

**Análisis en seguridad de la información basado en las** **normas ISO 27001, 27002 y 27005 – sistemas de seguridad de la información, riesgos y controles dirigido a la Universidad de Ibagué**

**Johann Sebastian Montaña Mahecha**

**Luis Miguel Espinosa Rubio**

**Facultad de Ingeniería**

**Ingeniería de Sistemas**

Ibagué, 2021



**Análisis en seguridad de la información basado en las normas ISO 27001, 27002 y 27005 – sistemas de seguridad de la información, riesgos y controles dirigido a la Universidad de Ibagué**

**Johann Sebastian Montaña Mahecha**

**Luis Miguel Espinosa Rubio**

Trabajo de grado que se presenta como requisito parcial para optar al título de:

**Ingeniero de Sistemas**

Director:

Ingeniero Carlos Andrés Lugo González

Docente Universidad de Ibagué

Co-director:

Ingeniero Daniel Palomo

Administrador Consola Kaspersky Universidad de Ibagué

**Facultad de Ingeniería**

**Ingeniería de sistemas**

Ibagué, 2021

*Este trabajo lo dedicamos a Dios que nos iluminó y nos permitió avanzar en cada etapa de nuestro estudio; a nuestros padres por su compresión, cariño y en todo momento brindarnos su ayuda; a todos los docentes que con sus enseñanzas nos brindaron la oportunidad de alcanzar este nuevo éxito en nuestra vida.*

Agradecimientos

Agradecemos a Dios por habernos dado salud, vida y lo necesario día a día para lograr nuestros objetivos.

A nuestros padres Gustavo Montaña, Miguel Espinosa, Martha Mahecha e Idis Rubio quienes, con su cariño, apoyo, desvelos y dedicación siempre se encontraban junto a nosotros impulsándonos a convertir nuestros sueños en realidad y ser profesionales.

Al ingeniero Carlos Andrés Lugo González por aceptarnos para realizar este trabajo bajo su dirección, su dedicación, asesoría y la orientación que siempre nos brindó para la finalización exitosa de esta monografía.

Al ingeniero Daniel Palomo administrador de la consola Kaspersky de la Universidad Ibagué por el tiempo dedicado a brindarnos información sobre la consola y la utilidad de las funcionalidades de este software.

A todos los docentes de la facultad de Ingeniería que nos enseñaron no solo temas de la profesión sino de la vida impulsándonos a alcanzar el éxito.

Resumen

En esta época de grandes avances tecnológicos el sector educativo no es ajeno a las vulnerabilidades existentes en torno a la información. Para realizar el presente trabajo Análisis en seguridad de la información basado en las normas ISO 27001, 27002 y 27005 – sistemas de seguridad de la información, riesgos, controles dirigido a la Institución Educativa Universidad de Ibagué, se recopiló la información a través del ingeniero responsable de la consola Kaspersky que sirve de guía para determinar los peligros a los cuales son susceptibles la base de datos de la Institución e identificación de los controles según las normas ISO. En este proyecto se propone una política de seguridad que aplicando las funcionalidades del software busca contribuir a la mitigación de riesgos analizados en matrices de acuerdo con su probabilidad e impacto para que se cumplan con los pilares de la información como son confidencialidad, integridad y disponibilidad

**Palabras clave:** Seguridad de la información, riesgos, controles, consola Kaspersky, política de seguridad, impacto, probabilidad

**Abstract**

In this era of great technological advances the education sector is no stranger to the existing vulnerabilities around information, to carry out this work Analysis in information security based on ISO 27001, 27002 and 27005 standards – information security systems, risks, controls aimed at the Educational Institution University of Ibagué, the information is collected through the engineer responsible for the Kaspersky console who serves as a guide to determine the hazards to which the Institution's database is susceptible and identification of the controls according to ISO standards. This project proposes a security policy that by applying the functionalities of the software seeks to contribute to the mitigation of risks analyzed in matrices according to their probability and impact so that the pillars of the information such as confidentiality, integrity and availability are met.

**Keywords:** Information security, risks, controls, Kaspersky console, security policy, impact, probability

Contenido

[Introducción 1](#_Toc87620573)

[Antecedentes 4](#_Toc87620574)

[Objetivos 7](#_Toc87620575)

[Justificación 8](#_Toc87620576)

[1. Normas ISO 9](#_Toc87620577)

[2. Riesgos 11](#_Toc87620578)

[2.1 Definición 11](#_Toc87620579)

[2. 2. Clasificación 11](#_Toc87620580)

[2.2.1. Riesgos de integridad 12](#_Toc87620581)

[2.2.2. Riesgos de relación 12](#_Toc87620582)

[2.2.3. Riesgos de acceso 12](#_Toc87620583)

[2.2.4. Riesgos de utilidad 12](#_Toc87620584)

[2.2.5. Riesgos de infraestructura 13](#_Toc87620585)

[2.2.6 Riesgos de seguridad general 13](#_Toc87620586)

[2.3. Identificación de los riesgos en la Universidad de Ibagué 13](#_Toc87620587)

[2.4. Evaluación 18](#_Toc87620588)

[2.5. Priorización 20](#_Toc87620589)

[3. Controles 25](#_Toc87620590)

[3.1 Definición 25](#_Toc87620591)

[3.2 Tipos de controles 25](#_Toc87620592)

[3.2.1 Controles preventivos 25](#_Toc87620593)

[3.2.2 Controles detectivos 26](#_Toc87620594)

[3.2.3 Controles correctivos 26](#_Toc87620595)

[3.3 Sugerencias de controles que se puedan desarrollar con la consola disponible en la Universidad 26](#_Toc87620596)

[3.4 Atributos de los controles identificados 31](#_Toc87620597)

[3.5 Tratamiento de los riesgos con los controles sugeridos 37](#_Toc87620598)

[4.1 Objetivo 45](#_Toc87620599)

[4.2 Alcance 45](#_Toc87620600)

[4.3 Política control de acceso 45](#_Toc87620601)

[4.3.1 Categorías de acceso 45](#_Toc87620602)

[4.3.2 Gestión de usuarios 46](#_Toc87620603)

[4.3.3 Control de accesos a sistemas y aplicaciones 46](#_Toc87620604)

[4. 4 Política de seguridad física y ambiental 46](#_Toc87620605)

[4.4.1 Política de escritorio y pantallas limpias 47](#_Toc87620606)

[4.5 Política de transferencia de información 47](#_Toc87620607)

[4.6 Política de dispositivos móviles y teletrabajo 47](#_Toc87620608)

[4.7 Política de restricciones a las instalaciones y uso del software 48](#_Toc87620609)

[4. 8 Política de protección contra software malicioso 48](#_Toc87620610)

[4.9 Política de seguridad de recursos humanos 48](#_Toc87620611)

[Conclusiones 50](#_Toc87620612)

[Referencias bibliográficas 51](#_Toc87620613)

[A. Anexo: Tablas de valoración controles en los riesgos identificados en la Universidad Ibagué 55](#_Toc87620614)

[B. Anexo: Tablas de acciones sugeridas para los riesgos identificados en la Universidad Ibagué 63](#_Toc87620615)

Lista de figuras

Pág.

Figura – 1 Mapa de calor ………………………………………………………………… 19

Figura – 2 Nomenclatura parámetros y criterios ……………………………………… 37

Lista de tablas

Pág.

Tabla 1: Identificación de riesgos ………………………………………….………………….14

Tabla 2: Análisis Riesgo Uso de medios removibles sin supervisión ………..………….. 20

Tabla 3: Análisis Riesgo Averías eléctricas ……………………………………………….. 21

Tabla 4: Análisis Riesgo Uso dispositivos móviles sin control …… ….………………….. 21

Tabla 5: Análisis Riesgo Error humano ……………………………………………………. 22

Tabla 6: Análisis Riesgo Uso de sistemas operativos diferentes ……………………….. 22

Tabla 7: Análisis Riesgo Descarga y uso de activadores para algunos programas ….. 22

Tabla 8: Análisis Riesgo Permisos administrador en los equipos ……………………….. 23

Tabla 9: Análisis Riesgo Falta de documentación de políticas en seguridad de la información …………………………………………………………………………………….. 23

Tabla 10: Carencia de actualización profesional ………………………………………….. 23

Tabla 11: Identificación de controles ……………………………………………………….. 28

Tabla 12: Atributos controles ……………………………………………………………….. 32

Tabla 13: Rangos de calificación controles ………………………………………………. 38

Tabla 14: Evaluación de controles …………………………………………………………. 39

Tabla 15: Valoración controles en el riesgo uso de medios removibles sin supervisión 42

Tabla 16: Valoración controles en el riesgo averías eléctricas ……………………….. 43

Tabla 17: Valoración controles en el riesgo uso dispositivos móviles sin control …….. 55

Tabla 18: Valoración controles en el riesgo error humano ……………………………… 56

Tabla 19: Valoración controles en el riesgo uso de sistemas operativos diferentes …. 57

Tabla 20: Valoración controles en el riesgo descarga y uso de activadores para algunos programas ……………………………………………………………………………………. 58

Tabla 21: Valoración controles en el riesgo permisos administrador en los equipos ... 59

Tabla 22: Valoración controles en el riesgo falta de documentación de políticas en seguridad de la información …………………………………………………………………..60

Tabla 23: Valoración controles en el riesgo carencia de actualización profesional ….. 61

Tabla 24: Acciones sugeridas para el riesgo uso de medios removibles sin supervisión ………………………………………………………………………………………………... 63

Tabla 25: Acciones sugeridas para el riesgo averías eléctricas ……………………….. 65

Tabla 26: Acciones sugeridas para el riesgo uso de sistemas operativos diferentes .. 66

Tabla 27: Acciones sugeridas para el riesgo uso de dispositivos móviles sin control . 67

Tabla 28: Acciones sugeridas para el riesgo error humano ……………………..……. 68

Tabla 29: Acciones sugeridas para el riesgo descarga y uso de activadores para algunos programas ……………………………………………………………………………………. 70

Tabla 30: Acciones sugeridas para el riesgo permisos administrador en los equipos ... 72

Tabla 31: Acciones sugeridas para el riesgo falta de documentación de políticas en seguridad de la información…………………………………………………………………… 73

Tabla 32: Acciones sugeridas para el riesgo carencia de actualización profesional ….. 74

.

# Introducción

En la actualidad es de vital importancia la seguridad de la información en entes gubernamentales y no gubernamentales ya que se manejan datos de gran relevancia. Las Instituciones Educativas no se encuentran al margen de este proceso pues manejan información sensible y por lo tanto deben contar con medios que le permitan descubrir e impedir el uso indebido de la información de la comunidad académica que reposa en sus bases de datos. La Universidad de Ibagué busca fortalecer procesos que le brinden protección a los activos que poseen información y para tal fin se realizó un análisis del sistema de seguridad de la información, regida por las normas ISO 27001 (ICONTEC, 2013), ISO 27002 (MinTIC, 2013) e ISO 27005 (ICONTEC, 2009).

Las normas ISO utilizadas en este trabajo son normas estandarizadas a nivel internacional que propenden por la mejora empresarial brindando herramientas que ayudan al perfeccionamiento en la eficiencia y el uso de los recursos definiendo de manera genérica la forma de planificar, verificar y controlar un sistema de gestión de la información sin tener presente el entorno, activos, las TIC, información que maneje y cultura organizacional ya sea interna o externa. Esto permitirá mitigar el impacto de incidencias en la seguridad de la base de datos de la entidad educativa antes mencionada, brindar servicios de alta calidad y continuar con el alto índice de credibilidad que tiene entre la población ibaguereña.

La Universidad de Ibagué se encuentra implementando un nuevo software de protección que se maneja a través de la consola (Kaspersky Security Center) que permite monitorear constantemente los equipos que se encuentren vinculados y que hallan descargado previamente el antivirus. Además, cuenta con una amplia variedad de funcionalidades como el bloqueo de puertos, mantenimiento remoto de los equipos, soporte, control de versiones, controlar despliegues y configuraciones iniciales de los equipos, la red y la nube o servidores que brindan seguridad a la información que maneja la entidad. También, brinda semáforos con la información de la infraestructura, estados de protección y estadísticos que se utiliza para verificar el estado actual de los equipos conectados a la red y que tengan instalado el antivirus.

