UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: "Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador".

Proyecto de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ing. Hugo Patricio Heredia Mayorga

Director: PhD Vicente Rolando Merchán Rodríguez.

Ambato – Ecuador

2019

A LA UNIDAD ACADÉMICA DE TITULACIÓN de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación precedido por la ingeniera Elsa Pilar Urrutia, Mg, e integrado por los señores ingeniero Franklin Oswaldo Mayorga Mayorga, Mg., ingeniero Jaime Bolívar Ruiz Banda, Mg. designados por la *Unidad Académica de Titulación* de la Universidad Técnica de Ambato, para receptar el trabajo de investigación con el tema:" *Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador"* elaborado y presentado por el señor ingeniero, Hugo Patricio Heredia Mayorga, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del trabajo de investigación del Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

.....

Ing. Elsa Pilar Urrutia Urrutia, Mg.

Presidente del Tribunal

.....

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.

Miembro del Tribunal

.....

Ing. Jaime Bolívar Ruiz Banda, Mg.

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador, le corresponde exclusivamente a: Ingeniero, Hugo Patricio Heredia Mayorga, Autor bajo la Dirección del Ingeniero Vicente Rolando Merchán Rodríguez, PhD, Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero, Hugo Patricio Heredia Mayorga

CC: 1715590970

Ingeniero Vicente Rolando Merchán Rodríguez, PhD

CC: 1708003924

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como documento disponible para su lectura, consulta y procesos de investigación, según las normas de la institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

HEREDIA M.

Ingeniero, Hugo Patricio Heredia Mayorga

CC: 1715590970

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

AGRADECIMIENTO

La gratitud es uno de los dones más grandes del ser humano, consecuentemente quiero expresar el agradecimiento a todos quienes de una u otra manera me apoyaron en la consecución de este logro académico.

Quiero expresar mi eterno agradecimiento a mi madre Gloria, que ha sido un ejemplo de lucha y tenacidad, siendo mi ejemplo a seguir día a día en cada una de mis acciones.

Gracias, madre por todo lo que me enseñaste mientras estabas conmigo en este mundo terrenal.

Hugo Heredia Mayorga.

DEDICATORIA

Dedico este trabajo de investigación como un gesto de admiración y respeto a mi madre Gloria, que cuando estaba en curso de mis estudios partió de esta vida dejándome muchas enseñas.

A mi sobrino Sebastián quien me enseño que siempre se debe luchar en esta vida por cumplir sus sueños e ideales.

Hugo Heredia Mayorga.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADOS
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador

AUTOR: Ingeniero, Hugo Patricio Heredia Mayorga
DIRECTOR: Ingeniero, Vicente Rolando Merchán Rodríguez, PhD
FECHA:

RESUMEN EJECUTIVO

Las Instituciones de Educación Superior se han visto continuamente amenazadas ante la falta de dirección y control desde la óptica de la seguridad de la información en el contexto del gobierno de tecnologías de la información. La norma ISO/IEC 27014:2013 representa una oportunidad para gobernar la seguridad de la información, sin embargo, adolece de clara alineación que permita articular sus actividades con el gobierno de tecnologías de la información y brindar visibilidad al gobierno organizacional.

Este estudio ha llevado adelante un proceso de armonización entre los estándares ISO/IEC 27014:2013 e ISO/IEC 38500:2015 con el propósito de identificar problemas de sobre posición y elementos fuertemente relacionados que coadyuve a un modelo consistente de gobierno de seguridad de la información en tres niveles: principios (responsabilidad, desempeño, estrategia, análisis de riesgos, conformidad y comportamiento humano), objetivos e indicadores.

Como resultado, se han definido los componentes del modelo de gobierno de seguridad de la información fuertemente relacionados con el gobierno de

tecnologías de la información. Este trabajo contribuye al conocimiento y colaboración de quienes toman decisiones en los comités estratégicos de dirección y control de la seguridad de la información en las instituciones de educación superior del Ecuador.

Con los elementos determinados en la armonización de las normas y la importancia que tiene los activos de información que se genera en las funciones sustantivas de docencia, investigación y vinculación se ha estructurado el Modelo de Gobierno de Seguridad de la Información para las Instituciones de Educación Superior MoGSIIES.

Este modelo considera los aspectos de información, talento humano, infraestructura y estrategia por el parte de las IES, y como resultado de la armonización de dichos modelos se considera los principios y objetivos. La validación del modelo por partes de expertos mediante el coeficiente V de Aiken permitió estadísticamente comprobar la validez del modelo.

Trabajos futuros se enfocarán en el análisis factorial de componentes del modelo con la participación de actores de las instituciones, con el fin de afianzarlo hacia lo que efectivamente las instituciones no pueden dejar de prescindir

Descriptores: Seguridad de la Información, Gobierno de Seguridad de la Información, Gobierno de Tecnologías de la Información, Funciones Sustantivas, Activos de Información.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADOS
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

The information Security Government Model for Higher Education Institutions of Ecuador

AUTHOR: Ingeniero, Hugo Patricio Heredia Mayorga
DIRECTED BY: Ingeniero, Vicente Rolando Merchán Rodríguez, PhD
DATE:

EXECUTIVE SUMMARY

Institutions of Higher Education have been continually threatened by the lack of direction and control from the perspective of information security in the context of information technology governance. ISO/IEC 27014:2013 represents an opportunity to govern information security, however, it lacks a clear alignment to articulate its activities with IT governance and provide visibility to organizational governance.

This study has carried out a harmonization process between the ISO/IEC 27014:2013 and ISO/IEC 38500:2015 standards with the purpose of identifying overlapping problems and strongly related elements that contribute to a consistent information security governance model at three levels: principles (responsibility, performance, strategy, risk analysis, compliance and human behavior), objectives and indicators.

As a result, the components of the information security governance model have been defined strongly related to information technology governance. This work contributes to the knowledge and collaboration of decision-makers in the strategic

steering and control committees for information security in Ecuador's higher education institutions.

With the elements determined in the harmonization of standards and the importance of the information assets generated in the substantive functions of teaching, research and networking, the design of the Government Model of Information Security for Higher Education Institutions MoGSIIES has been structured.

This model considers the aspects of information, human talent, infrastructure and strategy on the part of IES, and as a result of the harmonization of these models, the principles and objectives are considered. The validation of the model by experts using Aiken's V coefficient allowed the validity of the model to be statistically verified.

Future work will focus on factorial analysis of components of the model with the participation of actors from the institutions, in order to consolidate it towards what institutions cannot do without.

Keywords: Information Security, Information Security Government, Information Technology Government, Substantive Functions, Information Assets.

INTRODUCCIÓN

El crecimiento de las Tecnologías de la Información y Comunicaciones (TIC) está obligando a plantear nuevos mecanismos que garanticen la transversalidad en el desarrollo del Ecuador.

Este avance vertiginoso trae consigo grandes interrogantes en términos de seguridad de la información. Padilla-Verdugo, Cadena-Vela, Enríquez-Reyes, Córdova-Ochoa, y Llorens-Largo (2018) en su trabajo de investigación, estado de las tecnologías de la información y comunicación en las universidades ecuatorianas en la sección 3.7 establecen que "existen amenazas, eventos o incidentes contra la integridad, disponibilidad y confiabilidad de los datos" (p. 71). Por lo tanto, la presente investigación propone un modelo de Gobierno de seguridad de la información para las instituciones de educación superior del Ecuador alineado a los objetivos de la institución para crear valor y reducir el impacto en los servicios y manejo de la información que prestan las instituciones educativas de nivel superior.

Si se traslada los elementos contenidos en los modelos de gestión de TI que tiene Cobit, la ISO 38500, conjuntamente con los modelos de gobernanza de seguridad de la información de la ISO 27014, surge la idea de un modelo de Gobierno de Seguridad de la Información que articule espacios de colaboración conjunta entre los actores principales de las instituciones de educación superior (Padilla-Verdugo et al., 2018a).

El objetivo principal de la presente investigación es proponer un modelo de Gobierno de Seguridad de la Información para las instituciones de educación superior del Ecuador que genere valor de forma conjunta con las estrategias organizacionales.

Para lograr este fin, se ha contextualizado y determinado el problema, se lo ha delimitado y se han planteado las interrogantes y los objetivos que permitieron desarrollar la investigación. En el presente estudio se aborda temas como: la

fundamentación filosófica y legal, el planteamiento de la hipótesis y determinación de las variables.

El enfoque y tipo de la investigación son analizados para determinar la población y muestra, así como, la operacionalización de las variables junto con su plan de recolección y procesamiento de la información. Posteriormente se definen los recursos, el cronograma y la bibliografía que sustentará el trabajo que se va a realizar.

CAPÍTULO 1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de investigación

Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador.

1.2 Planteamiento del Problema

1.2.1 Contextualización

El Gobierno de Tecnologías de la Información es una responsabilidad del nivel directivo de las instituciones de educación superior. Por tanto, su éxito va estar ligado a la comprensión y apoyo que obtenga de su parte (Martínez, 2009a).

Todas las organizaciones incluidos los centros de educación superior (universidades, institutos técnicos, tecnológicos, pedagógicos y artes) generan gran cantidad de información en las actividades que realizan (académicas, investigativas, de vinculación, administrativas y financieras) (Consejo de Educación Superior, 2013). Si estas no son gestionadas de forma eficiente e integrada pueden acarrear grandes pérdidas de información y repercusiones en gastos económicos de los cuales difícilmente las instituciones se podrían recuperar.

Marulanda Echeverry y López Trujillo (1995) en su trabajo de investigación manifiestan que para la implantación de cualquiera de los modelos de gobierno de Tecnologías de la Información se requiere entender que las organizaciones son un todo. La gobernanza en Tecnologías de la Información y Comunicación está cada vez más alineada con la estrategia organizacional, la aplicación de los estándares y/o normativas, las que deben estar articuladas a las funciones sustantivas para direccionar a las instituciones de educación superior a una economía del conocimiento capaz de generar valor agregado a los datos e información.

Por su parte, Cairo, Puga, Mallea, Cobas, y Sánchez (2016) establecen que para implementar una gestión automatizada de controles de seguridad informática dentro del contexto del Gobierno de Tecnologías de la Información es importante la combinación de varios métodos, gobernados a través de un manejo adecuado de riesgos durante las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información.

Las Tecnologías de la Información dentro de las Instituciones de Educación Superior proporcionan grandes beneficios y también nuevos desafíos. Uno de estos está muy relacionado con la protección y privacidad de la información personal de los estudiantes, docentes y personal administrativo; sobre todo lo que tiene que ver con los datos de las actividades académicas, investigativas y de vinculación, entre otros (Pillo-Guanoluisa y Enríquez-Reyes, 2017).

Por otro lado, Martínez (2009) sostiene en su tesis Doctoral "Análisis, Planificación y Gobierno de las Tecnologías de la Información en las Universidades" que uno de los aspectos que se deben gestionar en las universidades es el riesgo en los aspectos tecnológicos y organizacionales, tanto a nivel interno como externo. Dado que esto puede afectar e impactar negativamente en las actividades y procesos poniendo en peligro la consecución de sus ejes estratégicos, así como, sus objetivos institucionales.

En función de lo anterior, las Instituciones de Educación Superior deben preservar su valor de negocio, proteger sus activos de información y conservar la continuidad de los servicios. Al diseñar sus estrategias futuras, las instituciones deben evaluar los nuevos riesgos que aparecen a partir de la incorporación de las Tecnologías de la Información y revisar las políticas y procesos de gobernanza de seguridad de la información (Martínez, 2009).

Padilla-Verdugo, Cadena-Vela, Enríquez-Reyes, Córdova-Ochoa, y Llorens-Largo (2018) en su investigación "Estado de las Tecnologías de la Información y Comunicación en las Universidades Ecuatorianas" exponen en los resultados que

existen procesos de Tecnologías de la Información y Comunicación que tienen una baja implementación como la gestión de aceptación del cambio y cultura del uso de las Tecnologías de la Información y Comunicación. Además, los componentes de Tecnologías de la Información y Comunicación dentro de la institución engloban elementos relacionados con la planificación, control y gestión. Los indicadores que se manejan toman en cuenta seis dimensiones de Tecnologías de la Información y Comunicación que son: organización, servicios generales, servicios para la docencia y la investigación, sistemas de información, infraestructura y seguridad (Padilla-Verdugo et al., 2018). Pero ninguno de ellos aborda elementos como el gobierno y gestión de Tecnologías de la Información peor aún un gobierno de seguridad de la información.

1.2.2 Análisis crítico

La información es uno de los activos más importantes de toda organización, en especial de las Instituciones de Educación Superior. La información que se genera resultado de las actividades de docencia, trabajo práctico, trabajo autónomo, investigación, vinculación, gestión administrativa y financiera debe ser gestionada mediante el establecimiento de políticas y normas que regulen la privacidad, confidencialidad e integridad de la misma. Estos elementos deben formar parte de un marco de gobierno de TI de tal manera que se garanticen los controles de auditoría de los procesos administrativos, académicos y financieros.

Al no contar con un modelo de Gobierno de Seguridad de la Información, las instituciones de educación superior corren el riesgo de que sus activos de información no sean tratados con la debida confiabilidad, integridad y disponibilidad. Esto podría derivar en problemas en la prestación de los servicios a los estudiantes, docentes y público en general incumpliendo de esta manera con las leyes y reglamentos que establecen los entes reguladores de la educación superior.

1.2.3 Prognosis

De no definirse un Modelo de Gobierno de Seguridad de la Información que establezca las normas, políticas y procedimientos de gobernanza para la gestión, disponibilidad, fiabilidad de los activos de información de las instituciones de educación superior, se corre el riesgo de sufrir accesos indebidos a la información, tanto interna como externa. Además, se podría perder información vital para los procesos de acreditación que exige el Consejo de Aseguramiento de la Calidad de Educación Superior (CACES).

1.2.4 Formulación del Problema

¿Cómo definir con criterio de rigurosidad a un Gobierno de Seguridad de la Información que minimice el impacto y la probabilidad de amenazas y riesgos potenciales a las que se ven expuestas las instituciones de educación superior del Ecuador?

