stream eq 0) · wireshark_7F6E62E6-53D6-4525-B25F-474187...
{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}{"version": [2, 0], "port": 17500, "host_int": 208437173671421525415686653832366417340, "namespaces": [1365702464, 2115388560, 1434140373, 1374079784, 1374766202, 1350810333, 1439337357], "displayname": ""}


Zenmap
Scan Tools Profile Help
Target: 192.168.131.1/24
Profile:
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.131.1/24
Hosts
Services
OS Host
1dot1dot1dot1.clou
192.168.65.123
192.168.131.225
192.168.248.1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v 192.168.131.1/24
Details
SYN Stealth Scan Timing: About 5.55% done; ETC: 18:49 (0:25:49 remaining)
Increasing send delay for 192.168.131.21 from 5 to 10 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.131.22 from 5 to 10 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 6.21% done; ETC: 18:54 (0:30:27 remaining)
Warning: 192.168.131.22 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 6.66% done; ETC: 18:59 (0:35:17 remaining)
SYN Stealth Scan Timing: About 7.05% done; ETC: 19:04 (0:39:46 remaining)
SYN Stealth Scan Timing: About 7.30% done; ETC: 19:09 (0:44:39 remaining)
Increasing send delay for 192.168.131.24 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.131.24 from 5 to 10 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 7.50% done; ETC: 19:15 (0:49:33 remaining)
SYN Stealth Scan Timing: About 7.72% done; ETC: 19:20 (0:54:00 remaining)
Warning: 192.168.131.24 giving up on port because retransmission cap hit (6).
Discovered open port 2968/tcp on 192.168.131.9
SYN Stealth Scan Timing: About 8.17% done; ETC: 19:23 (0:56:56 remaining)
Discovered open port 13148/tcp on 192.168.131.9
SYN Stealth Scan Timing: About 10.67% done; ETC: 19:13 (0:46:37 remaining)
SYN Stealth Scan Timing: About 14.20% done; ETC: 19:04 (0:36:39 remaining)
SYN Stealth Scan Timing: About 17.12% done; ETC: 19:00 (0:31:47 remaining)
SYN Stealth Scan Timing: About 19.54% done; ETC: 18:57 (0:29:06 remaining)
Increasing send delay for 192.168.131.14 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.131.14 from 5 to 10 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 21.86% done; ETC: 18:56 (0:27:03 remaining)
SYN Stealth Scan Timing: About 25.24% done; ETC: 18:53 (0:23:53 remaining)
SYN Stealth Scan Timing: About 28.98% done; ETC: 18:51 (0:21:00 remaining)
SYN Stealth Scan Timing: About 32.27% done; ETC: 18:49 (0:19:02 remaining)
SYN Stealth Scan Timing: About 35.57% done; ETC: 18:48 (0:17:20 remaining)
SYN Stealth Scan Timing: About 38.85% done; ETC: 18:47 (0:15:51 remaining)
SYN Stealth Scan Timing: About 42.32% done; ETC: 18:46 (0:14:32 remaining)
SYN Stealth Scan Timing: About 47.42% done; ETC: 18:46 (0:13:16 remaining)
Completed SYN Stealth Scan against 192.168.131.9 in 742.98s (7 hosts left)
Warning: 192.168.131.21 giving up on port because retransmission cap hit (6).
Completed SYN Stealth Scan against 192.168.131.10 in 756.16s (6 hosts left)
SYN Stealth Scan Timing: About 51.50% done; ETC: 18:46 (0:11:56 remaining)
Completed SYN Stealth Scan against 192.168.131.11 in 762.01s (5 hosts left)
Warning: 192.168.131.14 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 59.53% done; ETC: 18:54 (0:13:10 remaining)
Discovered open port 8187/tcp on 192.168.131.24

Bibliografía

Alaminos, A., & Castejón, J. L. (2006). *Elaboración, análisis e interpretación de encuestas, cuestionarios y escalas de opinión*: Universidad de Alicante.

Alonso-Arévalo, J. (2007). Gestión de la Información, gestión de contenidos y conocimiento.

Beltran, C., & Yesabeth, I. (2015). Diseño de un Plan para el Tratamiento de riesgos Tecnológicos utilizando la metodología NIST SP 800-30.

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*: Editorial Paraninfo.

Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*: Kogan Page Ltd.

Cater-Steel, A., & Tan, W.-G. (2005). *Implementation of IT Infrastructure Library (ITIL) in Australia: Progress and success factors.* Paper presented at the 2005 IT Governance International Conference.

CERT-PY. (2017). *Secretaría Nacional de Tecnologías de la Información y Comunicación* . Obtenido de https://www.cert.gov.py/index.php/download_file/view_inline/1375

CIS. (2018). *Center for Internet Security*. Obtenido de CIS: https://www.cisecurity.org/controls/

CSIRT. (2016). *Equipos de respuesta a incidentes de seguridad*. Obtenido de https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

Comer, D. E. (2015). *Redes globles de información con internet y TCP/IP*. México: Prentice Hall.

Chrissis, M. B., Konrad, M., & Shrum, S. (2003). *CMMI guidlines for process integration and product improvement*: Addison-Wesley Longman Publishing Co., Inc.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(02), 92.

Gavilánez, C., & de la Nube, Y. (2016). *Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final.* Escuela Superior Politécnica de Chimborazo.