De igual manera la consola expone los informes numéricos que muestran información detallada de la seguridad en la red e informes que se presentan en sectores como los de nivel de importancia (eventos críticos, fallas funcionales, advertencias y mensajes informativos), por otro lado, se encuentran eventos por tiempo que hacen referencia a la actividad más reciente, también se hallan mensajes de eventos por tipo (las solicitudes de los usuarios y eventos de auditoría). El software abre caminos que con controles y políticas bien definidas se convierte en una parte importante de los procedimientos de administración de los datos en la entidad para asegurar confiabilidad en la seguridad de la información.

El presente trabajo monográfico buscó analizar el sistema de seguridad de la información en la Universidad de Ibagué basado en las normas ISO 27001,27002 y 27005, el conocimiento de la consola (Kaspersky Security Center) y la infinidad de aportes que brinda al sistema de gestión informática, mediante la identificación y categorización de los riesgos a los que se encuentra vulnerable la información. Se toma como base la información brindada por el ingeniero a cargo de la consola, quien trabaja de acuerdo con las limitaciones que la pandemia ha obligado a cumplir dentro de la relativa normalidad con la que se labora actualmente.

Una vez recopilada la información se elaboraron matrices que cuentan con la descripción del riesgo y la calificación de este. De esta manera permite sugerir controles que mitiguen el impacto e incidencia de los riesgos aprovechando al máximo las funcionalidades del software utilizado en la Institución. Además, se propone una política de seguridad de información basada en las normas legales vigentes en el país (requisitos y pautas de actuación) desarrollada dentro de un marco apropiado para salvaguardar la información de la Universidad. Se caracteriza por su fácil implementación, brinda opciones de registro, seguimiento de actividades, manejo adecuado de los equipos, dispositivos y demás sistemas de información utilizados por la población vinculada con los servicios que presta la Institución.

La política de seguridad que se sugiere es adaptada a los requerimientos propios de la Universidad de Ibagué que pretende generar un impacto positivo en la percepción de controles que se usan y el implemento de otros que garanticen un buen desempeño de la Institución educativa objeto de estudio. En cuanto a la seguridad de la información, los procesos que se originan, el aumento del grado de efectividad y el uso de las herramientas con las que cuenta la Universidad garantizan el cumplimiento de los principios de la seguridad de la información como son disponibilidad, integridad y confidencialidad.

Esta monografía es de tipo documental basada en la obtención de datos de fuentes documentales sobre el tema (fruto de la interpretación, estudio y asimilación elaborados por otros) y de campo mediante la observación de la realidad y entrevistas con el ingeniero a cargo del manejo de la consola del antivirus utilizado en la Institución. En el trabajo se revisó las funcionalidades del antivirus y su repercusión en la seguridad de la información en la entidad objeto de estudio y aspira abrir caminos hacia la búsqueda e implementación de mecanismos que proporcionen seguridad efectiva y eficaz a la información que maneja la Universidad.

# Antecedentes

A nivel mundial la seguridad de la información en todas las Instituciónes es de gran importancia ya que posee datos que debe custodiar y que se mueven en una dinámica diaria, por lo que es necesario la implementación de controles que garanticen confidencialidad, integridad y disponibilidad que son la base de la información, pensando en el cumplimiento de estos fines. La primera entidad que formuló estándares de normalización fue la BSI (British Standards Institution) en el año 1979, luego de varias modificaciones se llega al estándar ISO 27001, aprobado, difundido, reconocido y publicado en el 2005.

En Colombia, al igual que en muchos otros países alrededor del mundo, se han realizado varios estudios y propuestas de diseños de administración de información. A partir de los resultados obtenidos en las auditorias sobre la seguridad de la información realizada en instituciones se ha obtenido datos susceptibles de estudio. Gracias a los avances y disposición de herramientas tecnológicas al servicio de la humanidad se observa que existen gran cantidad de fallos en las organizaciones que manejan información y de ello no escapan las Instituciones de educación superior (Mena, 2020).

La implementación de la política de seguridad de la información la determina la Universidad teniendo en cuenta las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño, la estructura de esta, eficiencia en el manejo de los activos de información, las incidencias registradas, malware, las funcionalidades de la consola Kaspersky, garantizando buen uso y la privacidad de los datos (Mintic, 2016); para ello, analiza y toma nota de los resultados de acuerdo con las normas y teorías expuestas sobre el cumplimiento de seguridad de la información (Yupanqui y Oré, 2017).

Se puede afirmar sin temor a equivocaciones que hoy en día toda entidad que maneje datos debería programar un presupuesto anual para proteger la información y la seguridad de esta y se debe basar en la norma ISO 27000 (Porras y Alvarado, 2018). Además, los parámetros de la norma ISO 27002 deben contar con características y componentes según el nivel académico (Kurniawan y Riadi, 2018). Así mismo, debe adoptar políticas de seguridad claras con sus respectivas pautas de seguimiento, control y evaluación (Nieles et al., 2017) para el manejo de la información sin que afecte el ambiente de trabajo (Ifinedo, 2018) y que sea de fácil acceso para todo el personal administrativo, empleados, servicios adquiridos a terceros y usuarios que pertenecen a la empresa (Ríos et al,2018). Las empresas en el sector educativo no son ajenas a la implementación de políticas de seguridad de la información (Government technology, 2020), quienes deben enfrentar las críticas de la seguridad en la industria de la educación (Morrow, 2020) y aplicarlas teniendo en cuenta la guía existente para ello.

La Universidad de Ibagué delegó a terceros la función de garantizar la seguridad de los sistemas críticos, pero presenta una serie de falencias en la gestión de la seguridad de la información manejada por usuarios de la Universidad como son el uso inadecuado de herramientas tecnológicas y aplicaciones, el desconocimiento de la seguridad informática, falta de documentación de controles y políticas de seguridad de la información. Por este motivo se originan peligros de ataque cibernético.  Una vez realizada la observación y entrevista con el ingeniero a cargo surge la siguiente pregunta ¿Se puede fortalecer el sistema de gestión de la información manejada por usuarios de la Universidad de Ibagué a partir de la utilización de las funcionalidades del software y la implementación de una política de seguridad de la información?

# Objetivos

**Objetivo General**

Fortalecer el sistema de seguridad de la información para la Universidad de Ibagué basado en las normas ISO 27001,27002 y 27005.

**Objetivos específicos**

- Identificar y categorizar los riesgos a los que está expuesta la información de la Universidad de Ibagué.

- Verificar el cumplimiento de los controles implementados y proponer controles adicionales teniendo en cuenta las funcionalidades de la consola Kaspersky para la mitigación de riesgos en la Universidad.

- Formular una propuesta de política de seguridad de la información para la Universidad de Ibagué.

# Justificación

La finalidad del fortalecimiento de la gestión de información manejada por usuarios de la Universidad de Ibagué se basa en un proceso de mejora continua que permita detectar a tiempo la existencia de nuevos riesgos que amenacen la información, la toma de decisiones que permitan el aprovechamiento de las tics existentes generando oportunidades de perfeccionamiento y ejecución de todas las actividades de la Institución garantizando la disponibilidad, continuidad y calidad de los servicios adscritos a la gestión de información.

El presente trabajo tiene como objeto de estudio la Universidad de Ibagué centro educativo de educación superior con sede en la ciudad capital del Tolima y se fundamentó en la necesidad de realizar un análisis al sistema de gestión de seguridad de la información implementado en la Universidad de Ibagué con el fin de fortalecerlo, para lo cual, se identificaron nuevos riesgos asociados a la plataforma tecnológica manejada por el personal de la Institución, amenazas que acechan la información basados en el manejo de riesgos con el software que posee la Universidad desarrollando controles que influyan favorablemente en la reducción de los riesgos identificados, llevando el riesgo a un nivel aceptable por la Universidad.

Además, se propuso políticas de seguridad con recomendaciones claras y ajustadas a la normatividad vigente en la ley colombiana que sirven de guía no solo a la Institución objeto de estudio sino a entidades que deseen fortalecer el sistema de gestión de seguridad de la información dando origen a cambios favorables en la idea que se tiene sobre los controles y establece pautas para desarrollar investigaciones futuras encaminadas a incrementar los niveles de seguridad de la información en las empresas

# 

# Normas ISO

La Organización Internacional de Normalización (ISO) es una organización no gubernamental que funciona a nivel mundial a partir de 1947, que hasta los años 80 en su política de estandarización de normas creo guías para los productos y la tecnología, a partir de esta fecha y teniendo presente las vulnerabilidades y amenazas a los que se encuentran expuestos los diferentes bancos de datos de la información, amplió sus procesos y en la actualidad pertenecen a la organización más de 165 países (Bureau Veritas, s.f) que pretenden brindar progreso a las empresas a nivel regional e internacional a través de la estandarización de sus sistemas para brindar eficazmente sus servicios. Colombia es uno de estos países que acata los estándares y a través del Ministerio de las TICs proporciona guías relacionadas con sistemas y herramientas específicas de gestión aplicables a toda entidad (Mintic,2016).

Es así como en el país hoy se emplea el término SGSI utilizado principalmente por la **ISO/IEC 27001(ICONTEC, 2006)**, “que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission” (ISOTools Excellence,2013). La implementación del Modelo de Seguridad y Privacidad de la Información – MSPI (Benavides, 2013), lo determina la entidad teniendo en cuenta las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño, su estructura, eficiencia en el manejo de los activos de información, garantizando su buen uso y la privacidad de los datos (Mintic, 2016), siempre y cuando se respete la normatividad.

Por lo tanto en la nación la política de seguridad de la información se encuentra enfocada a la práctica de las normas legales vigentes en Colombia y el cumplimiento de las guías sobre seguridad de la información basadas en las normas ISO 27001:2013 y al modelo de seguridad y privacidad de la información de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (Mintic,2016), todas las orientaciones se encuentran en la Cartilla de políticas de manejo de la información cuya finalidad es alcanzar un idóneo nivel de garantía de las cualidades de calidad y seguridad de la información para tomar decisiones preventivas y correctivas claves, de esta manera cumplir con los pilares básicos de la información.

Aplicar las normas y obtener el éxito deseado requiere conocimientos y para ello se cuenta con una gran gama de literatura en libros y páginas web sobre este aspecto. Algunas de estas obras nos hablan de cómo implementar la norma ISO/IEC 27001 de 2013 según lo planteado por MinTIC (Benavides, 2013), al igual que las normas expuestas en ISO 27001 y 27002 (Solarte et al, 2015), que son una guía que facilita la identificación de los principales activos de la información, los riesgos más comunes a los que se exponen los datos (ICONTEC, 2009), herramientas que facilitan esta actividad (Faris et al, 2014), comprobación y adopción de controles (normaiso27001.es) que sean necesarios para reducir la incidencia de los riesgos y se recomiendan medidas para evitar un gran impacto en la entidad que sea atacada (exabeam, s.f.). También es de vital importancia conocer la metodología para implementar un sistema de seguridad de la información descrita en las normas ISO 27001, 27002 y 27005 (Valencia y Orozco, 2017) para no incurrir en sanciones disciplinarias, ni legales y aplicar la gestión necesaria según las características de la falla (Kavanagh, et al, 2020) con las propuestas pertinentes para una buena política de seguridad.

La Universidad de Ibagué como entidad que funciona en el estado colombiano se acoge a la normatividad de estandarización y toma como una de sus prioridades el tratamiento de datos, por eso se preocupa por disponer con una serie de controles que aseguren confidencialidad, integridad, acceso oportuno, conceptos y principios básicos de la información ya que una buena política de seguridad analiza, toma nota de los resultados de acuerdo con las normas y teorías expuestas sobre el cumplimiento de seguridad de la información (Yupanqui y Oré, 2017) con el fin de contar con un Sistema de Gestión de la Seguridad de la Información, con políticas claras de administración de la información, más conocido con el término en inglés “Information Security Management System” (ISMS) (Yupanqui y Oré, 2017).