1.2.5 Interrogantes (Subproblemas)

- ¿Cómo definir los elementos que componen a un Modelo de Gobierno de Seguridad de la Información a fin de garantizar la disponibilidad, integridad y accesibilidad en el uso estratégico de las TI en las instituciones?
- ¿Cómo estructurar un Modelo del Gobierno de Seguridad de la Información para instituciones de educación superior a fin de promover los beneficios en el uso de las TI?

1.2.6 Delimitación del objeto de investigación

Campo: Tecnologías de la Información y Comunicación
Área: Innovación basada en Tecnología.
Aspecto: Modelo de Gobierno de Seguridad de la Información

1.2.6.1 Delimitación Espacial:

Instituciones de educación superior del Ecuador

1.2.6.2 Delimitación Temporal:

Desde octubre 2018 hasta noviembre 2019

1.2.6.3 Unidades de Observación:

Instituciones de educación superior del Ecuador.

1.3 Justificación

El uso de las Tecnologías de la Información y Comunicación (TIC) ha ido tomando un gran impulso en la sociedad del conocimiento, así como también, ha transformado la vida de las personas y por ende, el cómo se hace las cosas.

Si se compara la evolución de las Tecnologías de la Información y Comunicación y la educación se puede notar que estas no pueden ser fijas, cerradas y aisladas de este vertiginoso avance. Llorens, Bayona, Gomez, y Sanguino (2010) resaltan que los sistemas de información con los que trabaja la Universidad de Alicante están interconectados y se alimentan entre sí como un motor de innovación educativa y de difusión abierta de la producción docente y científica.

Además, Bayona Soto, Lastra Colobon, y Trigos Sánchez (2014) señalan que los involucrados en procesos de gobernanza de Tecnologías de la Información deben tener un conocimiento sobre la funcionalidad de cómo, los sistemas de gestión sobre políticas, procesos y estructuras que dan soporte al gobierno corporativo de Tecnologías de la Información y la Comunicación deben alinearse con el gobierno Corporativo de la institución de educación superior, en el marco de los procesos estratégicos, misionales y de apoyo. Todo ello, como un componente para la toma de decisiones en todos los servicios que se ofertan, así como también, para tener la disponibilidad y confiabilidad de la información que se genera dentro de los procesos organizacionales.

Aliaga Flores (2013) sostiene que la seguridad de información dejará de ser una actividad poco organizada y apoyada por los miembros de las instituciones de Educación Superior. Lo que demuestra una etapa de madurez del gobierno de la Tecnología de Información (Armendáris y López, 2017) al ser un conjunto de actividades metódicas y controladas que han logrado instalarse en la cultura organizacional e incluir a todos los empleados del instituto sus protagonistas y responsables (Aliaga Flores, 2013).

Para las instituciones de educación superior contar un modelo de Gobierno de Seguridad de la Información que permita la interoperabilidad, transparencia, manejo y acceso libre a la información es importante e indispensable para cumplir con las políticas y objetivos institucionales, y de esta manera, garantizar la confiabilidad y disponibilidad de la información en cada uno de los procesos que gobiernan su accionar organizacional.

Finalmente, el diseñar un Modelo de Gobierno de Seguridad de la Información permite a las organizaciones mantener una ventaja competitiva (Melorose, Perroy, y Careas, 2015) mediante una integración sistemática de los datos que se producen en las actividades de docencia, trabajo práctico, trabajo autónomo, investigación, vinculación, gestión administrativa y financiera. Todo ello, de una manera controlada y metódica, de tal forma que los niveles de confiablidad de la información se enmarquen en procesos, políticas y procedimientos de gobernanza de seguridad de la información que se ajusten a sus realidades organizativas.

Por lo descrito en los párrafos anteriores se puede determinar que el proyecto es factible, pues se puede disponer de los recursos técnicos, operativos y económicos para llevarlo a cabo.

- **Factibilidad Técnica:**

  La investigación cuenta con los recursos tecnológicos necesarios en cuanto a infraestructura, sistemas de información, accesos a datos e información requerida.

- **Factibilidad Operativa:**

  El apoyo por parte de las autoridades de la institución de la unidad de observación es de vital importancia para la consecución operativa del proyecto, así como también, de las direcciones de acreditación, vicerrectorados académico y tecnológico, y cada una de las unidades académicas y departamentos, quienes se constituyen como proveedores directos de los datos e información.

- **Factibilidad Económica:**

  Se puede mencionar que económicamente el presente proyecto es factible ya que los costos que implican el análisis, estudio, tiempo empleado son asumidos por el investigador, mientras que costo del tiempo del personal de la institución involucrado es asumido por la unidad de observación de la investigación.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar un modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador.

1.4.2 Objetivos Específicos:

- Analizar formalmente el domino de Gobierno de Seguridad de la Información.
- Realizar el proceso de Armonización de los Modelos de Gobierno de TI ISO/IEC 38500:2015 e ISO/IEC 27014:2013.
- Diseñar un modelo que sostenga el funcionamiento del gobierno de seguridad de la información en las Instituciones de Educación Superior del Ecuador.
- Validar el modelo de gobierno de seguridad de la información por expertos de instituciones de educación superior.

CAPÍTULO 2. MARCO TEÓRICO

2.1 Antecedentes de Investigativos

Un modelo de Gobierno de seguridad de la Información, para las instituciones de Educación Superior, debe tener componentes estratégicos fundamentados por el alineamiento al Plan Estratégico, la participación del nivel Directivo en las decisiones de TI; también componentes tácticos enfocados por el cumplimiento de regulaciones, costo, eficiencia de los requerimientos de información de la Institución; y componentes operativos soportados por los procesos de gobierno y la gestión de seguridad y de TI (Cordero Guzmán, 2015).

Sin embargo, Morales Andaluz (2015) afirma que el principal problema para la implementación del gobierno de seguridad de la Información y de TI en las IES es que no existe una metodología clara y definida para el efecto. Es importante que se establezcan políticas que generen confianza entre los beneficiarios y autoridades, para lo cual es necesario contar con modelos específicos y todas sus herramientas de implementación.

Padilla-Verdugo et al. (2018), en su trabajo UETIC 2017 habla de la complejidad de los procesos críticos de TIC y el cumplimiento de las políticas de seguridad que determinan la necesidad de contar con un responsable de la seguridad de la información. Con el objeto de controlar y garantizar la seguridad de la información frente a las diferentes amenazas e incidentes, así como para determinar las oportunidades de mejora, es importante contar con un modelo de gobierno de seguridad de la información que permita no solo la interacción de los procesos sino que enfoque su trabajo en la Seguridad de la Información y de sus activos.

Uno de los elementos claves en la adopción de un modelo de Gobierno de seguridad de la información según A. Fernández, Llorens, Fernández Martínez, y Llorens Largo (2011) es establecer la madurez de los procesos gobernantes con el fin de mejorar e intensificar la participación de todos los actores. Para facilitar el proceso

de adopción se debe crear un Comité de Gobierno de las TI en cada Institución de Educación Superior, mismo que, debe estar integrado por todos los responsables TI de la institución, las autoridades y demás integrantes.

Más allá del concepto teórico o metafórico de gobierno se seguridad de la información, se necesitan propuestas que avancen en su implementación e implantación en contextos reales. En este sentido, existen propuestas como el proyecto *Arranque* que ha permitido a todos los participantes conocer las ventajas de contar con un sistema de gobierno de TI (Fernández Mayor y Martínez Fernández, 2010), el mismo que tiene que ver con el proyecto GTI4U de la Universidad de Alicate.

Los estudios sobre gobiernos de seguridad de la información son escasos y en muchas ocasiones son teóricos, es decir, sin ninguna implantación o resultados. En Latinoamérica no existe un modelo que permita a las instituciones de educación superior medir su etapa de madurez y la capacidad en la definición de los aspectos de gobernabilidad de seguridad de la información como lo sostiene Torres Bermúdez y Lucumí Sánchez (2015) en su trabajo de investigación.

El resultado más relevante del trabajo realizado por Buitrago, Bonilla, y Murillo es que los procesos de gobernabilidad deben ser dinámicos y fácilmente adaptables a los cambios, basados en la mejora continua y con un enfoque sistémico, como el que propone la norma ISO/IEC 27001 (Buitrago, Bonilla, y Murillo, 2012).

Si se logra un modelo que además de gobernar los procesos de seguridad de la información mediante un análisis de riesgos, maneje la seguridad de la información, se podrá apoyar a los procesos de gestión de conocimiento, la integración de cada uno de sus componentes y su evolución tanto individual como colectiva (García-Holgado y García-Peñalvo, 2015). Este no será un tema que competa solo a los departamentos de tecnologías sino que involucre a toda la organización (Berrío López, 2016).

En el ámbito educativo es importante diseminar el conocimiento acerca de los marcos de gobierno de seguridad de la información y las normas que permiten su implementación. Para Vargas-Bermúdez (2015) el proceso de gobernanza de seguridad de la información es un proyecto a largo plazo, que implica un arduo trabajo por parte de los funcionarios involucrados en el área de TI, de los directivos, de los administrativos y de los clientes. Lo más importante es cumplir con las cinco áreas focales (Alineamiento estratégico, Entrega de valor, Administración de riesgos, Administración de recursos y Medición del desempeño) de los niveles de madurez de los procesos de gobernanza, sin importar que marco de control se utilice.

2.2 Fundamentación Filosófica

La presente investigación se enmarca en el paradigma *Crítico Propositivo*: es crítico porque realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al mismo.

2.3 Fundamentación Legal

Uno de los ejes estratégicos críticos de las Instituciones de Educación Superior es la calidad, y excluir a las Tecnologías de la Información y Comunicación de este proceso no es una opción. Es por eso que se ha impulsado a la calidad de la Educación Superior desde la reforma constitucional del 2008 y se le ha dado viabilidad a través de la nueva Ley Orgánica de Educación Superior (Cordero Guzmán, 2015).

Los cambios y transformaciones internas de las Instituciones de Educación Superior son cada vez más intensos, pues están orientados a cumplir con los indicadores de los modelos de acreditación impuestos por los organismos de control de la calidad en la educación.

En la **Constitución Política de la República del Ecuador** se habla de la calidad de la educación (Constitución de la República del Ecuador, 2008) en el capítulo segundo sección quinta – Artículo 26 "… Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir…" (Constitución de la República del Ecuador, 2008).

De la misma manera en el Artículo 27 se establece que "La educación es indispensable para el conocimiento, el ejercicio de los derechos y la construcción de un país soberano, y constituye un eje estratégico para el desarrollo" (Constitución de la República del Ecuador, 2008).

Por otro lado, en el Capítulo sexto – Derechos de libertad, en el artículo 66 se reconoce y garantiza a las personas "El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica. Es necesario mencionar que para la publicación de cierta información personal es necesario tener autorización por parte del titular para así evitar problemas judiciales" (Constitución de la República del Ecuador, 2008).

En el Título V – Calidad de la Educación Superior, Capítulo 1 – Principio de Calidad, el Artículo 93 de la ley Orgánica de Educación Superior 2008 expresa claramente en forma textual "El principio de calidad consiste en la búsqueda constante y sistemática de la excelencia, pertinencia, producción, óptima, transición del conocimiento y desarrollo del pensamiento mediante la autocrítica, la crítica externa y el mejoramiento permanente" (LOES, 2008). En este sentido se busca generar un gobierno de seguridad de la información que garantice lo expresado en la Ley y además conlleve a trabajar en la información veraz, disponible y confiable que los entes de regulación de la educación superior así lo requieran y dispongan.