Guagalango Vega, R. N., & Moscoso Montalvo, P. E. (2011). *Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército*. SANGOLQUI/ESPE/2011.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). Metodología de la investigación.

Herzog, P. (Producer). (2017, Noviembre 15). OSSTMM3. Retrieved from www.osstmm.org

Lindao, M., & Alexander, Á. (2017). *Análisis de vulnerabilidades en dispositivos de red ethernet del Complejo Universitario Norte CAFF*. Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.

Martín Torres, D., Marrero Llinares, M., Barra Zavaleta, E., Moreiro González, J. A., & Urbano Merino, J. (2011). Virtualización, una solución para la eficiencia, seguridad y administración de intranets.

Matalobos Veiga, J. M. (2009). Análisis de Riesgos de Seguridad de la Información.

May, L., & Lane, T. (2006). A Model for improving e-Security in Australian Universities. *Journal of Theoretical and Applied Electronic Commerce Research, 1*(2).

Mieres, J. (2009). Ataques informáticos. *Debilidades de seguridad comúnmente explotadas)*. *Recuperado* http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf.

Milagros, P. B. L., & Steven, Y. C. E. (2017). *Análisis De Vulnerabilidades En La Infraestructura Tecnológica De Una Empresa, Utilizando Herramientas De Test De Intrusión*. Universidad De Guayaquil. Facultad De Ciencias Matemáticas Y Físicas. Carrera De Ingeniería En Networking Y Telecomunicaciones.

Molina, K. J. M., Meneses, J. P., & Silgado, I. Z. (2009). Firewall-linux: una solución de seguridad informática para pymes (pequeñas y medianas empresas). *Revista UIS Ingenierías, 8*(2), 155-165.

NIST. (2012). Guide for conductingrisk assessments. *Information securyti*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Pazmiño Naranjo, P. D. (2007). *Análisis de los riesgos y vulnerabilidades de la red de datos de Escuela Politécnica Nacional.* QUITO/EPN/2007.

Peltier, T. R. (2010). *Information security risk analysis*: Auerbach publications.

Snyder, C., & Dionisio, C. S. (2017). *A project manager's book of forms: A companion*

to the PMBOK guide: John Wiley & Sons.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 28*(5).

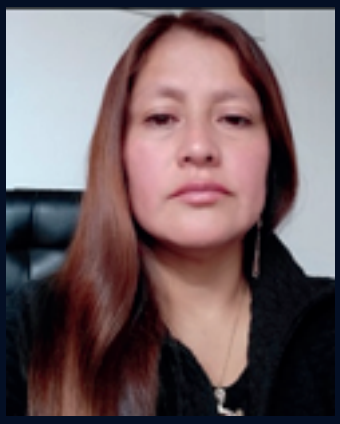
Stoneburner, G., Goguen, A., & Feringa, A. (2015). *Risk management guide for informaton technology systems*. Washington: U.S. Department of Commerce.

Tápies, J. (2010). Filantropía en la empresa familiar. Más allá del beneficio económico. *Cátedra de Empresa Familiar, 53*.

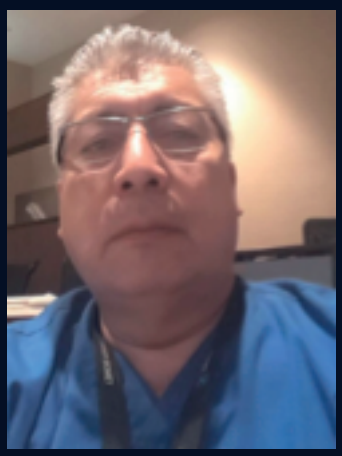
Valdez Alvarado, A. (2013). OSSTMM 3. *Revista de Información, Tecnología y Sociedad*, 29.

Vásquez Alvarado, A. (2014). OSSTMM3. 20-30.

Yanchapaxi, G., & Marcelo, C. (2017). *Propuesta metodológica para la implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema SCADA/EMS del Centro de Control de Transmisión de CELEC EP–TRANSELECTRIC*. Quito, 2017.



IIng. Elva Gioconda Lara Guijarro, MSc.
Ingeniera en Electrónica en Telemática, Magister en Tecnología de la Información mención Seguridades en Redes Informáticas. Coordinadora de Investigación del Instituto Superior Tecnológico Central Técnico. He realizado ponencias dentro y fuera del país. Tengo varias publicaciones en revistas indexadas, una de ellas "Uso del triángulo del fraude, para determinar la incidencia del fraude académico en estudiantes", revista indexada UNIANDES EPISTEME. Vol. 5, Núm. 3 (2018): julio-septiembre (01/07/2018)



Dr. Edgar F. Castaneda G., PhD
Médico especialista en Ortopedia y Traumatología Infantil en el Instituto Pirogov Ukrania, Ing. en Informática, MSc. en Seguridad Informática y Redes, MSc. Ortopedia y traumatología general. MSc. Gerencia en Sistemas de Salud. Docente titular universidad UNIANDES-ext. Tulcán en la Escuela de Enfermería e Ingeniería de Sistemas. Director del Área de Traumatología del Hospital Luis G. Dávila de Tulcán-Ecuador.

compAS
Grupo de capacitación e investigación pedagógica

UNIVERSIDAD DE ORIENTE