# 

# 2. Riesgos

Este estudio monográfico se basa en el análisis de los riesgos encontrados en uno de los principales activos de la información usados por la Universidad de Ibagué como es la consola (Kaspersky Security Center) según informes obtenidos en entrevistas brindada por el ingeniero a cargo del manejo del software (Ingeniero a cargo, comunicación personal, mayo 2021) , ya que los sistemas de información crítica son manejados por terceros lo que imposibilita la obtención de datos relevantes para la realización del presente trabajo.

## 2.1 Definición

Riesgo es un término realmente nuevo en el contexto de seguridad informática que se refiere a la incertidumbre o la probabilidad de que se presente un evento que produzca daño a los servicios informáticos. En el presente siglo muchos autores nos presentan una amplia gama de literatura en este aspecto con el fin de prevenir sobre estas amenazas cada vez más frecuentes dirigidas a las entidades que almacenan datos de importancia vital de los usuarios.

La *Revista Tecnológica - ESPOL*, *28* publicó el concepto de riesgo expuesto por Solarte que dice así “Los riesgos informáticos son problemas potenciales que pueden afectar a los sistemas de información o a los equipos de cómputo, si no se tienen las medidas adecuadas para salvaguardar los datos y la información” (Solarte, et al. 2015, p.7), que es uno de los más acertados frente a las amenazas que hoy aqueja la seguridad de la información. Además, hay que tener presente que la exposición a riesgos se presenta por defectos y boicots en diferentes oportunidades y que se debe manejar una serie de controles que permitan salvaguardar la información a partir del conocimiento de la clasificación de los riesgos que faciliten la toma de decisiones, manejo oportuno de la información, de aplicaciones, seguimiento de procesos, control de acceso y peligros de infraestructura (Solarte et al, 2015).

También hay que tener presente que la norma ISO 27000 define a la amenaza como “la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización” (Glosario ISO27000, s.f). Para prevenir estas amenazas la Universidad cuenta con un excelente antivirus, software que se encuentra monitoreado por el Ingeniero a cargo quien es el responsable directo de todos los eventos que esta consola con sus funcionalidades puede administrar en bien de la protección de la información de la Institución.

## 2. 2. Clasificación

A nivel mundial toda entidad que maneje información se encuentra expuesta a una gran variedad de factores que puedan afectar su desarrollo y credibilidad. Es verdad que la tecnología ha brindado una serie de beneficios para los usuarios, pero a la vez abre las puertas a un sin número de tipos de riesgos informáticos que están latentes y que generan eventualidades difíciles de sortear. Es mucha la bibliografía existente sobre los riesgos y sus tipos por ello daremos una breve explicación sobre los tipos de riesgos mencionada en una publicación da la Universidad nacional de la Plata como son: riesgos de integridad, de relación, de acceso, de utilidad, de infraestructura y de seguridad general (Corda et al , 2017). Cabe mencionar que la Universidad puede agregar todos los riesgos que considere pertinentes o que pueden vulnerar los pilares de la información como son disponibilidad, confidencialidad e integridad.

### 2.2.1. Riesgos de integridad

Este tipo de peligros informáticos se encuentran relacionados con las actividades asociadas a permisos, diligenciamiento y certeza del ingreso, procedimientos y bitácora de los programas utilizados en una entidad, se encuentran en todas las aplicaciones

### 2.2.2. Riesgos de relación

Se trata de riesgos relacionados con la toma de decisiones y se refieren al uso oportuno de la información creada en un programa como los bancos de datos que poseen información personal.

### 2.2.3. Riesgos de acceso

Estos riesgos se encuentran relacionados con el uso incorrecto de programas e información que implica **“**riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la base de confidencialidad de la información”(Corda et al, 2017, p.8)

### 2.2.4. Riesgos de utilidad

En este tipo de riesgos aparecen tres niveles

* Los riesgos son detectados, se enrutan y enfrentan antes de que se presenten dificultades complicadas de resolver.
* Se aplican procedimientos de reparación para aminorar los daños en los programas.
* Copias de seguridad y plan de emergencia frenan catástrofes en el tratamiento de dato

### 2.2.5. Riesgos de infraestructura

Hacen referencia a las fallas de la empresa debido a la inexistencia de equipamiento efectivo de computadores, programas, redes, personal y protocolos que permitan cumplir con las obligaciones de la entidad con un valor asumible. Estos riesgos están relacionados con los procesos de la información tecnológica que determinan, ejecutan, conservan y actúan en un entorno de tratamiento de datos y programas adscritos como atención al cliente.

### 2.2.6 Riesgos de seguridad general

La normatividad que los rige esta consignada en el estándar IEC 950 que formula los parámetros para logra una excelente ciberseguridad y aminorar la presencia de riesgos como:

* Amenazas de descargas eléctricas.
* Peligros de incendio.
* Riesgos de manejo inadecuados de los niveles de energía eléctrica.
* Riesgos de propagación de Ondas sonoras, rayos láser y ondas ultrasónicas.
* Inseguridad mecánica.

## 2.3. Identificación de los riesgos en la Universidad de Ibagué

El rápido avance de la tecnología ha generado una serie de oportunidades que se han visto opacadas con las amenazas, todo ello gracias al internet, redes, creaciones de virus, aparición de hackers y una serie de dificultades que intervienen directamente con el cumplimiento de metas y perdida de documentos que interfieren con el cumplimiento de los pilares de la información de una entidad, sin tener que ver el contexto en el que presta sus servicios. El propósito del análisis de los riesgos es brindar información confiable sobre el efecto y repercusión de estos (Porras, et al 2018).

La Universidad de Ibagué consciente de los grandes retos que la vertiginosa carrera de la tecnología ha impuesto y porque cada día son más los riesgos que se presentan ante el uso indiscriminado de correos, el poco tiempo que los usuarios dedican a la ciberseguridad, los desafíos de seguridad en la nube, la falta de priorización de presupuestos, dispositivos de docentes y estudiantes. Los encargados de la gestión de la información se han propuesto la meta de salvaguardar la información y han adquirido un software administrado por el Ingeniero a cargo, quien, a través de entrevistas, brindó la información necesaria para realizar la identificación de los riesgos.

En la tabla 1 se encuentran descritos los nueve riesgos informáticos identificados en la Universidad de Ibagué donde el estudio de cada uno permitió conocer sus causas y consecuencias

Tabla

*Identificación de Riesgos*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riesgo | Descripción | Tipo | Causas | Consecuencias |
| **R1**  Uso de medios removibles sin supervisión (Conexión USB u otros dispositivos de almacenamiento) | La ausencia de políticas, cifrados, capacitación y desconfianza en las innovaciones tecnológicas, facilitan el uso indebido de medios removibles en la entidad, para ello es necesario crear políticas que faciliten la migración de la información dentro y fuera de la Universidad con altos estándares de seguridad. | Acceso | Falta de políticas para el uso de medios removibles que cuente con el aval de un responsable.  Inexistencia de cursos de formación y concienciación para capacitar al personal sobre la seguridad de la información a través del buen uso de medios removibles  Desconfianza en la ciberseguridad de la nube por considerarla vulnerable | Entrada de programa maligno en los equipos informáticos de la entidad.  Extracción de información sensible de la Universidad.  La información de la entidad puede sufrir perdida, fuga o modificación  Alterar la operación normal de los sistemas de información que maneja la Universidad |

Tabla 1: (Continuación)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Riesgo | | Descripción | | Tipo | | Causas | | Consecuencias | |
| **R2**  Averías eléctricas | | Mantenimiento y adecuaciones de la infraestructura y equipos, principalmente ante la presencia de desastres naturales que pueden originar una falla eléctrica dejando graves consecuencias para la entidad. | | Seguridad general | | Inadecuado plan de mantenimientos en los equipos y la infraestructura  Probabilidad de presencia de desastres naturales  Escasa supervisión del estado de los equipos | | Fallas en los sistemas informáticos y equipos de la Universidad  Perdida de información  Interrupción de la prestación de servicios  Aumento en costos por mal funcionamiento de equipos | |
| **R3**  Uso de dispositivos móviles sin control (Conexión bluetooth como auriculares, teléfono móvil) | La falta de políticas facilita el uso de dispositivos dentro y fuera de la Universidad sin ninguna supervisión, estos dispositivos se conectan a través del bluetooth lo que hace su seguimiento y supervisión difícil. | | Acceso | | Falta de información sobre seguridad en dispositivos móviles  Carencia de políticas para el uso de dispositivos móviles con conexión por bluetooth  Ausencia de herramientas para bloquear este tipo de conexión  Falta de protección de los dispositivos móviles autorizados en el manejo de la información de la Universidad | | Equipos afectados por la entrada de software malicioso  Incumplimiento de los niveles de disponibilidad de servicios e información que maneja la Universidad  Perdida o modificación de información  Infección de la red corporativa | |

Tabla 1: (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riesgo | Descripción | Tipo | Causas | Consecuencias |
| **R4**  Error humano | La negligencia de los usuarios y administrativos de la Universidad que interactúan con los sistemas junto a la falta de una herramienta de supervisión pueden llegar a ocasionar daños significativos en la información, equipos y demás sistemas manejados por la entidad. | Acceso | Falta de capacitaciones dando a conocer la importancia del buen manejo de los sistemas  Escaso interés en proteger los equipos propios con el antivirus que brinda la Universidad  Ausencia de políticas que minimicen la probabilidad de incidencia | Perdida o modificación de la información  Colapso de la red corporativa  Daños en los equipos y sistemas de información  Interrupción en operaciones de la Universidad |
| **R5**  Uso de sistemas operativos diferentes | El uso de 2 o más sistemas operativos por los cuales se puede pasar archivos de un sistema a otro generando tráfico de información infectada | Integridad | Facilidad en el manejo de programas  Programas más livianos y fáciles de usar  Permite ejecutar varias aplicaciones y procesos simultáneamente | Perdida de información  Falla en sistemas y equipos informáticos  Dificultades para actualizar sistemas y software  Operaciones lentas en la red |

Tabla 1: (Continuación)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Riesgo | Descripción | | Tipo | Causas | | Consecuencias |
| **R6**  Descarga y uso de activadores para algunos programas | Uso de activadores o generadores de clave para utilizar programas sin pagar | | Integridad | Facilidad de activación  No tener que pagar suscripción  Costo excesivo para adquirir licencias legitimas | | Infección de los sistemas con virus  Desactualización de los sistemas  Perdida de información |
| **R7**  Permisos de administrador en los equipos | | Al otorgar permisos de administrador en los ordenadores se puede instalar aplicativos sin restricciones | Acceso | Inexistencia de protocolos que permitan gestionar los permisos de administrador | Daños en los equipos  Perdida o modificación de la información  Interrupción de procesos | |
| **R8**  Falta de documentación de políticas en seguridad de la información | | No se cuenta con documentos escritos que determinen las acciones a seguir cuando se presente un incidente | Utilidad | Inexistencia de políticas bien definidas que cuenten con el aval de un responsable | No continuidad de los procesos  Demora del tiempo de respuesta ante un incidente  Desconocimiento de acciones antes, en momento y después del incidente | |

Tabla 1: (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riesgo | Descripción | Tipo | Causas | Consecuencias |
| **R9**  Carencia de actualización profesional | Conocimiento de saberes que permita estar a la vanguardia en cuanto a programación, software, innovaciones tecnológicas y demás temas de seguridad de la información | Infraestructura | Disponibilidad presupuestal  Falta de programas de capacitación  Disponibilidad de tiempo | Incumplimiento en la adecuada prestación de servicios  Dificultades para afrontar incidentes  Retraso en el desarrollo de los procedimientos |

## 2.4. Evaluación

La indagación de los distintos peligros que afectan a nivel informático (riesgos) se realizó con la metodología de la evaluación cualitativa empleando una serie de atributos para explicar el grado de las consecuencias potenciales en términos del grado de daño o costos considerando los siguientes aspectos: desfase en la seguridad de la información ya sea que afecte cualquier principio de la ciberseguridad debido a perdidas, procedimientos mal realizados, alteraciones de planes y fechas límites para las actividades programadas, lesiones para el prestigio e infracción de los requisitos legales. Para determinar la probabilidad e impacto de las vulnerabilidades se realizaron reuniones con la persona encargada del manejo del software existente en la Universidad con el objetivo de conocer los principales peligros y proporcionar la valoración pertinente.