2.4 Categorías Fundamentales

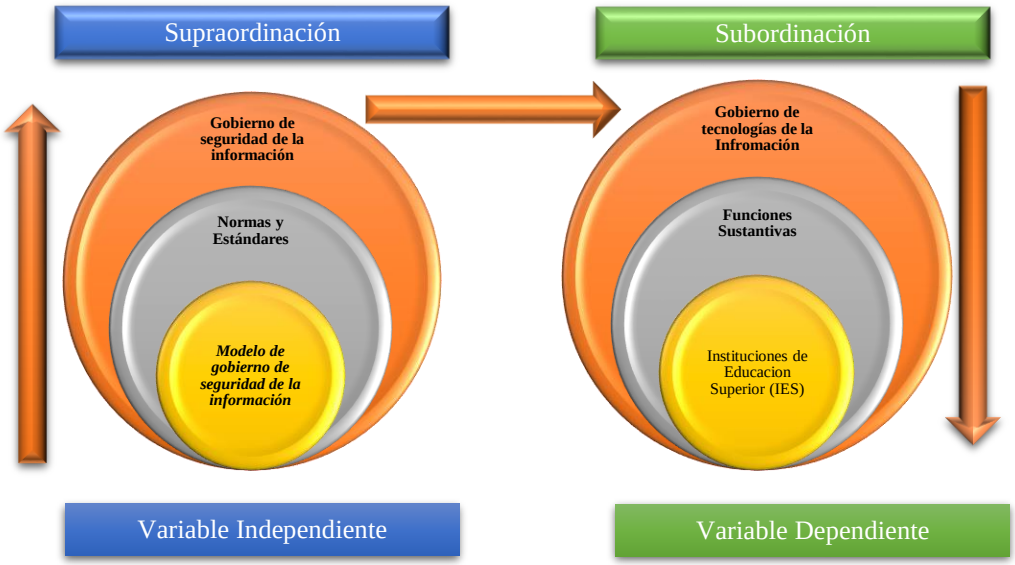

Gráfico 1. Inclusiones conceptuales

Elaborado por: El autor de la investigación

Constelación de Ideas, Mándala Variable Dependiente u otros

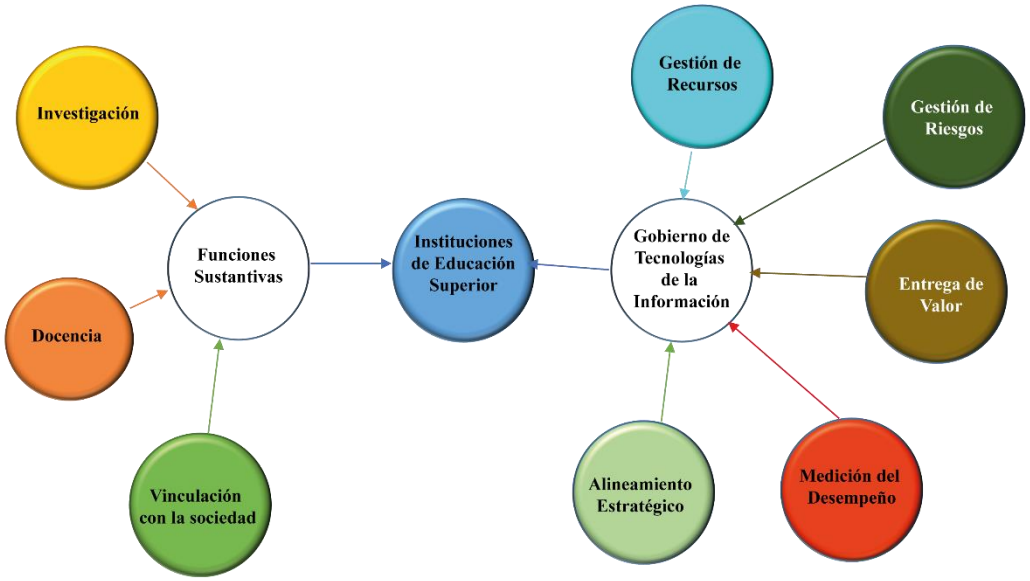

Gráfico 2. Constelación de Ideas de la Variable Dependiente

Elaborado por: El autor de la investigación

Constelación de Ideas, Mándala Variable Independiente u otros

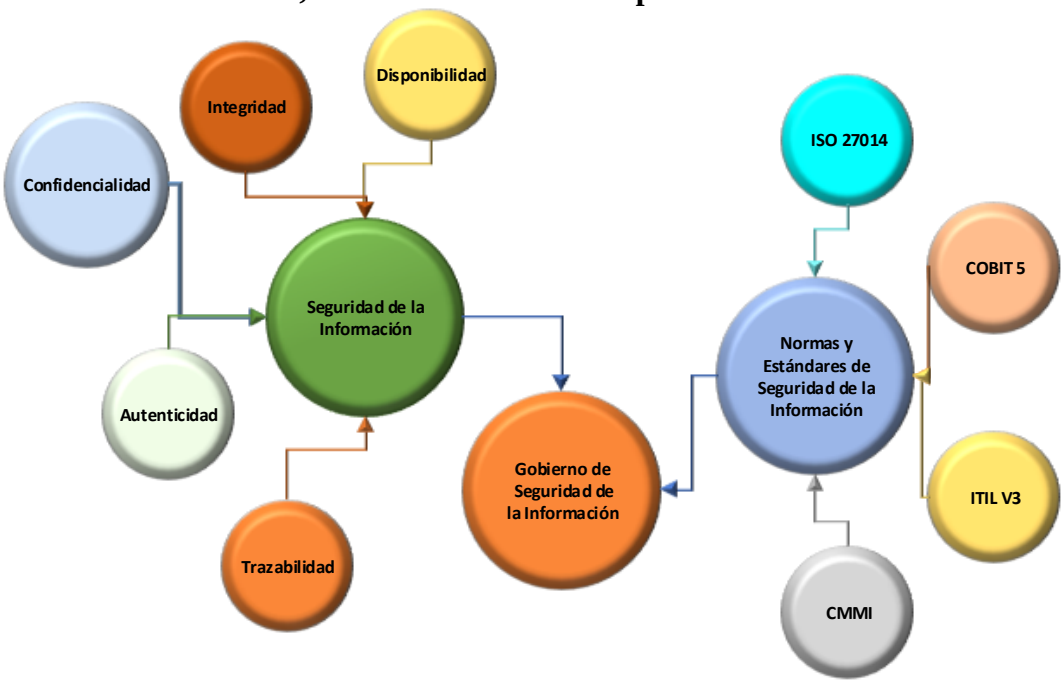

Gráfico 3. Constelación de Ideas de la Variable Independiente

Elaborado por: El autor de la investigación

2.4.1 Categorías de la Variable Dependiente

- **Gobierno de Tecnologías de la Información**

El concepto Gobierno de Tecnologías de la Información sirve para describir los componentes que aseguran la capacidad que tiene tecnología para mejorar las operaciones propias del negocio (Henderson y Venkatraman, 1999). Dicho concepto ha ido madurando a través del tiempo.

Para Zamora Jiménez (2010) el Gobierno TI es un marco de trabajo para la toma de decisiones y la asignación de responsabilidades para facilitar el resultado deseado respecto al uso de la TI.

Pérez Lorences y García Ávila (2013) en su trabajo de investigación hace referencia a que el gobierno de TI plantea un marco de responsabilidades

para fomentar el comportamiento que se desea tener sobre las Tecnologías de la Información para su desempeño eficiente y efectivo.

- **Normas y Estándares de Gobierno de Tecnologías de la Información**

La Organización Internacional de estandarización (ISO por sus siglas en inglés) establece un estándar sobre el gobierno corporativo de tecnologías de la información en su serie ISO 38500 cuyo objetivo es proporcionar los lineamientos necesarios para que las organizaciones puedan evaluar, dirigir monitorear el uso de tecnologías de la información (Periñán y Villegas, 2011).

Fernández y Piattini en su trabajo de modelo para el gobierno de las TIC en normas ISO sostienen que no solo se debe establecer un entorno de gobierno, sino que este, siempre debe estar acompañado de una gestión que permita que los procesos cumplan con los parámetros de un modelo de evaluación como la norma ISO 15504; en el caso de los activos de software la ISO 197770-1; y para la gestión de servicios la ISO 2000-1 (C. Fernández y Piattini, 2012).

- **Marcos de Referencia de Gobiernos de Tecnologías de la Información**

Un marco de referencia establece las mejores prácticas que han sido aprobadas, reconocidas y aceptadas internacionalmente (Vecino Pico, 2017).

Uno de los marcos de referencia que se utiliza comúnmente en el desarrollo de los procesos de gobernanza es ITIL, un conjunto de mejores prácticas enfocada a los servicios de TI (Periñán y Villegas, 2011). Por otro lado, Cobit apoya al gobierno de TI garantizando que las inversiones estén optimizadas y den lo mayores beneficios para la empresa, así como también, vinculen los objetivos de negocio con los objetivos de TI (Chaudhuri, 2011).

Por su parte, Quintanilla, (2016) en su trabajo "Modelo de referencia de gobierno de las tecnologías de la información para instituciones

Universitarias", muestra que existen muchos marcos de referencia de Gobierno de las TI, siendo el principal modelo el Control Objetives for Information Technology (Cobit) que brinda un marco de trabajo general que puede ser utilizado por cualquier tipo de empresa para implementar gobierno y gestión de las TI como parte del proceso de implantación de gobierno empresarial.

Mientras tanto, OpenGrupo en su guía de bolsillo de TOGAF versión 9.1 manifiesta que una herramienta para la creación de una arquitectura empresarial es el uso de herramientas tecnológicas, cuyo modelo interactivo de procesos se apoye en las mejores prácticas existentes (OpenGroup, 2013).

- **Funciones Sustantivas**

  De acuerdo al artículo 4 del reglamento de régimen académico que textualmente establece:

  > *"Las funciones sustantivas que garantizan la consecución de los fines de la educación superior, de conformidad con lo establecido en el Artículo 117 de la LOES, son las siguiente:*
  >
  > *a)* ***Docencia.*** *- La docencia es la construcción de conocimientos y desarrollo de capacidades y habilidades, resultante de la interacción entre profesores y estudiantes en experiencias de enseñanza-aprendizaje; en ambientes que promueven la relación de la teoría con la práctica y garanticen la libertad de pensamiento, la reflexión crítica y el compromiso ético.*
  >
  > *b)* ***Investigación****. - La investigación es una labor creativa, sistemática y sistémica fundamentada en debates epistemológicos y necesidades del entorno, que potencia los conocimientos y saberes científicos, ancestrales interculturales. Se planifica de acuerdo con el modelo educativo, políticas, normativas, líneas de investigación y recursos de las IES y se implementa mediante programas y/o proyectos desarrollados bajo principios éticos y prácticas colaborativas.*

c) ***Vinculación.*** *- La vinculación con la sociedad, como función sustantiva, genera capacidades e intercambio de conocimientos acorde a los dominios académicos de las IES para garantizar la construcción de respuestas efectivas a las necesidades y desafíos de su entorno. Contribuye con la pertinencia del quehacer educativo, mejorando la calidad de vida, el medio ambiente, el desarrollo productivo y la preservación, difusión y enriquecimiento de las culturas y saberes" (CES, 2019).*

Categorías de la Variable Independiente

- **Gobierno de Seguridad de la información**

  Según Meyer (2014) las decisiones propias de la seguridad de la información deben responder a un esquema de gobierno de seguridad de la información, misma que debe alinearse a las estrategias y los objetivos del negocio proporcionando capacidad para la toma de decisiones estratégicas corporativas.

  La ISO 270014 define un escenario, donde el monitoreo de la gestión es una responsabilidad del gobierno. Además, esta norma proporciona conceptos y principios para que las organizaciones puedan evaluar, dirigir, monitorear y comunicar todas y cada una de las actividades relacionadas con la seguridad de la información en torno a la organización (ISO, 2013).

- **Seguridad de la Información**

  De acuerdo a la Organización Internacional de estandarización (ISO por sus siglas en inglés) la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad (ISO, 2013), así como, la de los sistemas implicados en su tratamiento, dentro de una organización.

  Así pues, la seguridad de la información considera todos los elementos tecnológicos, procesos organizacionales y los responsables; dado que

proveer de contraseñas e instalar corta fuegos no son suficientes para gestionar las amenazas sobre el manejo de la información (Cárdenas-Solano, Martínez-Ardila, y Becerra-Ardila, 2016).

En el trabajo realizado por Cárdenas-Solano et al. (2016) se afirma que existen investigaciones donde se han definido los elementos estructurales de la seguridad de la información y cómo una organización debería implementarlos (Thiagarajan, 2006). Dichos elementos estructurales de seguridad de la información se conciben como los principios para su implementación y mantenimiento.

De acuerdo a lo anterior, la seguridad de la información al ser potenciada con el concepto de Gobierno de la Seguridad de la Información puede acelerar y reconocer la percepción de cómo la seguridad es un problema de IT (Meyer, 2014).

- **Normas y estándares de seguridad de la información**

  Es indudable que una de las normas que aborda el concepto de seguridad de la información es la norma ISO/IEC 27000. Según Valencia Duque y Orozco – Alzarte, "…la familia ISO/IEC 27000 para llevar a cabo la implementación de un sistema de gestión de seguridad de la información, se pone de manifiesto una complejidad adicional al proceso de desarrollo de un sistema de gestión de seguridad de la información..." (Valencia Duque y Orozco-Alzate, 2017).

  Velasco Melo (2008) sostiene que las Tecnologías de la Información y las Comunicaciones deben tener respuestas a los nuevos retos que se enfrenta en función del avance tecnológico y para ello deben generarse elementos jurídicos enmarcados dentro de la norma ISO/IEC 27000; para lo cual se debe capacitar y entrenar a todos los involucrados con el fin de apoyar a la sociedad en la solución de las problemáticas derivadas del uso de la tecnología.

En la conferencia realizada por Yory (2006) sobre un acercamiento a las mejores prácticas de seguridad de la información internacionalmente reconocidas en el estándar ISO 17799, él manifiesta que este ofrece recomendaciones importantes al momento de realizar una gestión de seguridad en las organizaciones.

Para Meyer (2014) todas las publicaciones de seguridad de la información comprenden un conjunto de familias entre las que se encuentran la ISO 27000 que contiene un vocabulario en el que se apoyan el resto de normas, la ISO 27001 que describe los requisitos para implementar un SGSI, la ISO 27002 que recopila las buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control, la ISO 27005 que recoge un conjunto de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones y, finalmente, la ISO 27014 que aborda la conceptualización de un gobierno de seguridad de la información.

- **Modelo de Gobierno de Seguridad de la Información**

Martelo, Maderay, y Betín (2015) en su artículo sostienen que un Modelo de Gobierno de Seguridad de la Información es un conjunto de políticas que asegura, construye, desarrolla, y mantiene la seguridad tanto en el hardware como en el software**.**

Para Camacho (2008) un Modelo de Gobierno de Seguridad de la Información busca proteger el activo más importante dentro de las organizaciones, conociendo los riesgos y minimizándolos, con el propósito de garantizar la continuidad del negocio.

Ochoa Arévalo (2015) en su trabajo de investigación "Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio"

concluye que todo el entorno de la seguridad de la información se lo debe concebir como un Gobierno, en cuyo marco regulatorio, la responsabilidad directa la tienen la Junta Directiva y la Gerencia Ejecutiva.

El trabajo realizado por McDermid, Mahncke, y Williams (2010) demuestra la viabilidad de establecer en SGSI como un marco de gobernanza que permita evaluar la seguridad de la información.

Por otro lado, Salazar y Campos (2009) mencionan los aspectos que involucran un modelo de seguridad de la información, el mismo que debe ser totalmente predecible, ajustable. Dicho modelo puede ser dimensionado conforme a la particularidad de la organización y servir de base para establecer un Gobierno de TI.

2.5 Hipótesis

H1: Una solución de gobierno de seguridad de la información fortalece los aspectos de gobernanza que se relacionan con los activos de seguridad de la información en las Instituciones de Educación Superior del Ecuador.

2.6 Señalamiento de Variables

Variable Independiente: Modelo de Gobierno de Seguridad de la Información

Variable Dependiente: Instituciones de Educación Superior

CAPÍTULO 3. METODOLOGÍA

3.1 Enfoque

El trabajo de investigación tiene un enfoque mixto, cuantitativo porque se van a medir parámetros que permitan contrastar la variable independiente; y es cualitativo porque se emitirá juicios de valor con expertos respecto al modelo de gobierno de seguridad de la información para Instituciones de Educación Superior.