Para determinar el impacto del evento se tiene en cuenta la afectación presupuestal, perdida de cobertura en la prestación de servicios, pago de indemnizaciones, sanciones, tiempo de investigación, reparación, imagen, reputación, buen nombre, salud y seguridad, es decir se tiene presente la destrucción procedente de la materialización del riesgo y efecto pertinente, reseñables o graves para la Universidad. (Mintic, 2016). De acuerdo con el impacto se clasifican en cinco niveles: insignificante, menor, moderado, mayor y catastrófico, donde el más bajo impacto corresponde al nivel insignificante que afecta la ejecución presupuestal en un valor que oscila entre 0.5% y el 1% y el mayor impacto corresponde a cifras mayores o iguales al 50%

En cuanto a la probabilidad de ocurrencia del evento se clasifican de acuerdo con la frecuencia con la que sucede un incidente, se tienen en cuenta cinco niveles atribuyéndose una valoración de 5 al casi seguro, es decir si las eventualidades se presentan más de una vez al año y 1 si el acontecimiento se presenta muy poco o casi nunca (No se presenta en los últimos 5 años). Una vez revisada la probabilidad de ocurrencia del evento en contraste con el impacto de este se otorgó una calificación final al riesgo generando el siguiente grafico mapa de calor (Mintic, 2016).

La figura 1 muestra el resultado del análisis de la posibilidad de ocurrencia y efecto de los riesgos presentes en el establecimiento educativo objeto de estudio.

**Figura 1**

*Mapa de Calor**de los Nueve Riesgos Identificados en la Universidad de Ibagué*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | IMPACTO | | | | | |
| P  R  O  B  A  B  I  L  I  D  A  D |  | Insignificante | Menor | Moderado | Mayor | Catastrófico | |
| Casi seguro |  |  | **R8** | **R1** |  | |
| Probable |  | **R7** |  | **R3** |  | |
| Posible |  | **R9** | **R6** |  |  | |
| Improbable | **R4** |  |  |  |  | |
| Rara vez | **R5** | **R2** |  |  |  | |

Alto

Extremo

Bajo

Moderado

Fuente guía de riesgos DAFP, adecuación de los autores

## 2.5. Priorización

Para la jerarquización de los riesgos existen múltiples técnicas tanto cuantitativas como cualitativas. En este trabajo se realizó de forma cualitativa examinando los criterios de probabilidad e impacto teniendo presente las recomendaciones y sugerencias encontradas en los documentos expedidos por el gobierno nacional (Mintic, 2016). Esta priorizacion (Ver tablas 2 a la 10) se lleva a cabo con el fin de desarrollar acciones encaminadas a eliminar, mitigar o ignorar cada uno de los riesgos que afecta seguridad de la información en la Universidad, utilizando la consola (Kaspersky Security Center) para garantizar la protección eficaz de la información que reposa en cada uno de los archivos de la entidad educativa objeto de estudio.

La priorización otorgada por la calificación obtenida en la evaluación se observa en las tablas 2 a la 10 donde los resultados obtenidos de este análisis brindan a cada uno de los nueve riesgos identificados en la Universidad las medidas de respuesta para mitigar el riesgo.

**Tabla 2**

*Análisis del Riesgo Uso de Medios Removibles sin Supervisión (Conexión USB u otros dispositivos de almacenamiento)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Utilizar la funcionalidad de bloqueo de puertosque tiene la consola con el fin de controlar el acceso de medios removibles y crear políticas que faciliten la migración de la información dentro y fuera de la Universidad con altos estándares de seguridad. | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Casi Seguro | Mayor | Acceso | Extremo | Reducir el riesgo,  evitar,  compartir o transferir | **Alta** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 3**

*Análisis del Riesgo Averías Eléctricas*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Proponer políticas que permitan el control y seguimiento de procesos de ejecución y mantenimiento de infraestructura y equipos principalmente ante la presencia de desastres naturales. | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Rara vez | Menor | Seguridad general | Bajo | Asumir el riesgo | **Baja** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 4**

*Análisis del Riesgo Uso de Dispositivos Móviles sin Control (Conexión Bluetooth como Auriculares, Teléfono Móvil).*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Crear políticas que permitan el seguimiento y supervisión de dispositivos móviles dentro y fuera de la Universidad para los usuarios que interactúan con la información que reposa en los archivos de la Institución, utilizando la funcionalidad de bloqueo de conexiones bluetooth del software. | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Probable | Mayor | Acceso | Extremo | Reducir el riesgo,  evitar,  compartir o transferir | **Alta** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 5:**

*Análisis del**Riesgo Error Humano*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Crear políticas que favorezcan la capacitación de usuarios y administrativos vinculados al manejo de sistemas de información de la Universidad. | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Improbable | Insignificante | Acceso | Bajo | Asumir el riesgo | **Baja** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 6:**

*Análisis del Riesgo Uso de Sistemas Operativos Diferentes*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Generar políticas que supervisen el manejo de sistemas operativos autorizados para evitar el tráfico de información infectada | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Rara vez | Insignificante | Integridad | Bajo | Asumir el riesgo | **Baja** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 7:**

*Riesgo Descarga y Uso de Activadores para algunos Programas*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Crear políticas que promuevan el uso de software legítimo y adquisición de licencias | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Posible | Moderado | Integridad | Moderado | Asumir, reducir el riesgo | **Moderada** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 8:**

*Riesgo**Permisos de Administrador en los Equipos*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Formular proceso a seguir para la gestión de permisos | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Probable | Menor | Acceso | Alto | Reducir el riesgo,  evitar,  compartir o transferir | **ALTA** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 9:**

*Análisis del Riesgo Falta de Documentación de Políticas en Seguridad de la Información*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Documentar y publicar las políticas de seguridad de la información para que sea del conocimiento de los usuarios | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Casi seguro | Moderado | Utilidad | Extremo | Reducir el riesgo,  evitar,  compartir o transferir | **ALTA** |

Fuente guía de riesgos DAFP, adecuación de los autores

**Tabla 10:**

*Análisis del Riesgo Carencia de Actualización Profesional*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OBJETIVO** capacitaciones sobre el software, código seguro e innovaciones tecnológicas | | | | | |
| **Calificación** | | **Tipo Impacto** | **Evaluación** | **Medidas de respuesta** | **Priorización** |
| **Probabilidad** | **Impacto** | **Zona de riesgo** |
| Posible | Menor | Infraes-  tructura | Moderado | Asumir, reducir el riesgo | **Moderada** |

Fuente guía de riesgos DAFP, adecuación de los autores

Según los datos obtenidos en el mapa de calor la ubicación de los riesgos identificados se desarrollaron las tablas de análisis del riesgo donde se observa que en el momento solo dos riesgos requieren una pronta intervención debido a su alta prioridad.

# 3. Controles

## Definición

Uno de los recursos más valioso de los Centros Educativos son los datos y aunque se trata de algo intangible requieren ser controlados y evaluados, según la Norma ISO 27001:2013 determinó como objetivo de la seguridad de la información proteger la información de manera que se encuentre siempre disponible basada en la implementación de controles determinados en la Norma UNE-ISO/IEC 27002. En el caso particular de la Universidad de Ibagué, este requisito lo cumple mediante la contratación de terceros que son los encargados de salvaguardar la información de los sistemas críticos, sin embargo, mediante la utilización de la consola Kaspersky Security Center se brinda seguridad a los equipos asociados a la red corporativa ya que son manejados por personal de la Institución.

La constante evolución de las amenazas cibernéticas está presentando una amplia gama de riesgos nuevos, avanzados y presentes con una vertiginosa frecuencia. En los centros educativos no solo deben lidiar con estos riesgos, también con los que representan las desafiantes y jóvenes mentes que disfrutan de un amplio acceso a tecnología, a un mal juicio sobre las consecuencias de sus acciones y que tienen una amplia motivación para acceder a sus bases de datos (INFOSEC. s.f.). Es por eso que la Universidad de Ibagué debe convertirse en líder en seguridad de la información cumpliendo con las regulaciones diseñadas para proteger los datos de los usuarios de la entidad.

Los controles que se deben implementar a cada uno de los procesos relacionadas con la protección de la información deben contar con una excelente planeación, supervisión y constante evaluación para generar cambios encaminados al fortalecimiento de procedimientos operacionales, responsabilidades, protección ante software malicioso, registro, supervisión de incidentes, garantizar la integridad de los sistemas operativos, contar con una buena gestión de vulnerabilidad técnica, aminorar el efecto de las acciones de revisión de los sistemas operativos y todos aquellos que se encuentran claramente expuestos en la norma vigente (Norma ISO 27001, s.f)

## Tipos de controles

### 3.2.1 Controles preventivos

Los controles preventivos son los que se anticipan a la posibilidad de que sucedan eventos no deseados o inesperados que puedan afectar una meta en la entidad, descartan problemas antes de que surjan, previene desviaciones antes de iniciar o durante el proceso, Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo y aseguran el resultado esperado. Uno de ellos es el software que impide el ingreso a personal no autorizado para evitar errores fraudulentos, otro ejemplo es respaldar la información en archivos

### 3.2.2 Controles detectivos

Intervienen en el momento de la incidencia detectando las faltas y variantes antes de finalizar una operación. Incluso miden la efectividad de los preventivos, incluyen revisiones y comparaciones, edición de reportes, se pueden generar reprocesos y atacan la posibilidad de materialización de un riesgo. Ejemplo el registro de intentos de ingresos no autorizados.

### 3.2.3 Controles correctivos

Operan en la etapa final de un proceso permitiendo modificar o remediaren cierta medida faltas o variaciones, es decir facilitan la vuelta a la normalidad, corrige las consecuencias producidas, modifica el o los sistemas de procesamiento para minimizar que la situación se presente en el futuro, tiene un costo en su implementación y ataca el impacto del riesgo. Entre los ejemplos, se tiene la reparación de un archivo dañado a partir de las copias de seguridad y la planificación de contingencias.

## 3.3 Sugerencias de controles que se puedan desarrollar con la consola disponible en la Universidad

La herramienta adquirida por la Universidad para cumplir con la finalidad de salvaguardar la información que reposa bajo su responsabilidad es Kaspersky Security Center (KSC) Software de administración corporativa de los antivirus Kaspersky para empresas. KSC describe sus funcionalidades:

* **Instalación remota:** “Instalar remotamente el agente de red y el antivirus en los equipos Windows de nuestra red. (requisitos disponer de un usuario y una contraseña con permisos de administración local, o el equipo esté unido al dominio de la empresa)” (cint, s.f).
* **Inventario de equipos:** tan pronto se haya instalado el software en el ordenador se registrará en la consola, donde se podrá investigar información básica del equipo como su dirección IP, sistema operativo, hardware y software instalado y por supuesto el estado de Antivirus Kaspersky (cint, s.f).
* **Directivas:** la consola facilita precisar cómo funcionan las distintas unidades que hacen parte del antivirus Kaspersky que se encuentren registradas en la red. La configuración y autorización de cada unidad de los antivirus alojados en los equipos podrá ser definida por el administrador para cada usuario final.
* **Tareas**: “Desde la consola de administración (KSC) podremos definir tareas puntuales (Como por ejemplo un escaneado de todos los discos duros de todos los equipos de la red) o periódicas (como por ejemplo la tarea de actualización de firmas)” (cint, s.f).
* **Informes:** El software brinda la opción de generar documentos con información de malwares presentes en la red, estado de licencias, lista de ordenadores más infestados de virus y sitios web bloqueados.

Según la consultoría tecnológica Cint se pueden controlar los siguientes equipos desde Kaspersky Security Center

* Servidores: Windows 2003, 2008, 2012, 2016, Servidores Linux o MacOS
* Estaciones de trabajo: Windows XP, Windows 7, Windows 8, Windows 10, MacOS, y Linux
* Móviles: Android e iOS.

Los controles sugeridos en este apartado se realizaron teniendo presente la información sobre la consola y sus funcionalidades brindada por el ingeniero a cargo del manejo del antivirus en la Universidad de Ibagué (Ingeniero a cargo, comunicación personal, 2021) y teniendo presente la tabla de controles presentada por la norma(MinTIC, 2013). Las funcionalidades de la consola Kaspersky Security Center se mencionan en forma breve todas sus especificaciones con enlaces y se encuentran en la página web <https://support.kaspersky.com/>. Entre las opciones se cuenta con:

* Administración de la aplicación facilita la instalación y desinstalación remotamente, comenzar y parar Kaspersky Endpoint Security, modificar las características de aplicación disponibles, agregar contraseñas, empezar y suspender actualizaciones y trabajos de análisis.
* Gestión de tareas estas ejecutan las labores administrativas esenciales, como la asignación de contraseñas, revisión de equipos y la modernización de apartados del software de aplicaciones y bases de datos.
* Gestión de directivas emplea políticas para atribuir criterios Kaspersky Endpoint Security iguales a todos los equipos cliente registrados en un grupo de administración y se determina por el estado del candado si está cerrado bloquea los cambios de configuración e impide cambiar los ajustes que tengan este candado, por el contrario, si el estado del candado es abierto permite cambios y ajustes.
* Cifrado de datos facilita la encriptación de carpetas y archivos guardados en las unidades locales y medios removibles minimizando el riesgo de filtraciones de información en caso de pérdida de discos o accesos no autorizados.
* Control de aplicaciones vigila las tentativas del usuario de acceder a aplicaciones y controla el arranque de aplicaciones por medio de las pautas de control.
* Sensor de Endpoint (Kata) Por medio de esta funcionalidad se tiene una pronta respuesta ante ataques cibernéticos.
* Fácil comunicación entre el usuario y el servidor de Kaspersky Security Center con mensajes acordes a la directiva implantada por el administrador de la consola en situaciones de control de dispositivos, aplicaciones o la web.

.

A continuación, se presenta la tabla 11 con los controles sugeridos y que pueden ser ejecutados por el equipo que dirige el Ingeniero a cargo de la consola Kaspersky se encuentran con el número que aparecen identificados en la norma ISO 27001

**Tabla 11.**

*Identificación de Controles que se Pueden Aplicar en la Universidad de Ibagué*

|  |  |  |
| --- | --- | --- |
| Número | Nombre | Descripción |
| A5 | Politicas de seguridad de la información | Objetivo: Orientar y apoyar desde la dirección la seguridad de la información según los parámetros de la Universidad. |
| A5.1 | Políticas para la seguridad de la información | Controles:  Política control de acceso  Política de seguridad física y ambiental  Política de escritorio y pantallas limpias  Política de transferencia de información  Política de dispositivos móviles y teletrabajo  Política de restricciones a las instalaciones y uso del software  Política de protección contra software malicioso |
| A6 | Organización de la seguridad de la información | Objetivo: Caracterizar una gestión para emprender y vigilar la instauración y ejecución de los planes de la seguridad de la información en la Universidad |
| A6.2 | Dispositivos móviles y teletrabajo | Objetivo Brindar seguridad en dispositivos móviles y en condiciones de teletrabajo |
| A6.2.1 | Política de dispositivos móviles | Control: Esta política plantea que las unidades móviles sean registrados e instalen el cliente Kaspersky que gracias a sus funcionalidades garantizan la seguridad de la información que se encuentra en el dispositivo, para los medios removibles como USB se debe contar con autorización de parte del administrador de la consola para el uso de los mismos ya que se encontraron los puertos bloqueados para impedir su acceso a la información, a su vez también estará bloqueada la conexión a través de bluetooth |

**Tabla 11:** (Continuación)

|  |  |  |
| --- | --- | --- |
| Número | Nombre | Descripción |
| A6.2.2 | Teletrabajo | Control: Registrar en el grupo de administración de la Universidad en Kaspersky los equipos involucrados en teletrabajo |
| A7 | Seguridad relativa a los recursos | Objetivo: Asegurar el cumplimiento de responsabilidades y funciones por parte de los empleados |
| A7.2 | Durante la ejecución del empleo | Objetivo: Asegurar que los funcionarios y contratistas se concienticen de sus compromisos con la seguridad de la información en la Universidad y las cumplan |
| A7.2.1 | Responsabilidades de la dirección | Control: Supervisión a empleados y contratistas por parte de la dirección sobre la aplicación de la seguridad de la información de acuerdo con las políticas implementadas por la Universidad |
| A7.2.2 | Concientización, educación y formación en seguridad de la información | Control: Todos los empleados mediante capacitaciones organizadas por la dirección deben recibir orientaciones claras en toma de conciencia sobre la modernización de las políticas de seguridad de la información y procedimientos inherentes a su función. |
| A9 | Control de acceso | Objetivo: Limitar el acceso a la información y a las instalaciones del procesamiento de información a usuarios autorizados |
| A9.1 | Requisitos para el control de acceso | Objetivo: Permitir el acceso a la información exclusivamente a personal autorizado |
| A9.1.1 | Política de control de acceso | Control: Todos los usuarios y equipos que manejen información de la Universidad deben estar registrados en el grupo de administración de Kaspersky |
| A9.1.2 | Política sobre el uso de servicios de red | Control: Los usuarios para acceder a la red cuentan con usuario y contraseña para autenticarse en los sistemas críticos que posee la Universidad y son otorgados por la dirección acorde al cargo que desempeñan dentro de la Institución. |

**Tabla 11:** (Continuación)

|  |  |  |
| --- | --- | --- |
| Número | Nombre | Descripción |
| A11 | Seguridad física y del entorno | Objetivo: Impedir que se presenten daños, perdidas, ingresos no autorizados e intervenciones contra la infraestructura de tratamiento de la información de la Universidad |
| A11.2 | Equipamiento | Objetivo: Prevenir perdidas, daños o interrupción de las actividades de la Universidad |
| A11.2.2 | Elementos de Soporte | Control: La Universidad cuenta en el tema del fluido eléctrico con sistema de planta y UPS que soportan el datacenter en caso de cualquier falla eléctrica |
| A11.2.3 | Seguridad en el cableado | Control: El centro de cableado se encuentra aislado y con restricciones para su acceso |
| A11.2.4 | Mantenimiento del equipamiento | Control: Cumplir con la ejecución de las actividades de aseo y mantenimiento de las áreas donde se procesa la información, al igual que los equipos para garantizar su disponibilidad e integridad continuas |
| A11.2.8 | Equipamiento desatendido por el usuario | Control: El personal debe recibir capacitación sobre la importancia de cerrar sesión en todo equipo móvil o fijo cuando termine el uso de la red, aplicación o conexiones. |
| A11.2.9 | Política de escritorio y pantalla limpios | Control: Motivar a los usuarios en la política de mantener escritorio y pantalla limpios, asegurar documentos escritos y medios extraíbles para proteger la información. |
| A12 | Seguridad de las operaciones | Objetivo: Garantizar el tratamiento correcto y seguro de las instalaciones de procesamiento de la información y su protección contra el código malicioso |
| A12.1 | Procedimientos operacionales y responsabilidades | Objetivo: Asegurar la operación correcta y segura de la información |
| A12.1.1 | Procedimientos documentados de operación | Control: Todos los procesos que afecten o protejan la información deben estar documentados y disponibles ejemplo las políticas de seguridad de la Universidad y los informes emitidos por la consola Kaspersky |

**Tabla 11:** (Continuación)

|  |  |  |
| --- | --- | --- |
| Número | Nombre | Descripción |
| A12.2 | Protección ante software maliciosos | Objetivo: Proteger los datos y el equipamiento de tratamiento de información de código malicioso. |
| A12.2.1 | Controles ante el software malicioso | Control: Una vez instalado el cliente el equipo contara con la protección del antivirus Kaspersky y detectara amenazas de software malicioso, a su vez elimina los detectados por el antivirus |
| A12.4 | Registro y seguimiento | Objetivo: Registrar acontecimientos y generar pruebas |
| A12.4.1 | Registro de eventos | Control Se visualiza el registro de eventos a través a la funcionalidad de Kaspersky que permite el seguimiento de estos por medio de alertas de cada equipo registrado en el grupo de administración |
| A.12.6 | Gestión de la vulnerabilidad técnica | Objetivo: Evitar la utilización de equipos que presenten fallas técnicas. |
| A12.6.2 | Restricciones sobre la instalación de software | Control: Aprovechando la funcionalidad de la consola Kaspersky crear directivas para controlar la instalación de equipos que se encuentren registrados en el grupo de administración. |

Fuente Guía controles de Seguridad y privacidad de la información Min tic (2013)

## 3.4 Atributos de los controles identificados

Los controles se analizaron teniendo en cuenta los atributos relacionados con la eficiencia de estos para mitigar los riesgos, en ellos se tiene presente el tipo o acciones que realiza frente al riesgo que puede ser preventivo o sea que se anticipan al evento, detectivo como su nombre lo indica detectan y actúan en el momento de la incidencia o correctivo que es el que actúa al final de la eventualidad y la forma como se realiza la implementación que puede ser manual o automática. Otro de los atributos es la documentación donde se registra la información de eventos e incidencias, para dictaminar sobre este atributo se tiene en cuenta si existen documentos o falta documentar estas actividades, si la frecuencia es continua o aleatoria y si la evidencia se encuentra registrada o no. (Ver tabla 12)

**Tabla 12.**

*Atributos Controles Sugeridos para Implementar en la Universidad de Ibagué*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
| A5 | Políticas para la seguridad de la información | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |
| A 6 | Política de dispositivos móviles | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |
| Teletrabajo | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |

**Tabla 12:** (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
| A 7 | Responsabilidades de la dirección | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado |  |
| Sin documentar | X |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro |  |
| Sin registro | X |
|  | Sensibilización , instrucción y formación en seguridad de la información | Tipo | Preventivo |  |
| Detectivo |  |
| Correctivo | X |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua |  |
| Aleatoria | X |
| Evidencia | Con registro | X |
| Sin registro |  |
| A9 | Política de control de acceso | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |

**Tabla 12:** (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
|  | Política sobre el uso de servicios de red | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado | X |
|  |  |  | Sin documentar |  |
| Frecuencia | Continua |  |
| Aleatoria | X |
| Evidencia | Con registro | X |
| Sin registro |  |
| A11 | Elementos de soporte | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado |  |
| Sin documentar | X |
| Frecuencia | Continua |  |
| Aleatoria | X |
| Evidencia | Con registro | X |
| Sin registro |  |
| Seguridad en el cableado | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado |  |
| Sin documentar | X |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro |  |
| Sin registro | X |

**Tabla 12:** (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
| A11 | Mantenimiento del equipamiento | Tipo | Preventivo |  |
| Detectivo |  |
| Correctivo | X |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |
|  | Equipamiento desatendido por el usuario | Tipo | Preventivo |  |
| Detectivo |  |
| Correctivo | X |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado |  |
| Sin documentar | X |
| Frecuencia | Continua |  |
| Aleatoria | X |
| Evidencia | Con registro | X |
| Sin registro |  |
| Política de escritorio y pantalla limpios | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado |  |
| Sin documentar | X |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro |  |
| Sin registro | X |

**Tabla 12:** (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
| A 12 | Procedimientos documentados de operación | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático |  |
| Manual | X |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |
| A12 | Controles ante el software malicioso | Tipo | Preventivo |  |
| Detectivo | X |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
|  |  | Documentación | Documentado | X |
| Sin documentar |  |
|  |  | Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |
| Registro de eventos | Tipo | Preventivo |  |
| Detectivo | X |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |

**Tabla 12:** (Continuación)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N°. | Controles y sus características | | | |
|  | Restricciones sobre la instalación de software | Tipo | Preventivo | X |
| Detectivo |  |
| Correctivo |  |
| Implementación | Automático | X |
| Manual |  |
| Documentación | Documentado | X |
| Sin documentar |  |
| Frecuencia | Continua | X |
| Aleatoria |  |
| Evidencia | Con registro | X |
| Sin registro |  |

Fuente Min Tic

## 3.5 Tratamiento de los riesgos con los controles sugeridos

En la figura 2 se encuentran descritos los parámetros y criterios seleccionados para determinar la eficacia del control, cada uno de ellos registra la nomenclatura entre paréntesis que será utilizada para la evaluación de los controles en la tabla 14

**Figura 2.**

*Nomenclatura Parámetros y Criterios Utilizados para Determinar Eficacia del Control*

Parámetro (1)

Instrumentos para ejercer control

**Criterios**

Existe un instrumento para ejercer el control (**1.1)**

Se cuenta con guías, cartillas o procedimientos para el utilización de la herramienta (**1.2)**

Con el tiempo de uso de la herramienta se han visto cambios y por lo tanto se ha comprobado su efectividad (**1.3)**

Parámetro (2)

Seguimiento al control

Criterios

Ese encuentran definidos los responsables de la aplicación y vigilancia del control (**2.1)**

La periodicidad de aplicación del control y vigilancia es adecuada  **(2.2)**

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

Cada uno de los controles son examinados y se establece si aminora la posibilidad de ocurrencia o el efecto del riesgo. Para realizar este proceso se adicionan los valores obtenidos en cada uno de los parámetros y criterios expuestos en la figura 2 y se determina el rango al que pertenece de acuerdo a su ubicación en la matriz de evaluación y calificación de riesgos como se observa en la tabla 13.