3.2 Modalidad básica de la investigación

Investigación Bibliográfica

La investigación será bibliográfica, ya que se realizará una recopilación de referencias que sustenten el trabajo a través de artículos, ponencias, leyes y reglamentos. De esta manera se establecerá el marco teórico de las variables de la investigación.

Investigación de Campo

La investigación será también de campo porque se buscará obtener información respecto a qué tipo de modelo de Gobierno de TI es el más adecuado para las instituciones de educación superior.

3.3 Nivel o tipo de investigación

Investigación Correlacional

La investigación será correlacional puesto que toma en cuenta las dos variables de la investigación para relacionarlas y comprobar sus efectos; lo que dará como resultado un modelo de gobierno de seguridad de la información efectivo para las Instituciones de Educación Superior.

3.4 Población y Muestra

El presente proyecto trabajará con una muestra de 165 instituciones de educación superior de 215 que existen en el sistema de educación superior en la formación técnica tecnológica calculados con un margen de error del 5%.

$$n = \frac{Z^2 p * q * N}{e^2(N-1) + Z^2 p * q}$$

donde:

Z =Nivel de Confianza

N = Población

p = Probabilidad a favor

q = Probabilidad en Contra

e = Error de estimación

Además se trabajará con siete de expertos que realizarán la validación del modelo de gobierno de seguridad de la información para las instituciones de educación superior. Estos expertos serán escogidos en función de su perfil y experiencia en temas de seguridad. Todo esto, con el fin de establecer los elementos de validez del modelo planteado.

3.5 Operacionalización de Variables

3.5.1 Variable Dependiente:

Tabla 1. Variable Dependiente: Instituciones de Educación Superior

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Se entenderá como Institución de Educación Superior a la conceptualización realizada por el artículo 14 de la ley orgánica de educación superior son Instituciones de educación superior las universidades, escuelas politécnicas pública y privadas, debidamente, así como los institutos y conservatorios superior evaluadas y acreditados	• Gestión Corporativa • Docencia • Investigación • Vinculación con la Sociedad	• Alineamiento Estratégico • Procesos de Gobernanza • Estructura y mecanismos de toma de decisiones • Creación de Valor de las TI • Gestión de Riesgos • Medición del desempeño	• Tiene acceso a la información requerida. • La información que dispone es confiable. • Qué herramientas utiliza. • Cómo calificaría el tiempo que emplea procesar los datos. • La información obtenida sirve de apoyo para la toma de decisiones.	• Encuesta

Elaborado por: Investigador

3.5.2 Variable Independiente:

Tabla 2. Variable Independiente: Modelo de Gobierno de Seguridad de la Información

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Se entenderá como Gobierno de Seguridad de la Información al conjunto de Políticas, procedimientos para garantizar la confiabilidad, disponibilidad e integridad de la información.	• Disponibilidad	• Disponibilidad de las Información • Utilidad de la información • Reutilización de la Información • Respaldos de Información	• Información producida por cada uno de los procesos que gobiernan las instituciones educación superior. • Políticas de gobierno seguridad de la información establecidas en las instituciones educativas. • Nivel de fomento a las actividades de reutilización de la Información	• Encuesta
	• Integridad	• Completitud de los Datos • Precisión de los Datos • Conformidad de los Datos	• Información producida por cada uno de los procesos que gobiernan las instituciones educación superior. • Políticas de gobierno seguridad de la información establecidas en las instituciones educativas. • Nivel de fomento a las actividades de reutilización de la Información.	
	• Confiabilidad	• Métodos de captura de la información • Verificación de la Información • Validación de la Información.	• Permiten evaluar la validez de la información que está siendo suministrada por los procesos gobernantes de las Instituciones de Educación Superior.	

Elaborado por: Investigador

3.6 Recolección de Información

La técnica para emplearse será la encuesta dirigida, para lo cual es necesario utilizar como instrumento un cuestionario de preguntas cerradas, lo que ayudará a la obtención más concreta de la información.

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Validación de expertos del Modelo de Gobierno de Seguridad de la Información
¿De qué personas u objetos?	Expertos en seguridad de la información
¿Sobre qué aspectos?	Elementos del modelo de Gobierno de Seguridad de la Información
¿Quién, Quiénes?	Investigador: Ing. Hugo Heredia Mayorga
¿Cuándo?	Primer trimestre del 2019
¿Dónde?	Instituciones de Educación Superior
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Encuesta Datos Estadísticos
¿Con qué?	Cuestionario
¿En qué situación?	Dentro del horario de trabajo con profesionalismo investigativo y absoluta confidencialidad y reserva.

3.7 Procesamiento y Análisis

- Revisión crítica de la información recogida, es decir, depuración de la información defectuosa, contradictoria, incompleta, no pertinente o con otras fallas
- Tabulación o cuadros de variables de la hipótesis y objetivos
- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en el análisis)
- Análisis de datos para presentación de resultados

CAPÍTULO 4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de los resultados

REM1: ¿La institución de educación superior asigna responsabilidades relacionadas con el gobierno de seguridad de la información a su cuerpo directivos?

Tabla 3. Resultados REM1

Respuesta	Porcentaje	Cantidad
SI	35,29%	40
NO	44,64%	76
(NS)	20,07%	19

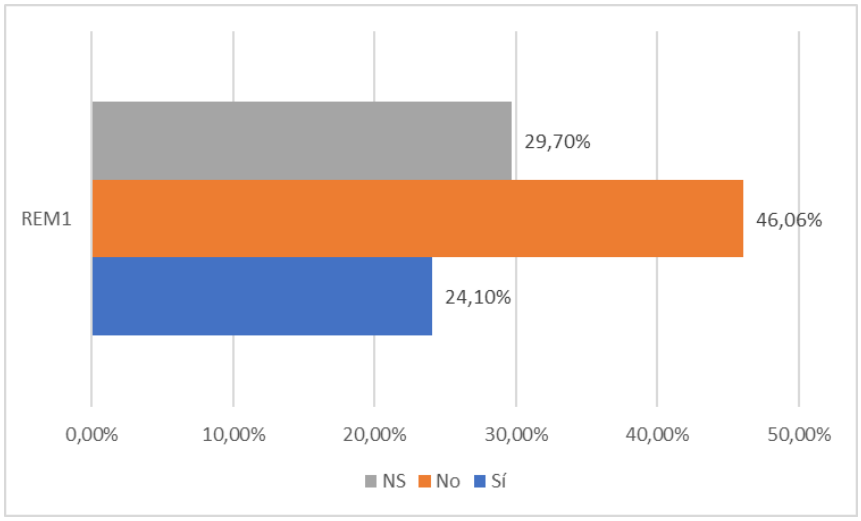

Gráfico 4. Resultados REM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 40 instituciones que representan el 24,10% indicaron que se ha asignado responsabilidades de seguridad de la información, el 46,06% que representa a 76 instituciones contestaron que no se han asignado ninguna responsabilidad de seguridad de la información y 49 no saben si existe o no responsabilidades lo que representa el 29,70%

INTERPRETACIÓN. – De acuerdo a los resultados presentados en la institución de educación superior se puede determinar que la institución de educación superior no asigna responsabilidades relacionadas con el gobierno de seguridad de la información a su cuerpo directivo.

REM2: ¿La institución de educación superior asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos?

Tabla 4. Resultados REM2

Respuesta	Porcentaje	Cantidad
SI	36,75%	61
NO	40,61%	67
(NS)	22,42%	37

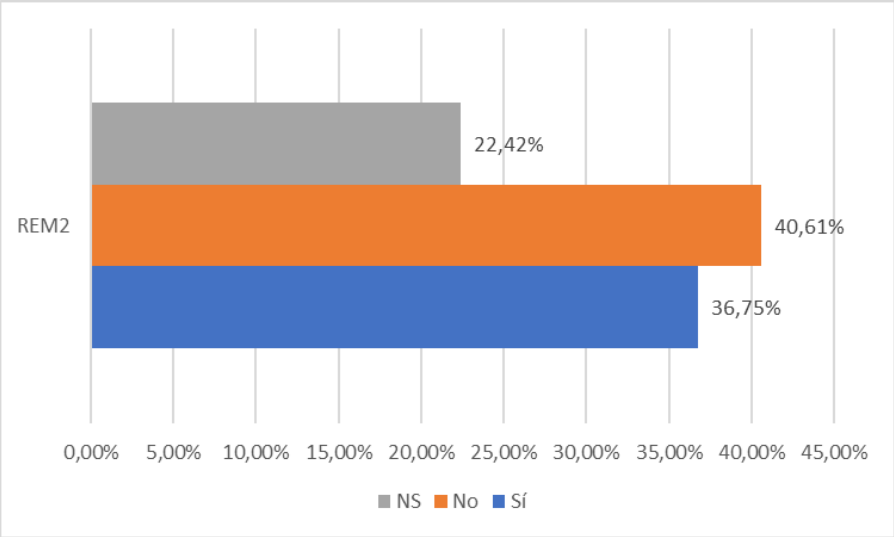

Gráfico 5. Resultados REM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 61 instituciones que representan el 36,75% indicaron que la institución de educación superior asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos, el 40,61% que representa a 67 instituciones desconocen que la institución de educación superior asigne responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos y 37 Instituciones de educación superior no saben absolutamente nada y representa el 22,42%

INTERPRETACIÓN. – De acuerdo a los resultados presentados las instituciones de educación superior no conocen como asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos.

REM4: ¿El cuerpo directivo de la institución de educación superior asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas para hacerlo?

Tabla 5. Resultados REM4

Respuesta	Porcentaje	Cantidad
SI	10,84%	18
NO	53,94%	89
(NS)	35,15%	58

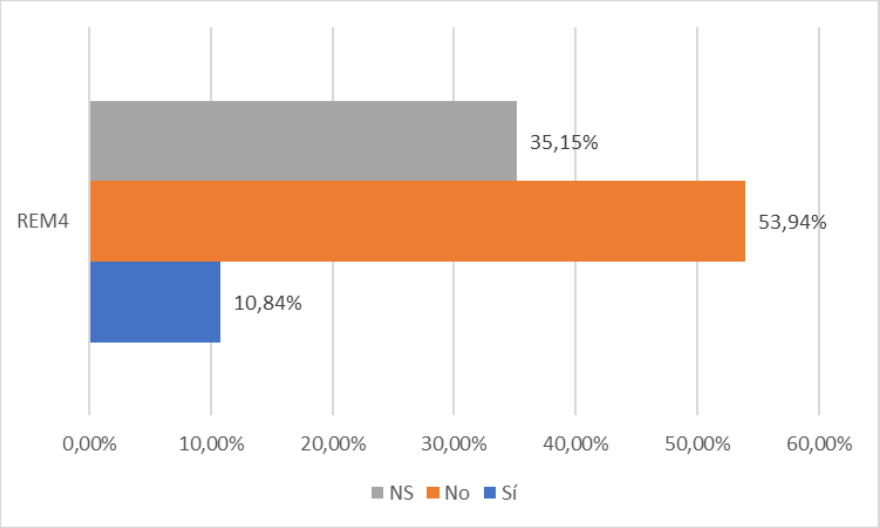

Gráfico 6. Resultados REM4

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 18 instituciones que representan el 10,84% indicaron que el cuerpo directivo de la institución de educación superior asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas para hacerlo, el 53,94% que representa a 89 instituciones desconocen si el cuerpo directivo de la institución de educación superior asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas y 68 instituciones desconocen si existen responsabilidades asignadas y representa el 35,15%.

INTERPRETACIÓN. – Los resultados determina que el cuerpo directivo de la institución de educación superior asignado para el manejo del gobierno de seguridad de la información no tiene las competencias adecuadas para hacerlo.

RDM1: ¿El cuerpo directivo encargado del gobierno de seguridad de la información supervisan los diferentes niveles de gestión de seguridad de la información?

Tabla 6. Resultados RDM1

Respuesta	Porcentaje	Cantidad
SI	19,88%	33
NO	67,88%	112
(NS)	12,12%	20

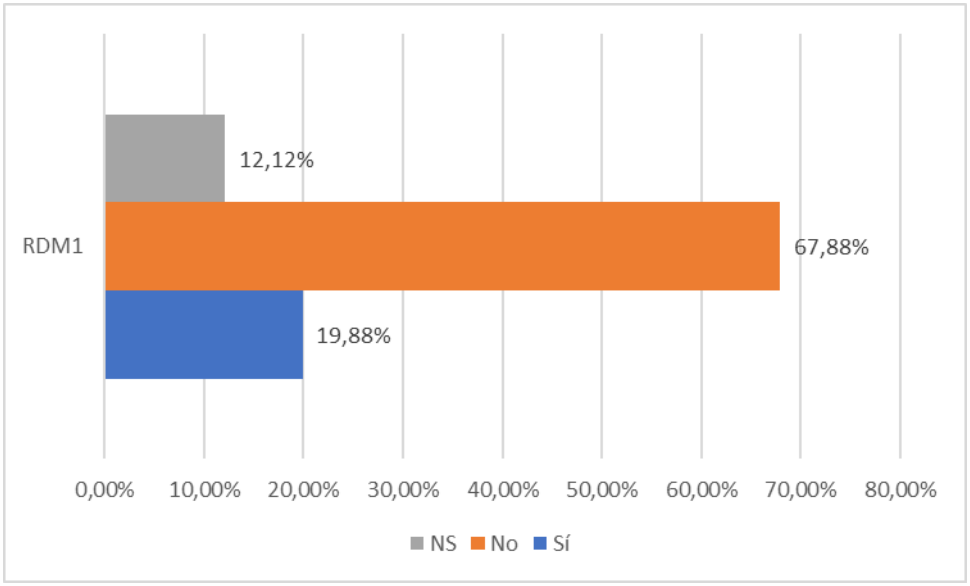

Gráfico 7. Resultados RDM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 33 instituciones que representan el 19,88% indicaron que el cuerpo directivo encargado del gobierno de seguridad de la información supervisan los diferentes niveles de gestión de seguridad de la información, el 67,88% que representa a 112 instituciones aseguran que el cuerpo directivo encargado del gobierno de seguridad de la información no supervisan los diferentes niveles de gestión de seguridad de la información y 20 instituciones desconocen si existen este tipo de seguimientos y representa el 12,12%

INTERPRETACIÓN. –El cuerpo directivo responsables de la seguridad de la información de la institución de educación superior o su comisión encargada no supervisan de manera planificada las estrategias, principios y políticas de los diferentes niveles de gestión de seguridad de la información.