**Tabla 13.**

*Matriz de Calificación de Controles*

|  |  |  |  |
| --- | --- | --- | --- |
| **Rangos de calificación de controles** | **Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz la calificación, evaluación y respuesta a los riesgos** | | **Calificador** |
| Cuadrantes para disminuir en la probabilidad | Cuadrantes para disminuir en el impacto |
| Entre 0 - 50 | 0 | 0 | **Bajo** |
| Entre 51 - 75 | 1 | 1 | **Medio** |
| Entre 76 - 100 | 2 | 2 | **Alto** |

Fuente Guía de Riesgos del DAFP, adecuación de los autores

A continuación, en la tabla 14 los autores predicen la eficacia del control aplicado al riesgo teniendo en cuenta el aprovechamiento de las funcionalidades de la consola Kaspersky. Los datos cuantitativo y cualitativo presentes en la columna puntaje de la tabla 14 corresponde a la relación entre la probabilidad e impacto que los autores predicen sobre la mitigación del riesgo al aplicar el control sugerido.

**Tabla 14.**

*Evaluación de Controles Sugeridos para Implementar en la Universidad de Ibagué*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controles**  No. Nombre | | **Para**  **metros** | **Criterios** | **Tipo de control**  Proba Impacto  bilidad | | | **Puntajes** | | |
| A5 | Políticas para la seguridad de la información | 1 | 1.1 | X |  | | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 0 | | |
| 2.2 | 15 | | |
| TOTAL | | | | | 75 | Medio | |
| A6 | Política de dispositivos móviles | 1 | 1.1 | X |  | | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | | 100 | | Alto |
| Teletrabajo | 1 | 1.1 | X |  | | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | | 100 | Alto | |
| A7 | Responsabilidades de la dirección | 1 | 1.1 | X | |  | 5 | | |
| 1.2 | 10 | | |
| 1.3 | 15 | | |
| 2 | 2.1 | 5 | | |
| 2.2 | 15 | | |
| TOTAL | | | | | 50 | Bajo | |
| Concientización, educación y formación en seguridad de la información | 1 | 1.1 |  | | X | 10 | | |
| 1.2 | 10 | | |
| 1.3 | 25 | | |
| 2 | 2.1 | 5 | | |
| 2.2 | 15 | | |
| TOTAL | | | | | 65 | Medio | |

**Tabla 14:** (Continuación)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controles**  No. Nombre | | **Para**  **metros** | **Criterios** | **Tipo de control**  Proba Impacto  bilidad | | **Puntajes** | | |
| A9 | Política de control de acceso | 1 | 1.1 | X |  | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 10 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 95 | Alto | |
| A 11 | Política sobre el uso de servicios de red | 1 | 1.1 | X |  | 15 | | |
| 1.2 | 10 | | |
| 1.3 | 20 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 20 | | |
| TOTAL | | | | 80 | Alto | |
| Elementos de Soporte | 1 | 1.1 | X |  | 15 | | |
| 1.2 | 10 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 95 | Alto | |
| Seguridad en el cableado | 1 | 1.1 | X |  | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 100 | | Alto |
| Mantenimiento del equipamiento | 1 | 1.1 |  | X | 15 | | |
| 1.2 | 10 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 20 | | |
| TOTAL | | | | 90 | Alto | |
| Equipamiento desatendido por el usuario | 1 | 1.1 |  | X | 10 | | |
| 1.2 | 10 | | |
| 1.3 | 20 | | |
| 2 | 2.1 | 10 | | |
| 2.2 | 15 | | |
| TOTAL | | | | 65 | Medio | |

**Tabla 14:** (Continuación)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controles**  No. Nombre | | **Para**  **metros** | **Criterios** | **Tipo de control**  Proba Impacto  bilidad | | **Puntajes** | | |
|  | Política de escritorio y pantalla limpios | 1 | 1.1 | X |  | 10 | | |
| 1.2 | 5 | | |
| 1.3 | 25 | | |
| 2 | 2.1 | 10 | | |
| 2.2 | 20 | | |
| TOTAL | | | | 70 | Medio | |
| A 12 | Procedimientos documentados de operación | 1 | 1.1 | X |  | 10 | | |
| 1.2 | 10 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 10 | | |
| 2.2 | 15 | | |
| TOTAL | | | | 75 | Medio | |
| Controles ante el software malicioso | 1 | 1.1 |  | X | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 100 | Alto | |
| Registro de eventos | 1 | 1.1 |  | X | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 100 | | Alto |
| Restricciones sobre la instalación de software | 1 | 1.1 | X |  | 15 | | |
| 1.2 | 15 | | |
| 1.3 | 30 | | |
| 2 | 2.1 | 15 | | |
| 2.2 | 25 | | |
| TOTAL | | | | 100 | Alto | |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

Una vez evaluados los controles de seguridad de la información teniendo presente que el objetivo es mitigar los riesgos ya identificados en la Institución y el uso de las herramientas con las que cuenta la Universidad, se genera la matriz de riesgos de la información determinando los controles asignados y la valoración para cada uno de ellos como se observa en las tablas 15 y 16 con el fin de determinar la eficiencia del control aplicado para cada riesgo identificado, se elaboró una matriz semejante a las dos anteriores (Ver Anexo A: tablas 17 a 23)

**Tabla 15**

*Valoración Controles**en el**Riesgo Uso de Medios Removibles sin Supervisión (Conexión USB u otros dispositivos de almacenamiento*

|  |
| --- |
| **OBJETIVO** Utilizar la funcionalidad de bloqueo de puertosque tiene la consola con el fin de controlar el acceso de medios removibles y crear políticas que faciliten la migración de la información dentro y fuera de la Universidad con altos estándares de seguridad. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Casi Seguro | Mayor | Política dispositivos móviles | Probabi lidad | 60 | 40 | 100 |
| Alto |
| Teletrabajo | Probabi lidad | 60 | 40 | 100 |
| Alto |
| Política de escritorio y pantalla limpios | Probabi lidad | 40 | 30 | 70 |
| Medio |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 16**

*Valoración Controles**en el**Riesgo Averías Eléctricas*

|  |
| --- |
| **OBJETIVO** Proponer políticas que permitan el control y seguimiento de procesos de ejecución y mantenimiento de infraestructura y equipos principalmente ante la presencia de desastres naturales |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Rara vez | Menor | Elementos de soporte | Probabi lidad | 55 | 40 | 95 |
| Alto |
| Seguridad en el cableado | Probabi lidad | 60 | 40 | 100 |
|  |
| Mantenimien  to del equipamiento | Impacto | 55 | 35 | 90 |
| Alto |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

La función principal de los controles es reducir la posibilidad de ocurrencia o el impacto de un incidente, para el manejo de los riesgos prevalecen los siguientes aspectos:

* Evitar o eliminar el riesgo: Consiste en planificar medidas de protección que minimicen cualquier evento futuro. Se utiliza en eventos con alta posibilidad de ocurrencia, con un alto efecto perjudicial para la entidad.
* Reducir o mitigar el riesgo: Proceso encaminado disminuir la probabilidad e impacto de un incidente a través de la optimización e implementación de controles.
* Compartir o transferir el riesgo: Minimiza su efecto buscando respaldo. La más usual es contratar una póliza de seguros.
* Asumir el riesgo: Cuando se asume el daño provocado por el riesgo, se convive con el riesgo, no hay como evitarlo y es baja la posibilidad de ocurrencia ejemplo desastres naturales.

El éxito en la seguridad de la información consiste en implementar los controles y realizar el debido seguimiento para que las acciones se cumplan y así lograr mitigar los riesgos. En las tablas 24 a la 32 (Ver anexo B) se califica cada uno de los riesgos identificando claramente el resultado luego de aplicar los controles asignados a cada uno de ellos. A partir de la calificación después de aplicado el control se sugieren acciones y la asignación de un responsable para aplicar, realizar control y seguimiento a las acciones. En el encabezado de cada tabla se registra la letra **P** presente en la casilla de calificación que corresponde a la probabilidad de ocurrencia y la letra **I** que se encuentra junto a la casilla **P** indica Impacto del riesgo.

1. **Política de seguridad**

La Universidad de Ibagué como empresa que presta servicios a la comunidad colombiana cumple con los requisitos estandarizados promulgados por las normas ISO y sus sistemas críticos son administrados por terceros quienes se encargan del mantenimiento y cumplimiento de los pilares de la información. La información que administra el personal de la Universidad se apoya en la practicidad de la consola Kaspersky, este software interno se caracteriza por el cumplimiento de estándares de calidad que administrado con eficacia y aprovechando sus funcionalidades, garantiza la mitigación de riesgos y asegura calidad en la gestión de la información.

## 4.1 Objetivo

Proponer lineamientos que fortalezcan la seguridad de la información de la Universidad de acuerdo con las disposiciones legales vigentes del país, basados en los riesgos que se pueden mitigar con capacitación y aplicación de las funcionalidades de la consola Kaspersky.

## 4.2 Alcance

Los parámetros presentes en este escrito son aplicables a todos los usuarios de la Universidad sea cual fuere su rol dentro de la entidad (empleados, estudiantes, docentes, terceros) y que se relacione a través de la obtención, tratamiento, registro, restauración, intercambio y revisión de información.

## 4.3 Política control de acceso

### 4.3.1 Categorías de acceso

* El acceso al cuarto de cómputo y todos los bienes de tecnología de la Universidad deben estar permitidos según los roles de los usuarios asignados por el equipo de gestión de la información.
* Todos los usuarios deben contar con las credenciales de ingreso a servicios de red y sistemas de información a los que hayan sido autorizados según su perfil y rol.
* Los usuarios y contraseñas son personales e intransferibles ya que las contraseñas se utilizan como mecanismo de autenticación en los accesos a la red, aplicaciones y sistemas de información de la entidad y será responsabilidad de la persona a la que se le haya asignado.

### 4.3.2 Gestión de usuarios

* La Universidad proporciona las credenciales de usuario al personal administrativo, estudiantes, docentes y terceros con las contraseñas respectivas para ingresar a los servicios de red que ella ofrece.
* Las claves de administrador deben ser cambiadas regularmente o cuando las personas a cargo sean reemplazadas o cambien de rol, el personal responsable debe realizar, conservar, renovar el proceso y las orientaciones para el buen uso de las contraseñas de usuario.
* Los usuarios creados no tienen permiso de administrador, por lo tanto, si lo requiere deberá gestionar el permiso para adquirir la autorización.

### 4.3.3 Control de accesos a sistemas y aplicaciones

El administrador de la consola únicamente permite a los usuarios autorizados el ingreso a programas, sitios web, funciones, servicios, características de software y protocolos utilizados en los controles de acceso e información importante de la configuración.

## 4. 4 Política de seguridad física y ambiental

* Todos los puntos de acceso, puertas y ventanas de las áreas seguras deben tener vigilancia continuamente para impedir el acceso físico de los no autorizados al sitio donde se encuentran alojados los servidores.
* Todos los puntos de acceso deben monitorear permanentemente las condiciones físicas y medioambientales del centro de cómputo con equipos que supervisen la temperatura y niveles de humedad, instrumentos de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y alarmas cuando se registren anomalías o una condición ambiental inadecuada.
* El personal que este a cargo del uso y mantenimiento de los elementos de soporte deben contar con supervisión y autorización de las directivas de la Universidad.
* El personal encargado del sistema de cableado cumplirá su función bajo la supervisión de la persona asignada para este fin.
* Los mantenimientos preventivos al centro de cómputo y centros de cableado deben ser realizados por personal competente, autorizado y acreditado. Se debe llevar un registro al plan de mantenimiento de servicios tecnológicos.
* Todo usuario debe terminar sesión cada vez que culmine las actividades inherentes a su cargo o cuando se presente alguna situación que le exija abandonar su puesto de trabajo.

### 4.4.1 Política de escritorio y pantallas limpias

Este apartado se enfoca en la formación del personal en aspectos asociados con la seguridad de la información con el fin de aminorar las fallas y peligros que se presentan a raíz de los errores humanos.

* Cada vez que el usuario se aparte del sitio de trabajo su escritorio debe estar libre de notas, apuntes, oficios, escritos y medios de almacenamiento que contengan información de la Universidad
* El lugar de trabajo debe mantener aseado y ordenado.
* Las impresoras y scanner deben mantener libres de documentos.
* Los ordenadores, impresoras y scanner deben permanecer apagados cuando no están en uso.

## 4.5 Política de transferencia de información

* La transmisión de información se realiza a través de solicitudes y debe garantizar la confidencialidad, disponibilidad y seguridad de la información.
* Solo se puede realizar intercambio de información entre personal autorizado, cuando dicho intercambio corresponda con el desarrollo de las actividades de su labor.
* La información enviada a través de correo electrónico Institucional debe tener el logo de la Institución y la firma del remitente.

## 4.6 Política de dispositivos móviles y teletrabajo

La Universidad consciente de la exposición de la información y los datos en los dispositivos móviles (Computadores portátiles, celulares y otros) plantea:

* Instalar el cliente Kaspersky en todo dispositivo móvil y equipo de teletrabajo que almacene información de la Universidad.
* Los dispositivos móviles y los equipos utilizados en el teletrabajo deben estar registrados en el grupo de administración de la consola Kaspersky para poder ser utilizados dentro y fuera de la Institución.
* Los dispositivos móviles y los equipos utilizados en el teletrabajo deben contar con su sistema operativo actualizado.
* Toda información accedida remotamente debe ser utilizada para el cumplimiento de las funciones del cargo.
* El administrador de la consola a través de la directiva creada para el grupo de administración de Kaspersky bloquea los puertos USB y conexiones bluetooth.
* El usuario que requiera el uso de los puertos o conexión bluetooth debe gestionar ante el administrador de la consola la autorización, él se encargara de escanear el dispositivo y tomara la decisión de otorgar o negar el permiso para su acceso.
* Es responsabilidad del usuario tener precaución con las unidades removibles que contengan información de la entidad para evitar accesos no autorizados, perjuicios, destrucción o modificación.

## 4.7 Política de restricciones a las instalaciones y uso del software

* Todas las instalaciones de programas en los equipos de la Universidad deben estar autorizadas.
* Está prohibida la instalación de programas ilegales que violen los derechos de autor. Cada una de estas tentativas se debe tratar como un incidente y ser investigado.
* Debe existir un inventario de software autorizados para uso e instalación en los sistemas de información del establecimiento educativo.
* La instalación de software está restringida por una de las funcionalidades de la consola Kaspersky impidiendo el uso de software no autorizados, si se requiere instalar un software se debe gestionar el permiso ante el administrador quien examinará y decidirá si otorga el permiso.
* Se deben implementar directivas en Kaspersky para que los usuarios no instalen en sus equipos software o herramientas que les permitan la obtención de privilegios no autorizados.

## 4. 8 Política de protección contra software malicioso

* Todos los dispositivos deben encontrarse inscritos en la consola para recibir la protección del antivirus Kaspersky y así con controles humanos, físicos, técnicos y administrativos ayudar a la reducción de riesgos asociados a amenazas provocadas por programas malignos o hackers.
* El administrador del software debe estar atento a las diferentes alertas emitidas por la consola y en caso de presentarse alertas rojas aplicar las acciones correspondientes.
* El administrador crea directivas para bloquear el tráfico de red y así evitar el desarrollo de actividades inusuales o lesivas para la información.
* Todo incidente debe ser reportado al administrador de la consola quien documentará y hará seguimiento al evento presentado.

## 4.9 Política de seguridad de recursos humanos

* Los funcionarios y/o usuarios que tengan acceso a los sistemas de información de la Institución deberán participar de las capacitaciones organizadas por las directivas de la Universidad sobre seguridad de la información e innovaciones tecnológicas.
* Las directivas de la Universidad deben nombrar un equipo para programar, planear e informar fechas de las capacitaciones sobre la seguridad informática.
* Cada jefe de dependencia debe supervisar y concientizar al personal a su cargo la importancia de salvaguardar la información manejada en las dependencias que se encuentran bajo su responsabilidad

# Conclusiones

El análisis de riesgos de seguridad de la información permitió evidenciar que la Universidad protege los sistemas críticos de la información con terceros y actualmente está implementado las funcionalidades de la consola Kaspersky en los sistemas de información manejados por el personal de la Institución con el fin de mitigar los riesgos entre los que figuran el uso de medio removibles y dispositivos móviles sin supervisión.

Todos los empleados de la Universidad con funciones inherentes a la información deben recibir capacitación sobre el uso adecuado de los recursos informáticos e innovaciones tecnológicas para evitar poner en riesgo la información de la Institución debido a errores humanos.

La implementación, seguimiento y evaluación de controles permite la detección y prevención de incidentes visualizándose en una disminución de la probabilidad de ocurrencia e impacto de los riesgos identificados.

Nombrar un equipo que vigile las alertas y reportes emanados por el software para detectar riesgos y reportarlos con el fin de reducir la probabilidad de ocurrencia e impacto de incidentes. Además, supervise periódicamente el cumplimiento de lineamientos para garantizar la seguridad de la información en la Institución.

El éxito de la seguridad de la información en la Universidad depende de los procesos de concientización y sensibilización de los involucrados en los sistemas de información con respecto a los beneficios que brinda la implementación, supervisión y evaluación de la política de seguridad adoptada por la Institución.



# Referencias bibliográficas

Benavides, J. (2019) *Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y Privacidad de la Información- MSPI del MinTIC*. Universidad Piloto de Colombia

http://repository.unipiloto.edu.co/

Bureau Veritas (s f) *Importancia de las normas ISO.* Consultado el 6 de noviembre de 2021

https://www.bureauveritas.com.mx/es/importancia-normas-iso

Cint (s f). *¿Qué es Kaspersky Security Center?* Kaspersky. Consultado 30 de julio de 2021

https://www.cint-consulting.com/

Corda, C.,Viñas, M., & Coria, M. (2017) *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje* . Universidad Nacional de la Plata. 7 (1)

https://www.redalyc.org/pdf/3505/350553375007.pdf

Exabeam. (2019) *Seguridad de la información (Infosec): La guía completa.* Seguridad de la Información. Consultado el 10 de agosto de 2021

https://www.exabeam.com/

GovernmentTechnology (2020) *Asegurar las escuelas: los 5 componentes clave de un enfoque integral de la ciberseguridad en la educación*. Noticias de educación. Consultado 19 de agosto de 2021

https://www.govtech.com/

ISO 27000 (s f) *Glosario.* Glosario. Consultado el 6 de noviembre de 2021

https://www.iso27000.es/

ISOTools Excellence (2013) *La Nch ISO 27001. Origen y evolución*. SGSI Blog. Consultado el 7 de noviembre 2021

https://www.pmg-ssi.com/

Faris, S., Ghazouani, M., Medromi, H., & Sayouti, A. (2014) *Information security risk Assessment—A practical approach with a mathematical formulation of risk.* International Journal of Computer Applications, 103(8).

https://citeseerx.ist.psu.edu/

Ríos, G.,Bohada, J, & Delgado, I. (2018) *Gestión de seguridad de la información en las organizaciones.* Investigación e Innovación, *111*.

https://www.researchgate.net/

ICONTEC. (2013) *Norma técnica colombiana NTC-ISO-IEC 27001*. Icontec

https://www.academia.edu/

ICONTEC. (2009) *Norma técnica colombiana NTC-ISO-IEC 27005*. Icontec

https://gmas2.envigado.gov.co/

Ifinedo, P. (2018) Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal*, *31*(1)

https://www.researchgate.net/

Kavanagh, K. M., Rochford, O., & Bussa, T. (2020) Magic quadrant for security information and event management. *Gartner Group Research Note*.

https://cryptos.com.mx/

Kurniawan, E., & Riadi, I. (2018) Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM. *arXiv preprint arXiv:1802.03613*.

https://www.researchgate.net/

Mena, A. (2020) *Estado actual de la auditoria de seguridad en los sistemas de información de educación superior.*

https://dspace.tdea.edu.co/

MinTIC. (2013) *Controles de seguridad y privacidad de la información*. Mintic

https://mintic.gov.co/

Mintic. (2016) *Sistemas de gestión de seguridad de la información (SGSI*). Mintic.

https://mintic.gov.co/

Morrow, S. (2020) Preocupaciones de seguridad críticas para la industria de la educación. *INFOSEC*.

https://resources.infosecinstitute.com/

Norma ISO 27001 (s f) ISO 27001 al completo. ISO 27001. Consultado 28 de agosto de 2021

https://normaiso27001.es/

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An introduction to information security. *NIST special publication*, *800* (12).

https://battleplan.org/

Nuestra identidad digital (s f) *Riesgos informáticos.* Riesgos informáticos. Consultado el 8 de noviembre de 2021

https://sites.google.com/site/nuestraidentidaddigital

Porras, J., Pastor, S., & Alvarado, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista peruana de computación y sistemas*, *1* (1)

https://core.ac.uk/

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. del C. (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).

http://200.10.147.88/index.php/tecnologica/article/view/456

Universidad Libre (2015) *Seguridad de la información*. La Universidad. Consultado el 23 de agosto de 2021

http://www.unilibre.edu.co/

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 22.

https://www.researchgate.net/

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 25.

https://pdfs.semanticscholar.org/

# A. Anexo: Tablas de valoración controles en los riesgos identificados en la Universidad Ibagué

**Tabla 17**

*Valoración Controles**en el**Riesgo Uso de Dispositivos Móviles sin Control (Conexión Bluetooth como Auriculares, Teléfono Móvil).*

|  |
| --- |
| **OBJETIVO** Crear políticas que permitan el seguimiento y supervisión de dispositivos móviles dentro y fuera de la Universidad para los usuarios que interactúan con la información que reposa en los archivos de la Institución, utilizando la funcionalidad de bloqueo de conexiones bluetooth del software |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Proba  ble | Mayor | Política dispositivos móviles | Probabi lidad | 60 | 40 | 100 |
| Alto |
| Teletrabajo | Probabi lidad | 60 | 40 | 100 |
| Alto |
| Política de control de acceso | Probabi lidad | 60 | 35 | 95 |
| Alto |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 18**

*Valoración Controles**en el**Riesgo Error Humano*

|  |
| --- |
| **OBJETIVO** Crear políticas que favorezcan la capacitación de usuarios y administrativos vinculados al manejo de sistemas de información de la Universidad |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Rara vez | Insignifi  cante | Responsabi  lidades de la dirección | Probabi lidad | 30 | 20 | 50 |
| Bajo |
| Concientización, educación y formación en seguridad de la información | Impacto | 45 | 20 | 65 |
| Medio |
| Equipamien  to desatendido por el usuario | Impacto | 40 | 25 | 65 |
| Medio |
| Política de escritorio y pantalla limpios | Probabi lidad | 40 | 30 | 70 |
| Medio |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 19**