RDM2: ¿Los responsables o directores de tecnologías de la información de las instituciones de educación superior toma las decisiones sobre seguridad de la información bajo aprobación del cuerpo directivo?

Tabla 7. Resultados RDM2

Respuesta	Porcentaje	Cantidad
SI	36,14%	60
NO	42,42%	70
(NS)	21,21%	35

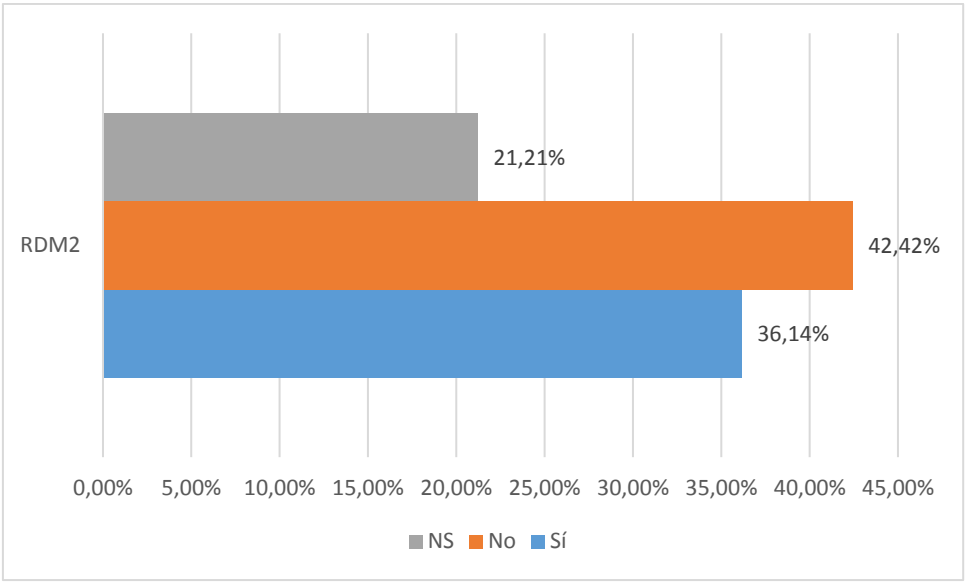

Gráfico 8. Resultados RDM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 60 instituciones que representan el 36,14% indicaron que los responsables o directores de tecnologías de la información de las instituciones de educación superior toma las decisiones sobre seguridad de la información bajo aprobación del cuerpo directivo, el 42,42% que representa a 70 instituciones manifiestan que los responsables o directores de tecnologías de la información de las instituciones de educación superior no siempre toman las decisiones sobre seguridad de la información bajo aprobación del cuerpo directivo? y 35 instituciones desconocen que representa el 21,21%

INTERPRETACIÓN. –Los resultados presentados muestran que los responsables o directores de tecnologías de la información de las instituciones de educación superior no toman las decisiones sobre seguridad de la información.

RDM4: ¿El cuerpo directivo de la institución de educación superior se preocupan que se planifique de manera adecuada los procesos de seguridad de la información?

Tabla 8. Resultados RDM4

Respuesta	Porcentaje	Cantidad
SI	37,35%	62
NO	46,67%	77
(NS)	15,76%	26

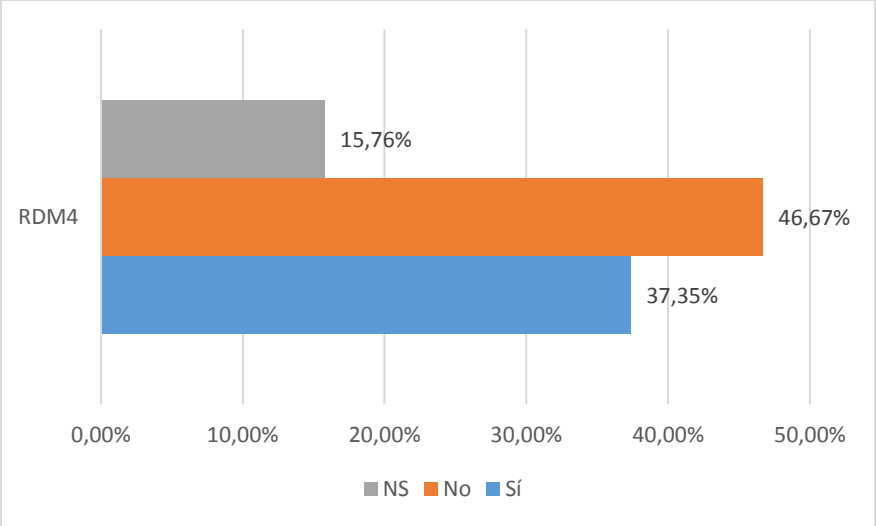

Gráfico 9. Resultados RDM4

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 62 instituciones que representan el 37,35% indicaron que existe una preocupación de los directivos por realizar una planificación de los procesos de seguridad de la información, el 46,67% que representa a 77 instituciones desconocen si se planifica de manera adecuada los procesos de seguridad de la información y el 15,76% no conocen si planifica o no y representa a 26 instituciones.

INTERPRETACIÓN. – Los resultados reflejan que el cuerpo directivo de la institución de educación superior no se preocupa que se planifique de manera adecuada los procesos de seguridad de la información

RDM5: ¿Comunican los directivos de la institución de educación superior las decisiones que se toma sobre seguridad de la información a docentes, estudiantes y personal administrativo de la institución?

Tabla 9. Resultados RDM5

Respuesta	Porcentaje	Cantidad
SI	37,35%	62
NO	55,76%	92
(NS)	6,67%	11

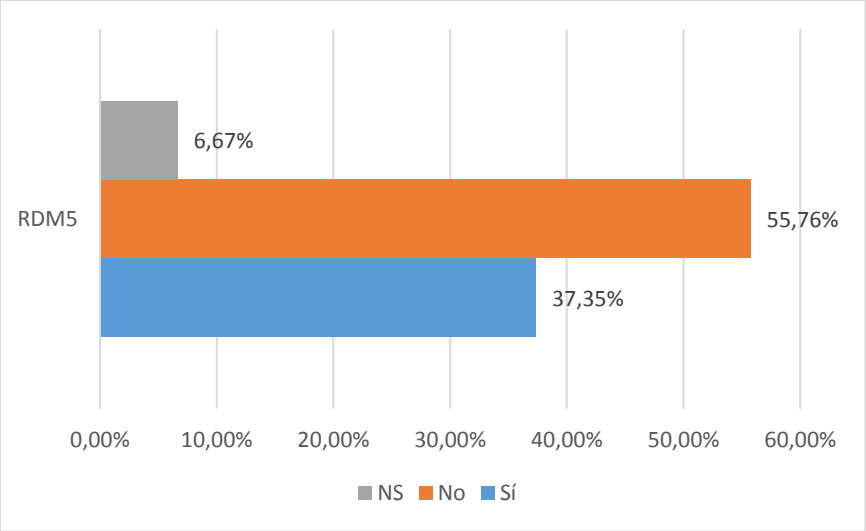

Gráfico 10. Resultados RDM5

ANÁLISIS. – En las encuestas realizadas a 165 Instituciones de educación superior, 62 instituciones de educación superior que representan el 37,35% indicaron que los directivos comunican las decisiones que se toma sobre seguridad de la información a docentes, estudiantes y personal administrativo de la institución, el 55,76% que representa a 92 instituciones manifiestan que los directivos no comunican las decisiones que se toma sobre seguridad de la información a docentes, estudiantes y personal administrativo de la institución y 11 instituciones tienen un desconocimiento sobre este tema y representa el 6,67%.

INTERPRETACIÓN. – Los resultados establecen que los directivos de la institución de educación superior no comunican las decisiones que se toma en materia de seguridad de la información a docentes, estudiantes y personal administrativo de la institución.

RDM6: ¿Los directivos de las instituciones de educación superior reciben información sobre las estrategias, políticas y procedimiento de seguridad de la información para apoyar su toma de decisiones?

Tabla 10. Resultados RDM6

Respuesta	Porcentaje	Cantidad
SI	10,24%	17
NO	55,76%	92
(NS)	33,94%	56

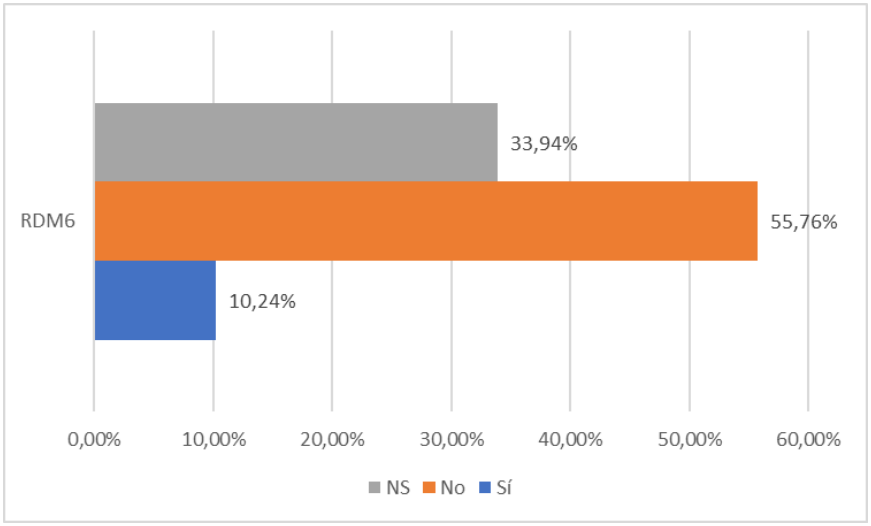

Gráfico 11. Resultados RDM6

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 17 instituciones que representan el 10,24% indicaron que se entregan algún tipo de información sobre seguridad de la información, el 55,76% que representa a 92 instituciones no se entregan información a directivos sobre seguridad de la información y 56 instituciones desconocen totalmente sobre estos temas y representa el 33,94%

INTERPRETACIÓN. – En función de los resultados presentados se determina los directivos de las instituciones de educación superior no reciben información sobre las estrategias, políticas y procedimiento de seguridad de la información para apoyar su toma de decisiones.

RMM1: ¿Se realiza un seguimiento a los roles y responsabilidades asignadas para garantizar que la ejecución de los procesos relacionadas con la seguridad de la información se realice de manera correcta?

Tabla 11. Resultados RMM1

Respuesta	Porcentaje	Cantidad
SI	37,95%	63
NO	55,76%	92
(NS)	6,06%	10

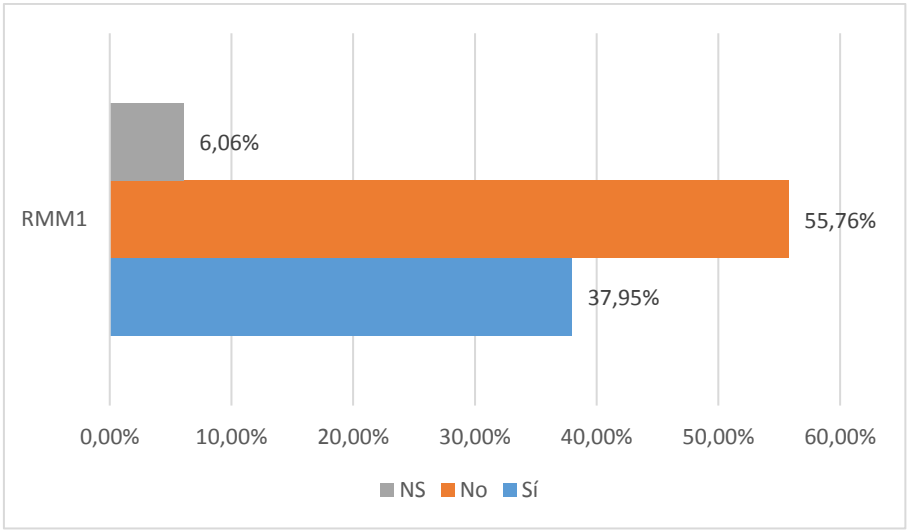

Gráfico 12. Resultados RMM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 63 instituciones que representan el 37,95% indicaron que se realiza un seguimiento a los roles y responsabilidades asignadas para garantizar que a ejecución de los procesos relacionadas con la seguridad de la información, el 55,76% que representa a 92 instituciones que no se realiza un seguimiento a los roles y responsabilidades asignadas para garantizar que la ejecución de los procesos relacionadas con la seguridad de la información 10 instituciones desconocen si existen responsabilidades asignadas y no conocen la existencia de responsabilidades definidas y representa el 6.06%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que la institución de educación superior no realiza un seguimiento a los roles y responsabilidades asignadas para garantizar que a ejecución de los procesos relacionadas con la seguridad de la información.

RMM2: ¿Docentes, estudiantes y personal académico comprenden las responsabilidades asignadas por el cuerpo directivo de la institución de educación superior en materia de seguridad de la información?