*Valoración Controles**en el**Riesgo Uso de Sistemas Operativos Diferentes*

|  |
| --- |
| **OBJETIVO** Generar políticas que supervisen el manejo de sistemas operativos autorizados para evitar el tráfico de información infectada |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Rara vez | Insignifi  cante | Politicas para la seguridad de la información | Probabi lidad | 60 | 15 | 75 |
| Medio |
| Restricciones sobre la instalación de software | Probabi lidad | 60 | 40 | 100 |
| Alto |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 20**

*Valoración Controles**en el**Riesgo Descarga y Uso de Activadores para algunos Programas*

|  |
| --- |
| **OBJETIVO** Crear políticas que promuevan el uso de software legítimo y adquisición de licencias |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Posible | Moderado | Restricciones sobre la instalación de software | Probabi lidad | 60 | 40 | 100 |
| Alto |
| Controles ante el software malicioso | Impacto | 60 | 40 | 100 |
| Alto |
| Registro de eventos | Impacto | 60 | 40 | 100 |
| Alto |
| Política sobre el uso de servicios de red | Probabi lidad | 45 | 35 | 80 |
| Alto |
| Política de control de acceso | Probabi lidad | 60 | 35 | 95 |
| Alto |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 21**

*Valoración Controles**en el**Riesgo**Permisos de Administrador en los Equipos*

|  |
| --- |
| **OBJETIVO** Formular proceso a seguir para la gestión de permisos |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Proba  ble | Menor | Política sobre el uso de servicios de red | Probabi lidad | 45 | 35 | 80 |
| Alto |
| Política de control de acceso | Probabi lidad | 60 | 35 | 95 |
| Alto |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 22**

*Valoración Controles**en el**Riesgo Falta de Documentación de Políticas en Seguridad de la Información*

|  |
| --- |
| **OBJETIVO** Documentar y publicar las políticas de seguridad de la información para que sea del conocimiento de los usuarios |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Casi se  guro | Modera  do | Procedimien  tos  documenta  dos de operación | Probabi lidad | 50 | 25 | 75 |
| Medio |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 23**

*Valoración Controles**en el**Riesgo Carencia de Actualización Profesional*

|  |
| --- |
| **OBJETIVO** Programar capacitaciones sobre el software, código seguro e innovaciones tecnológicas |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CALIFICACION** | | **CONTROLES** | **VALORACION** | | | |
| Proba  bilidad | Impacto | Tipo de controles  Prob. o  impacto | Puntaje  Herra  mientas para ejercer el control | Puntaje  Segui- miento al control | Puntaje final |
| Posible | Me  nor | Responsabi  lidades de la dirección | Probabi lidad | 30 | 20 | 50 |
| Bajo |
| Concientización, educación y formación. | Impacto | 45 | 20 | 65 |
| Medio |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

# B. Anexo: Tablas de acciones sugeridas para los riesgos identificados en la Universidad Ibagué

**Tabla 24**

*Acciones Sugeridas para el Riesgo Uso de Medios Removibles sin Supervisión (Conexión USB u otros dispositivos de almacenamiento*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Utilizar la funcionalidad de bloqueo de puertosque tiene la consola con el fin de controlar el acceso de medios removibles y crear políticas que faciliten la migración de la información dentro y fuera de la Universidad con altos estándares de seguridad. | | | | | | | | | | | |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| Ca  s  i  S  e  g  u  r  o | M  a  y  o  r | E  x  t  r  e  m  o | Política dispositi  vos móviles | R  a  r  a  V  e  z | M  a  y  o  r | A  l  t  o | Reducir el riesgo,  evitar,  compartir  o transferir | Todo medio removible debe estar autorizado por el administrador de la consola para activar los puertos | Adminis  trador de la consola |
| Tele  trabajo | Todo equipo de teletrabajo debe estar registrado en el grupo de administración de Kaspersky | Adminis  trador de la consola |

**Tabla 24** (Continuación)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
|  |  |  | Política de escritorio y pantalla limpios |  |  |  |  | Los usuarios deben asegurar los documentos escritos y medios extraíbles que contengan información | Superviso  res y usuarios |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 25**

*Acciones Sugeridas para el Riesgo Averías Eléctricas*

|  |
| --- |
| **OBJETIVO Proponer** políticas que permitan el control y seguimiento de procesos de ejecución y mantenimiento de infraestructura y equipos principalmente ante la presencia de desastres naturales |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| Ra  r  a  V  e  z | M  e  n  o  r | B  a  j  o | Elemen  tos  de soporte | R  a  r  a  V  e  z | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Asumir el riesgo, | La Universidad cuenta con sistema de planta y UPS | Gestión Directiva |
| Seguiri  dad en el cableado | Cumplir con las restricciones de acceso al centro de cableado | Personal autorizado |
| Manteni  miento del equipa  miento | Ejecutar las actividades de aseo y mantenimiento oportuna y eficazmente | Personal asignado |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 26**

*Acciones Sugeridas para el Riesgo Uso de Sistemas Operativos Diferentes*

|  |
| --- |
| **OBJETIVO** Generar políticas que supervisen el manejo de sistemas operativos autorizados para evitar el tráfico de información infectada |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| Ra  r  a  V  e  z | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Politicas para la seguridad informa... | R  a  r  a  V  e  z | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Asumir el riesgo, | Cumplir con las políticas implementadas por la U | Usuarios |
| Restricciones sobre la instala  ción de software | Crear directivas instalación de software en los equipos registrados en el grupo de administración de Kaspersky | Adminis  trador de la consola |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 27**

*Acciones Sugeridas para el Riesgo Uso de Dispositivos Móviles sin Control*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Crear políticas que permitan el seguimiento y supervisión de dispositivos móviles dentro y fuera de la Universidad para los usuarios que interactúan con la información que reposa en los archivos de la Institución, utilizando la funcionalidad de bloqueo de conexiones bluetooth del software | | | | | | | | | | |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| P  r  o  b  a  b  l  e | M  a  y  o  r | E  x  t  r  e  m  o | Política dispositi  vos móviles | R  a  r  a  V  e  z | M  a  y  o  r | A  l  t  o | Reducir el riesgo,  evitar,  compartir  o transferir | Los dispositivos móviles deben instalar el cliente Kaspersky y ser registrados en el grupo de admón. de la U y contar con los permisos para conexiones | Adminis  trador de la consola |
| Tele  trabajo |  | Todo equipo de teletrabajo debe estar registrado en el grupo de Kaspersky | Adminis  trador de la consola |
| Política de control de acceso |  | Los usuarios que manejen información relevante o tengan acceso a sistemas críticos deben estar registrados en el grupo de administración de Kaspersky | Adminis  trador de la consola |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 28**

*Acciones Sugeridas para el Riesgo Error Humano*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OBJETIVO** Generar políticas que supervisen el manejo de sistemas operativos autorizados para evitar el tráfico de información infectada | | | | | | | | | | |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| I  m  p  r  o  b  a  b  l  e | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Respon  sabilida  des de la dirección | R  a  r  a  V  e  z | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Asumir el riesgo, | Supervisión constante a empleados y contratistas sobre el cumplimiento de las políticas de seguridad de la información implementadas por la Universidad | Equipo de talento humano |
| Concienti  zación, educa  ción y formación en seguridad de la informa  ción | Programación de capacitaciones y actualizaciones sobre seguridad de la información e innovaciones tecnológicas por parte de la dirección  Asistencia de los empleados a las capacitaciones programadas | Gestión Directiva |

**Tabla 28** (Continuación)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
|  |  |  | Equipa  miento desatendi  do por el usuario |  |  |  |  | El usuario debe cerrar cesión cuando finalice el uso de la red, conexiones o aplicaciones para proteger la información | Usuarios |
| Política de escrito  rios y pantalla limpios | Los usuarios deben asegurar los documentos escritos y medios extraíbles que contengan información | Superviso  res y usuarios |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 29**

*Acciones Sugeridas para el Riesgo Descarga y Uso de Activadores para algunos Programas*

|  |
| --- |
| **OBJETIVO** Crear políticas que promuevan el uso de software legítimo y adquisición de licencias |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| P  o  s  i  b  l  e | M  o  d  e  r  a  d  o | A  l  t  o | Restriccio  nes sobre la instala  ción de software | R  a  r  a  V  e  z | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Reducir el riesgo,  evitar,  compartir  o transferir | Crear directivas para controlar la instalación de software en los equipos registrados en el grupo de administración de Kaspersky | Adminis  trador de la consola |
| Controles ante el software malicioso | Protección y detección de amenazas ante software malicioso con el antivirus Kaspersky | Consola Kaspersky |
| Registro de eventos | Seguimiento de las alertas emitidas por la consola Kaspersky | Adminis  trador de la consola |

**Tabla 29** (Continuación)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
|  |  |  | Política sobre el uso de servicios de red |  |  |  |  | Cada usuario debe ingresar con la cuenta asignada a su cargo para acceder a la red | Usuarios |
| Política de control de acceso | Los usuarios que manejen información relevante o tengan acceso a sistemas críticos deben estar registrados en el grupo de administración de Kaspersky | Adminis  trador de la consola |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 30**

*Acciones Sugeridas para el Riesgo Permisos de Administrador en los Equipos*

|  |
| --- |
| **OBJETIVO** Formular proceso a seguir para la gestión de permisos |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| P  r  o  b  a  b  l  e | M  e  n  o  r | A  l  t  o | Política sobre el uso de servicios de red | R  a  r  a  V  e  z | M  e  n  o  r | B  a  j  o | Reducir el riesgo,  evitar,  compartir  o transferir | Cada usuario debe ingresar con la cuenta asignada a su cargo para acceder a la red | Usuarios |
| Política de control de acceso | Los usuarios que manejen información relevante o tengan acceso a sistemas críticos deben estar registrados en el grupo de administración de Kaspersky | Adminis  trador de la consola |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 31**

*Acciones Sugeridas para el Riesgo Falta de Documentación de Políticas en Seguridad de la Información*

|  |
| --- |
| **OBJETIVO** Formular proceso a seguir para la gestión de permisos |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| C  a  s  i  s  e  g  u  r  o | M  o  d  e  r  a  d  o | E  x  t  r  e  m  o | Procedi  mientos documen  tados de operación | R  a  r  a  V  e  z | M  o  d  e  r  a  d  o | A  l  t  o | Reducir el riesgo,  evitar,  compartir  o transferir | Todos los procesos que afecten o protejan la información deben estar documenta  dos y disponibles | Usuarios |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores

**Tabla 32**

*Acciones Sugeridas para el Riesgo Carencia de Actualización Profesional*

|  |
| --- |
| **OBJETIVO** Programar capacitaciones sobre el software, código seguro e innovaciones tecnológicas |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CALIFICACION  **P I** | | Zona  de  riesgo | CONTROLES | NUEVA  CALIFICA  CION  **P I** | | Zona de riesgo | Medidas de respuesta | ACCIONES | RESPONSABLES |
| P  o  s  i  b  l  e | M  e  n  o  r | M  o  d  e  r  a  d  o | Respon  sabilida  des de la dirección | P  o  s  i  b  l  e | I  n  s  i  g  n  i  f  i  c  a  n  t  e | B  a  j  o | Asumir,  reducir el riesgo | Supervisión constante a empleados y contratistas sobre el cumplimiento de las políticas de seguridad de la información implementadas por la Universidad | Equipo de talento humano |
| Concienti  zación, educa  ción y formación en seguridad de la informa  ción | Programación de capacitaciones y actualizaciones sobre seguridad de la información e innovaciones tecnológicas por parte de la dirección  Asistencia de los empleados a las capacitaciones programadas | Gestión Directiva |

Fuente Guía controles de Seguridad y privacidad de la información Min tic, adecuación de los autores