Tabla 12. Resultados RMM2

Respuesta	Porcentaje	Cantidad
SI	36,75%	61
NO	60,00%	99
(NS)	3,03%	5

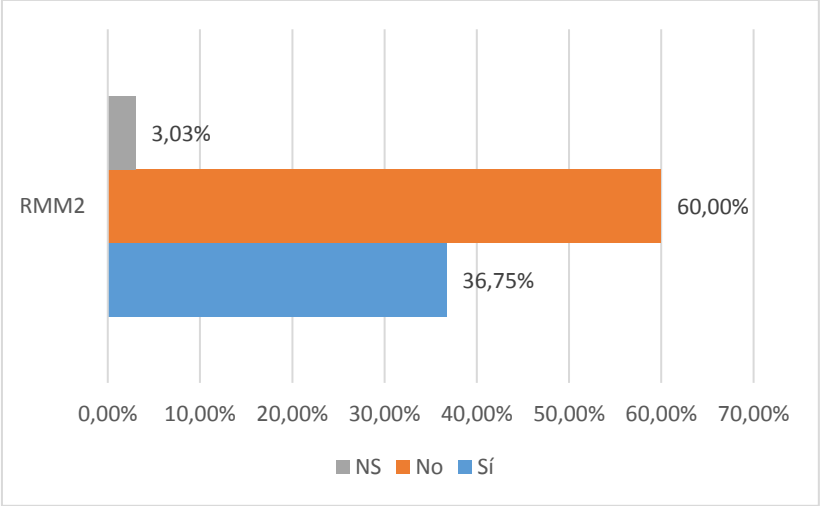

Gráfico 13. Resultados RMM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 61 que representan el 36,75% manifiesta que docentes, estudiantes y personal académico comprenden las responsabilidades asignadas por el cuerpo directivo de la institución de educación superior en materia de seguridad de la información, el 60,00% que representa a 99 establecen que docentes, estudiantes y personal académico no comprenden las responsabilidades asignadas por el cuerpo directivo de la institución de educación superior en materia de seguridad de la información y 5 desconocen si existen responsabilidades y representa el 3,03%

INTERPRETACIÓN. – En función de los resultados presentados se determina que docentes, estudiantes y personal académico no logran comprender las responsabilidades que se les han sido asignadas por el cuerpo directivo de la institución de educación superior en materia de seguridad de la información.

EEM1 : ¿La institución de educación superior dispone de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de Gobierno de seguridad de la Información?

Tabla 13. Resultados EEM1

Respuesta	Porcentaje	Cantidad
SI	15,06%	25
NO	60,61%	100
(NS)	24,24%	40

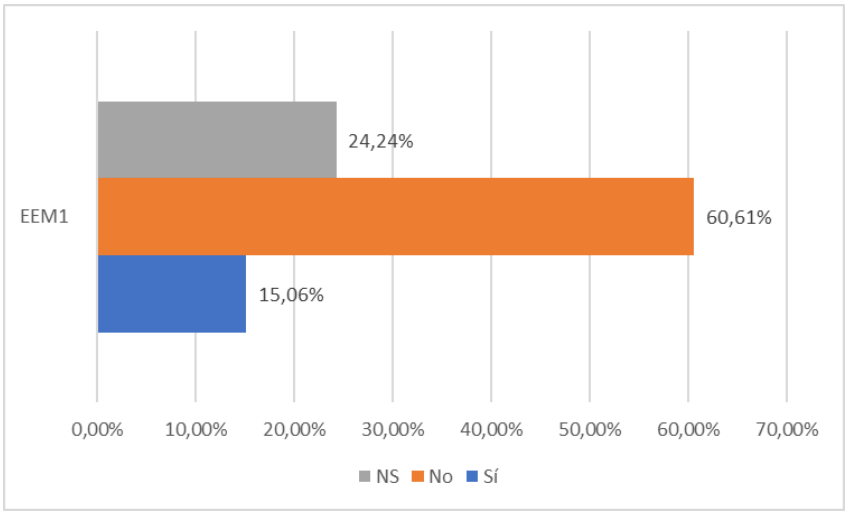

Gráfico 14. Resultados EEM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, el 15,06% que representa a 25 instituciones indicaron que la institución de educación superior dispone de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de gobierno de seguridad de la información, mientras que el 60,61% que representa a 100 manifiestan la institución de educación superior no dispone de un manejo de seguridad de la información integrados en las políticas de gobierno de seguridad de la información y 40 desconocen y representa el 24,24%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que las instituciones de educación superior no disponen de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de gobierno de seguridad de la información.

EEM2: ¿El cuerpo directivo de la institución superior supervisa las actividades de seguridad de la información de manera alineada con los objetivos estratégicos de la institución?

Tabla 14. Resultados EEM2

Respuesta	Porcentaje	Cantidad
SI	36,75%	61
NO	52,73%	87
(NS)	10,30%	17

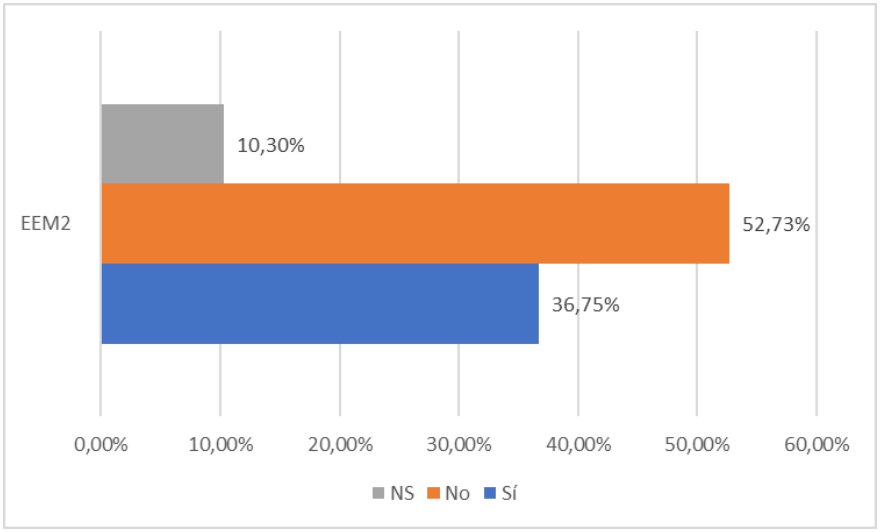

Gráfico 15. Resultados EEM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 61 que equivale al 36,75% indicaron que el cuerpo directivo de la institución de educación superior supervisa las actividades de seguridad de la información de manera alineada con los objetivos estratégicos de la institución, el 52,73% que representa a 87 instituciones de educación superior el cuerpo directivo de la institución de educación superior no supervisan las actividades de seguridad de la información de manera alineada con los objetivos estratégicos de la institución y 17 no saben nada y representa el 10,30%

INTERPRETACIÓN. – Al observar los resultados se puede determinar el cuerpo directivo de la institución de educación superior no supervisa las actividades de seguridad de la información de manera alineada con los objetivos estratégicos de la institución.

EEM3: ¿Analiza el cuerpo directivo los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo institucional?

Tabla 15. Resultados EEM3

Respuesta	Porcentaje	Cantidad
SI	12,05%	20
NO	70,91%	117
(NS)	16,97%	28

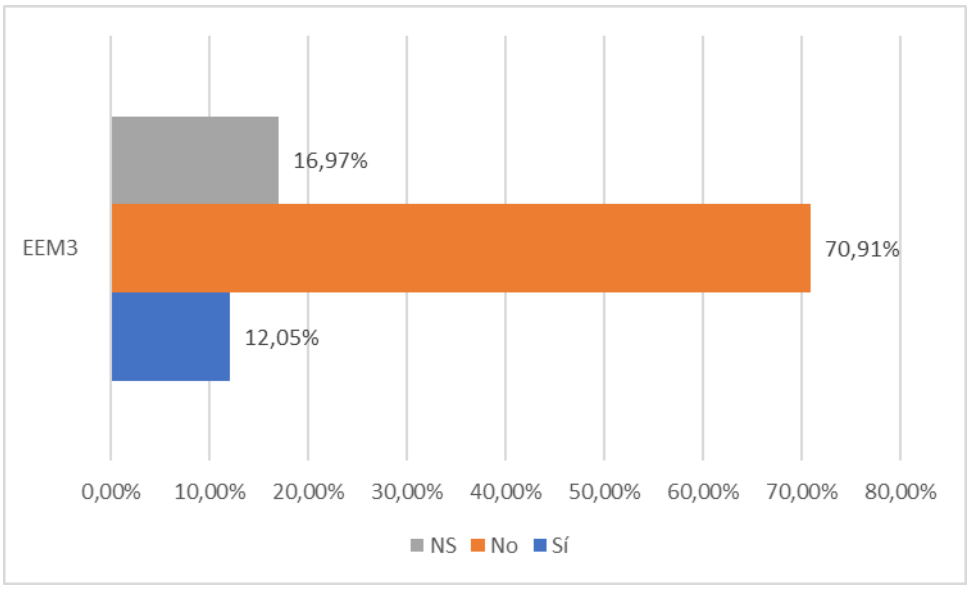

Gráfico 16. Resultados EEM3

ANÁLISIS. – En las encuestas realizadas a 165 Instituciones de educación superior, 20 instituciones de educación superior que representan el 12,05% indicaron que el cuerpo directivo analiza los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo institucional, el 70,91% especifican que el cuerpo directivo análisis de los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo institucional y 28 desconocen los temas que se están analizando y representa el 16,97%

INTERPRETACIÓN. – En función de los resultados presentados se determina el cuerpo directivo no realiza ningún análisis de riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo institucional.

EDM1: ¿El cuerpo directivo de la institución de educación superior diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información?

Tabla 16. Resultados EDM1

Respuesta	Porcentaje	Cantidad
SI	16,27%	27
NO	70,30%	116
(NS)	13,33%	22

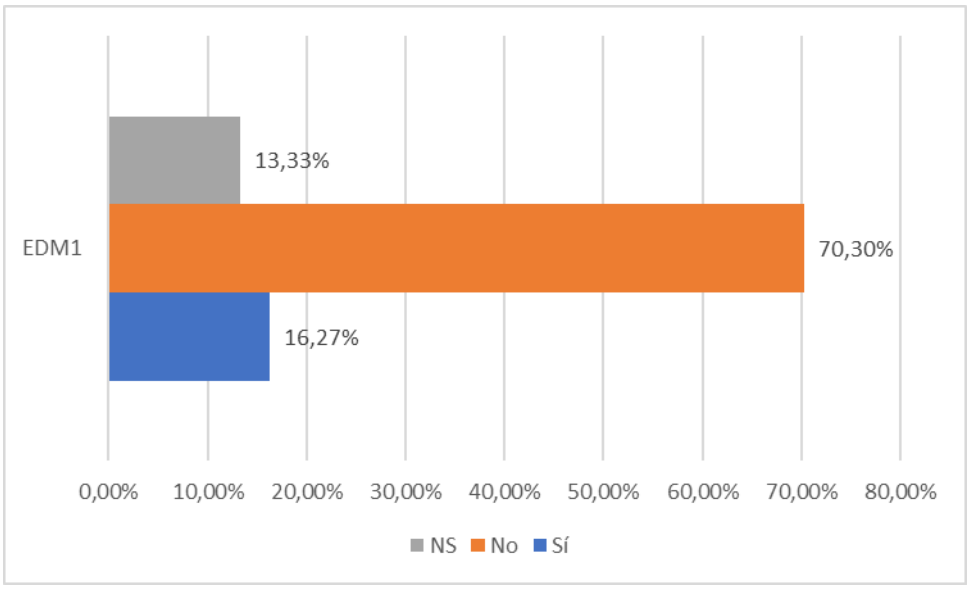

Gráfico 17. Resultados EDM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 27 instituciones de educación superior que representan el 16,27% indican que el cuerpo directivo de la institución de educación superior diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información, el 70,30% que representa a 116 instituciones de educación superior manifiestan el cuerpo directivo de la institución de educación superior no diseñan procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información y 22 Instituciones de educación superior desconocen y representa el 13,33%

INTERPRETACIÓN. – En función de los resultados presentados determinan que el cuerpo directivo de la institución de educación superior no diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información.

EDM2: ¿La institución de educación superior realiza una planificación de la seguridad de la información a pequeño, medio y largo plazo?

Tabla 17. Resultados EDM2

Respuesta	Porcentaje	Cantidad
SI	17,47%	29
NO	56,36%	93
(NS)	26,06%	43

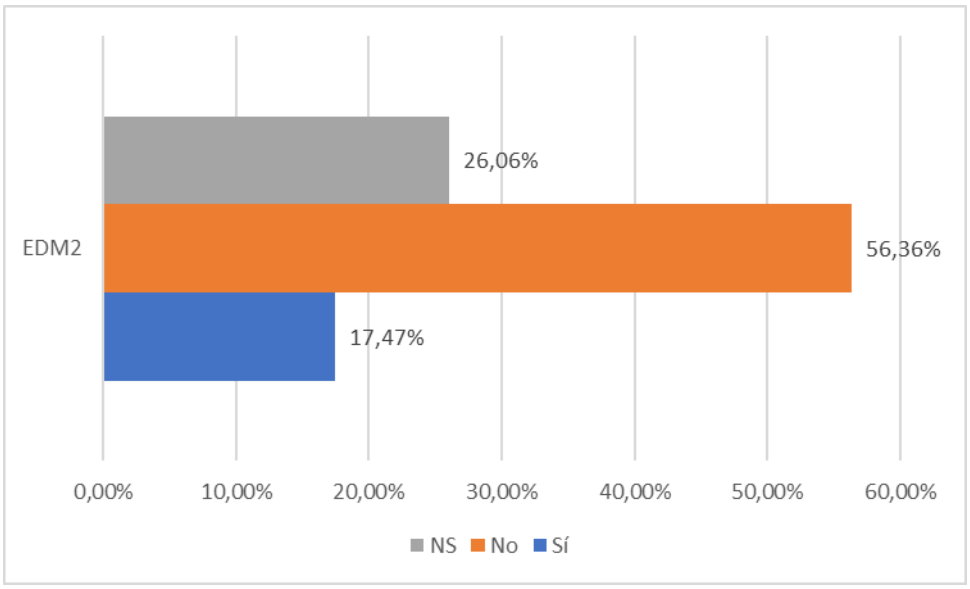

Gráfico 18. Resultados EDM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 29 que representan el 17,47% indicaron que la institución de educación superior realiza una planificación de la seguridad de la información a pequeño, medio y largo plazo, el 56,36% que representa a 93 instituciones de educación no realiza una planificación de la seguridad de la información a pequeño, medio y largo plazo y 43 Instituciones de educación superior desconocen y representa el 26,06%

INTERPRETACIÓN. – Los resultados muestran que la institución de educación superior realiza una planificación de la seguridad de la información a pequeño, medio y largo plazo.

EDM3: ¿La institución de educación superior informa a docentes, estudiantes, personal administrativo sobre los elementos estructurales de la planificación de la seguridad de la información?

Tabla 18. Resultados EDM3

Respuesta	Porcentaje	Cantidad
SI	9,04%	15
NO	69,09%	114
(NS)	21,82%	36

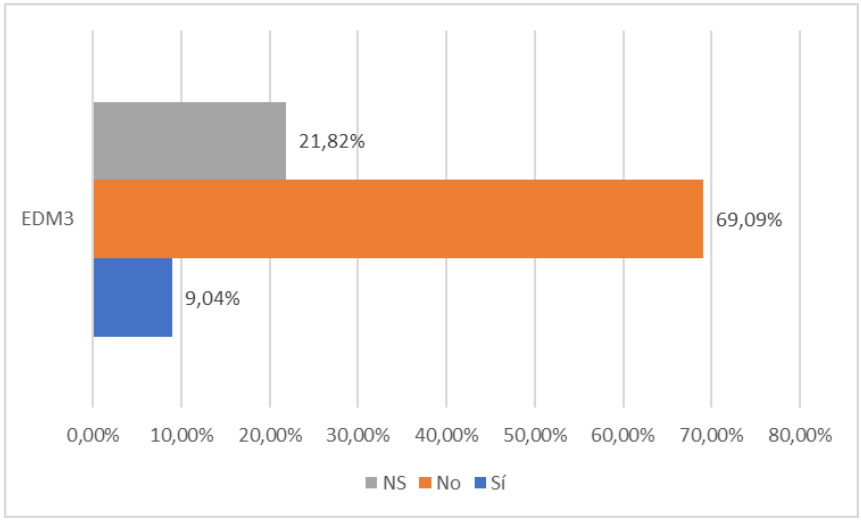

Gráfico 19. Resultados EDM3

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 15 instituciones de educación superior que representan el 9,04% indicaron que se informa a docentes, estudiantes, personal administrativo sobre los elementos estructurales de la planificación de la seguridad de la información, el 69,09% que representa a 114 instituciones de educación superior especifican que no se informa a docentes, estudiantes, personal administrativo sobre los elementos estructurales de la planificación de la seguridad de la información y 36 instituciones de educación superior desconocen y representa el 21,86%

INTERPRETACIÓN. – En función de los resultados presentados las instituciones de educación superior no informan a docentes, estudiantes, personal administrativo sobre los elementos estructurales de la planificación de la seguridad de la información.

.

EMM1: ¿Se lleva a cabo un seguimiento de la ejecución de la planificación de la seguridad de la información?

Tabla 19. Resultados EMM1

Respuesta	Porcentaje	Cantidad
SI	16,87%	28
NO	52,12%	86
(NS)	30,91%	51

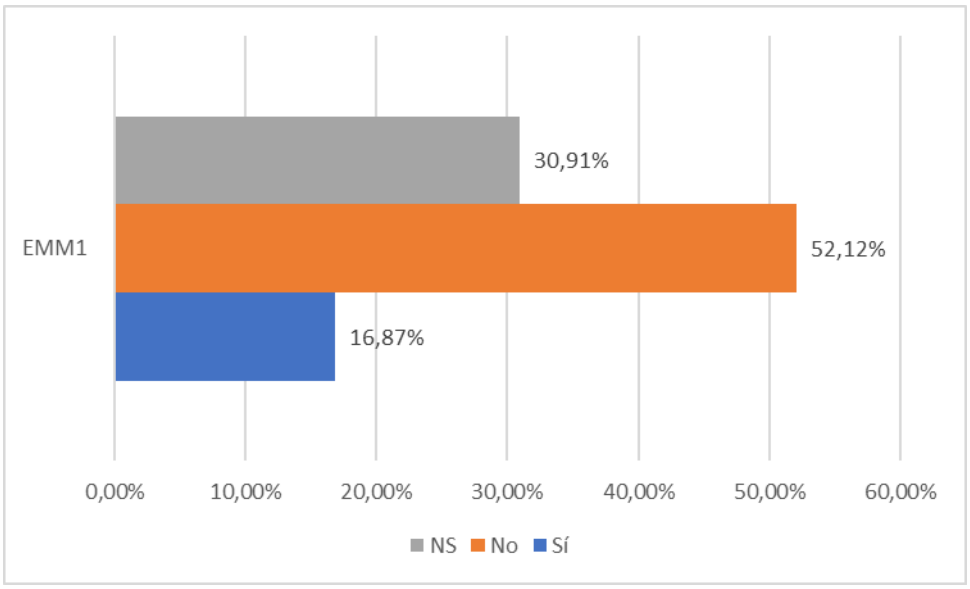

Gráfico 20. Resultados EEM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 28 instituciones de educación superior que representan el 16,87% indicaron es evidente que se lleva a cabo un seguimiento de la ejecución de la planificación de la seguridad de la información, el 52,12% que representa a 86 instituciones de educación superior no se lleva a cabo un seguimiento de la ejecución de la planificación de la seguridad de la información y 51 Instituciones de educación superior desconocen y representa el 30,91%.
INTERPRETACIÓN. – En función de los resultados presentados se determina que no se lleva a cabo un seguimiento de la ejecución de la planificación de la seguridad de la información.

EMM3: ¿Se comprueba si las políticas de seguridad de la información se están aplicando en todas las unidades administrativas y de gestión de la institución?

Tabla 20. Resultados EMM3

Respuesta	Porcentaje	Cantidad
SI	12,65%	21
NO	67,88%	112
(NS)	19,39%	32

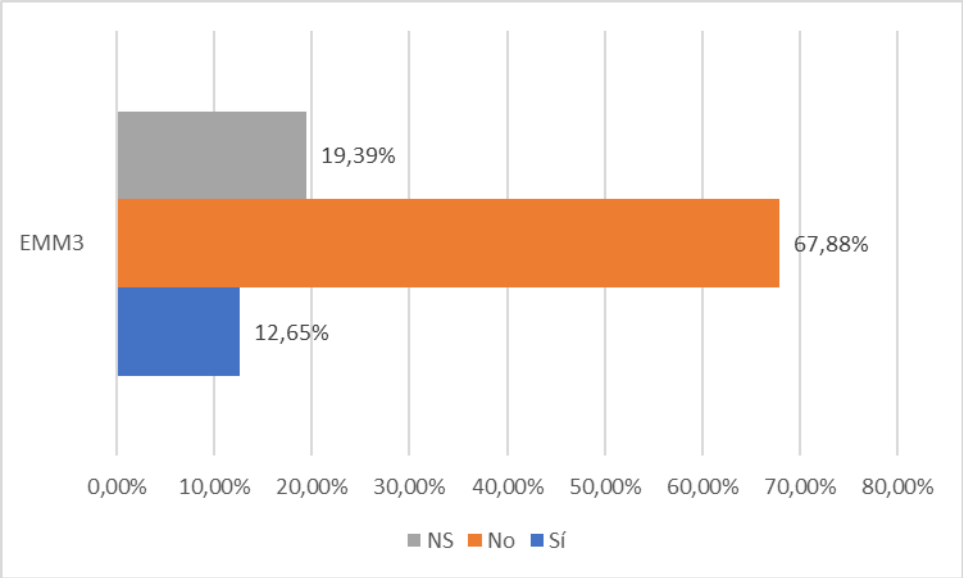

Gráfico 21. Resultados EMM3

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 21 instituciones de educación superior que representan el 12,65% indicaron que las políticas de seguridad de la información se están aplicando en las unidades administrativas y de gestión , el 67,88% que representa a 112 instituciones de educación superior desconocen que existen políticas de seguridad de la información que se estén aplicando en las unidades administrativas y de gestión y 32 instituciones de educación superior no saben y representa el 19,39%

INTERPRETACIÓN. – En función de los resultados presentados se determina que las políticas de seguridad de la información no se están aplicando en las unidades administrativas y de gestión de la institución.

DEM2: ¿Los gestores de tecnologías de la información toman las principales decisiones sobre la articulación de la seguridad de la información y los procesos estratégicos de la institución?

Tabla 21. Resultados DEM2

Respuesta	Porcentaje	Cantidad
SI	3,01%	5
NO	84,85%	140
(NS)	12,12%	20

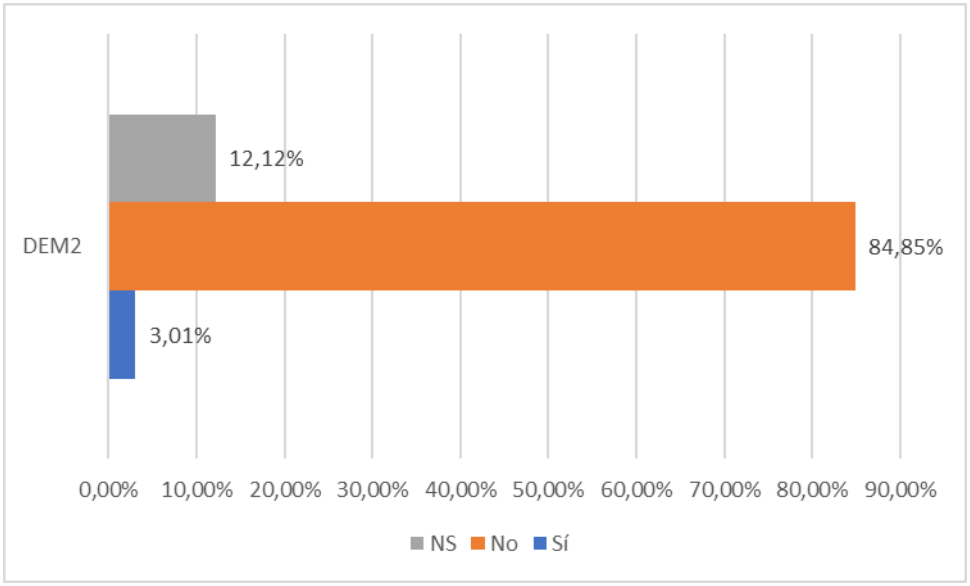

Gráfico 22. Resultados DEM2

ANÁLISIS. – De las 165 instituciones de educación superior el 3,01% manifiestan los gestores de tecnologías de la información toman las principales decisiones sobre la articulación de la seguridad de la información y los procesos estratégicos de la institución, mientras que 140 que corresponde al 84,85% de las instituciones establecen que los gestores de tecnologías de la información no toman las principales decisiones sobre la articulación de la seguridad de la información y los procesos estratégicos de la institución y 20 desconocen sobre el tema y representan el 12,12%

INTERPRETACIÓN. – Los resultados muestran que los gestores de tecnologías de la información no toman las principales decisiones sobre la articulación de la seguridad de la información y los procesos estratégicos de la institución.

DEM3: ¿Los directivos de la institución de educación superior comprenden los cuales son los riegos que tiene sobre los activos de información y toman de decisiones relacionadas con el desempeño los niveles de seguridad de la información?

Tabla 22. Resultados DEM3

Respuesta	Porcentaje	Cantidad
SI	17,47%	29
NO	49,09%	81
(NS)	33,33%	55

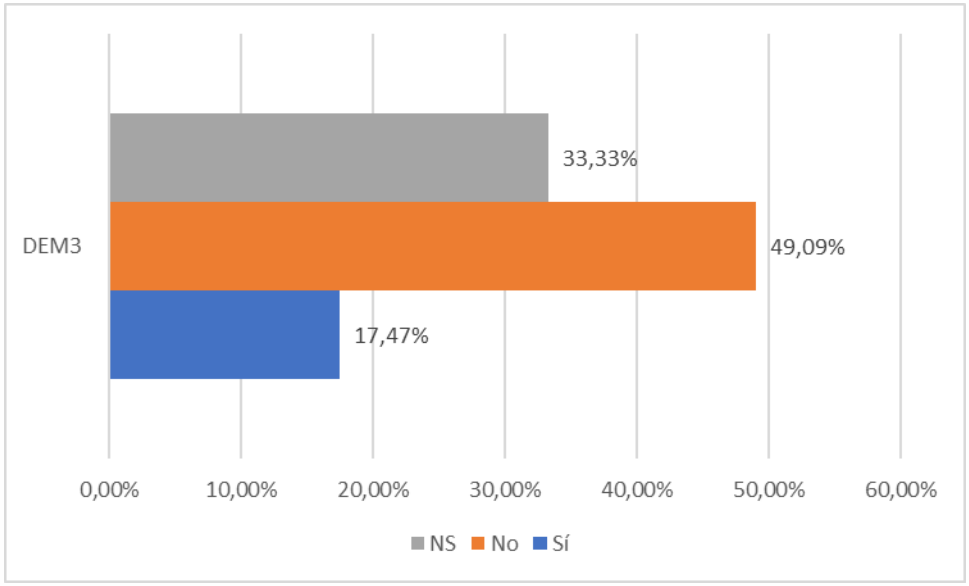

Gráfico 23. Resultados DEM3

ANÁLISIS. – De la 165 institución de educación superior el 17,47% de las instituciones comprenden cuales son los riegos que tiene sobre los activos de información y toman de decisiones relacionadas con el desempeño los niveles de seguridad de la información, el 49,09% no comprenden cuales son los riegos que tiene sobre los activos de información y toman de decisiones relacionadas con el desempeño los niveles de seguridad de la información, mientras que el 33,33% desconoce totalmente del tema.

INTERPRETACIÓN. – Los resultados muestran que las instituciones de educación superior no comprenden cuales son los riegos que tiene sobre los activos de información y toman de decisiones relacionadas con el desempeño los niveles de seguridad de la información.

DDM1: ¿Las estrategias de gobierno de seguridad de la información cubren todas las operaciones y servicios institucionales de la institución de educación superior?

Tabla 23. Resultados DDM1

Respuesta	Porcentaje	Cantidad
SI	22,29%	37
NO	48,48%	80
(NS)	29,09%	48

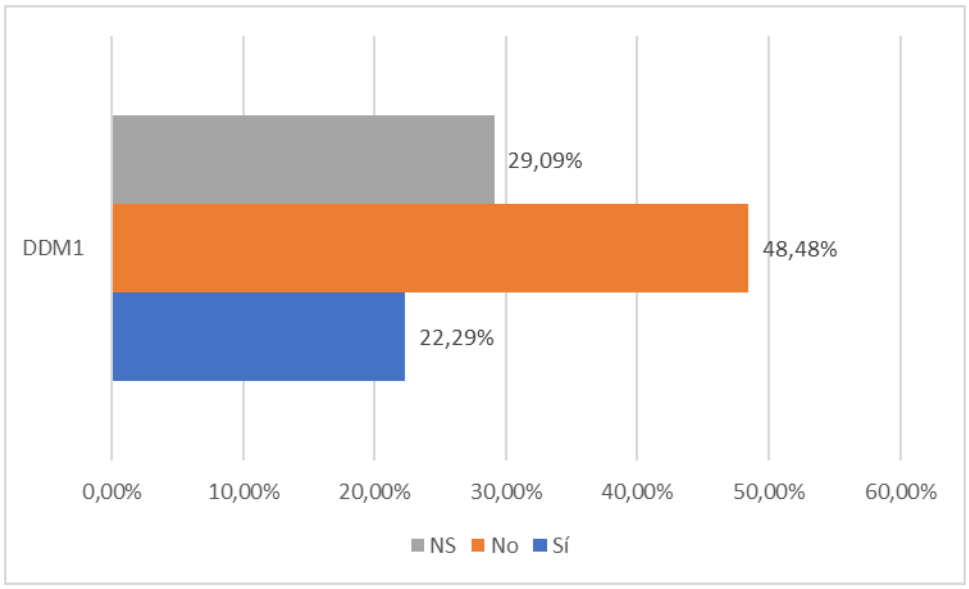

Gráfico 24. Resultados DDM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 37 que representan el 22,29% indicaron las estrategias de seguridad de la información cubren todas las operaciones y servicios institucionales de la institución de educación superior, el 48,48% que representa a 80 instituciones de educación superior indicaron las estrategias de seguridad de la información no cubren todas las operaciones y servicios institucionales de la institución de educación superior y 48 instituciones de educación superior desconocen y representa el 29,09%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que las estrategias de seguridad de la información no cubren todas las operaciones y servicios institucionales de la institución de educación superior.

DMM1: ¿La institución de educación superior establece indicadores para medir los niveles de seguridad de la información de la institución?

Tabla 24. Resultados DMM1

Respuesta	Porcentaje	Cantidad
SI	13,86%	23
NO	63,64%	105
(NS)	22,42%	37

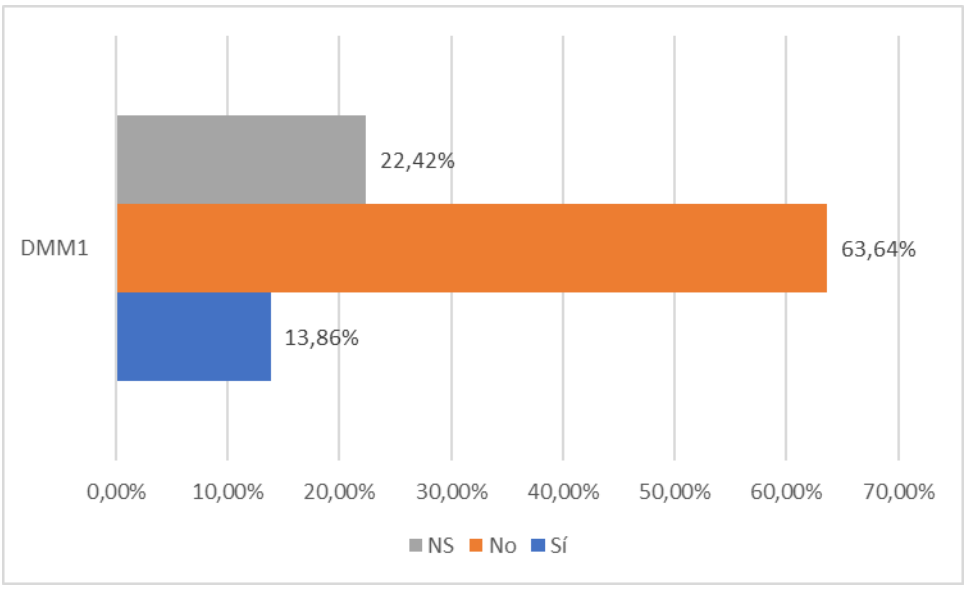

Gráfico 25. Resultados DMM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 23 que representan el 13,86% indicaron que se miden mediante indicadores los niveles de seguridad de la información a todos los recursos tecnológicos y procesos operacionales de la institución, el 63,64% que representa a 105 instituciones de educación superior indicaron que no se miden mediante indicadores los niveles de seguridad de la información a todos los recursos tecnológicos y procesos operacionales de la institución y 37 instituciones de educación superior desconocen y representa el 22,42%

INTERPRETACIÓN. – En función de los resultados presentados se determina que las instituciones de educación superior no miden mediante indicadores los niveles de seguridad de la información a todos los recursos tecnológicos y procesos operacionales de la institución.

DMM3: ¿Hay políticas y normas internas establecidas para los aspectos más importantes de seguridad de la información para los procesos institucionales?

Tabla 25. Resultados DMM3

Respuesta	Porcentaje	Cantidad
SI	15,06%	25
NO	43,64%	72
(NS)	41,21%	68

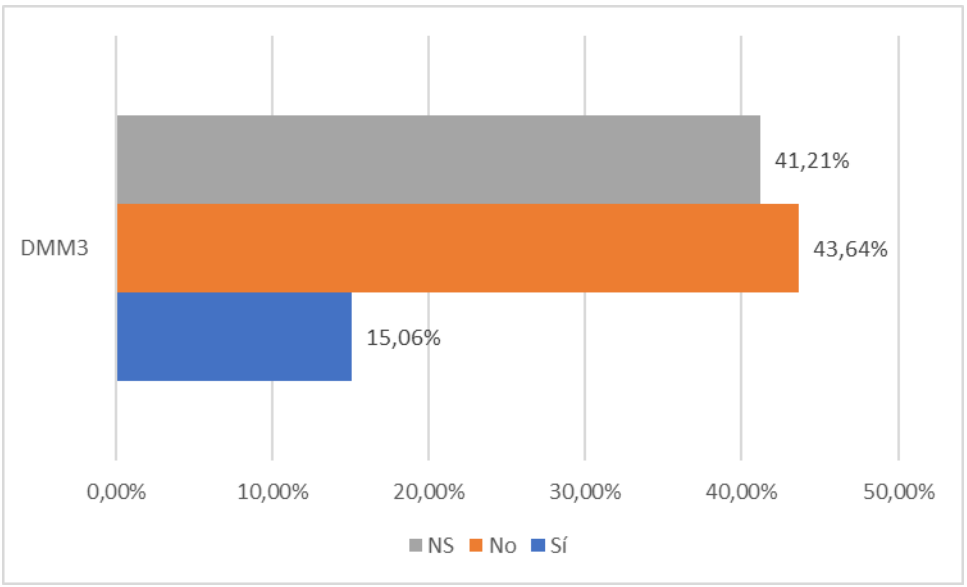

Gráfico 26. Resultados DMM3

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 25 que representan el 15,06% indicaron que hay políticas y normas internas establecidas para los aspectos más importantes de seguridad de la información para los procesos institucionales, el 43,64% que representa a 72 instituciones de educación superior indicaron que no hay políticas y normas internas establecidas para los aspectos más importantes de seguridad de la información para los procesos institucionales y 68 instituciones de educación superior desconocen y representa el 41,21%

INTERPRETACIÓN. – En función de los resultados presentados se determina que las instituciones de educación superior no tienen políticas y normas internas establecidas para los aspectos más importantes de seguridad de la información para los procesos institucionales.

CEM1: ¿El cuerpo directivo de la institución de educación superior conoce la normativa y el modelo de gobierno de seguridad de la información?

Tabla 26. Resultados CEM1

Respuesta	Porcentaje	Cantidad
SI	19,28%	32
NO	42,42%	70
(NS)	38,18%	63

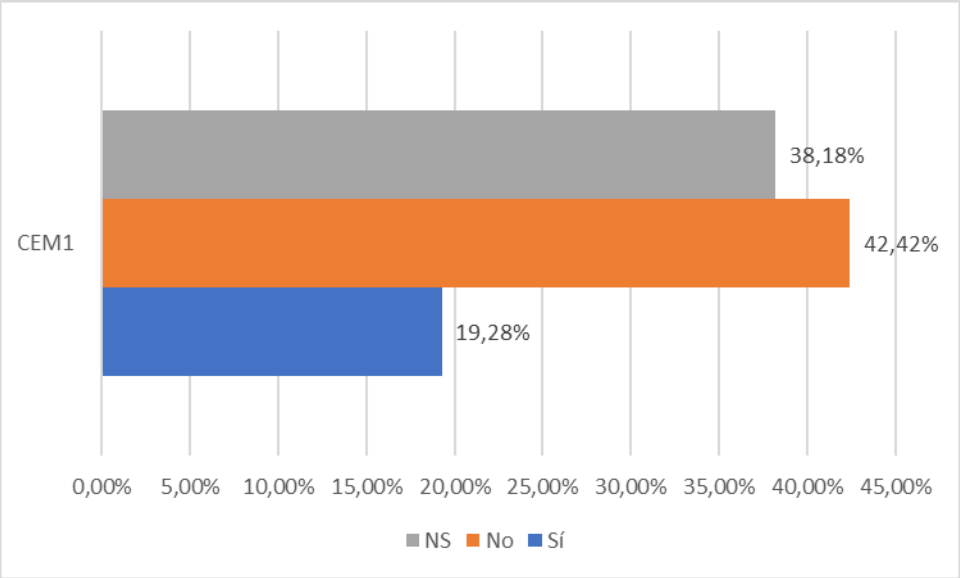

Gráfico 27. Resultados CEM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 32 que representan el 19,28% indicaron que el cuerpo directivo de la institución de educación superior conoce la normativa y el modelo de gobierno de seguridad de la información institucional, el 42,42% que representa a 70 instituciones de educación superior indicaron que el cuerpo directivo de la institución de educación superior no conoce la normativa ni el modelo de gobierno de seguridad de la información y 63 instituciones de educación superior desconocen y representa el 38,18%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior el cuerpo directivo de la institución de educación superior no conoce la normativa ni el modelo de gobierno de seguridad de la información.

CEM2: ¿El cuerpo directivo de las instituciones de educación superior conocen los principales estándares de gobierno de seguridad de la información?

Tabla 27. Resultados CEM2

Respuesta	Porcentaje	Cantidad
SI	21,08%	35
NO	50,30%	83
(NS)	28,48%	47

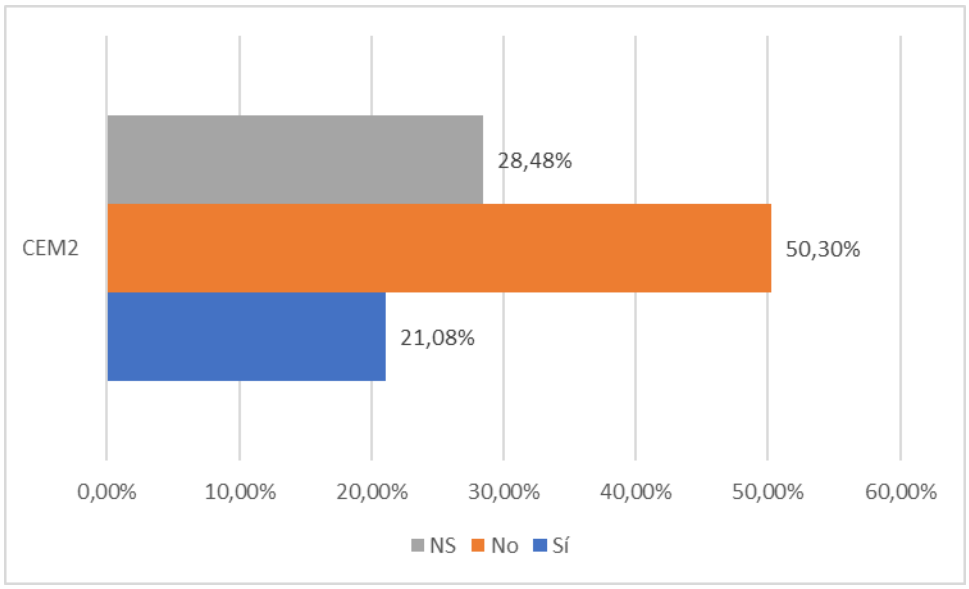

Gráfico 28. Resultados CEM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 35 que representan el 21,08% indicaron que el cuerpo directivo de las instituciones de educación superior conocen los principales estándares de gobierno de seguridad de la información, el 50,30% que representa a 83 instituciones de educación superior indicaron que el cuerpo directivo de las instituciones de educación superior no conocen los principales estándares de gobierno de seguridad de la información y 47 instituciones de educación superior desconocen y representa el 28,48%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior el cuerpo directivo de las instituciones de educación superior no conoce los principales estándares de gobierno de seguridad de la información.

CDM1: ¿Demuestran docentes, estudiantes y personal administrativo un comportamiento cumpliendo lo establecido en las normas y estándares de gobierno de seguridad de la información?

Tabla 28. Resultados CDM1

Respuesta	Porcentaje	Cantidad
SI	16,27%	27
NO	43,64%	72
(NS)	40,00%	66

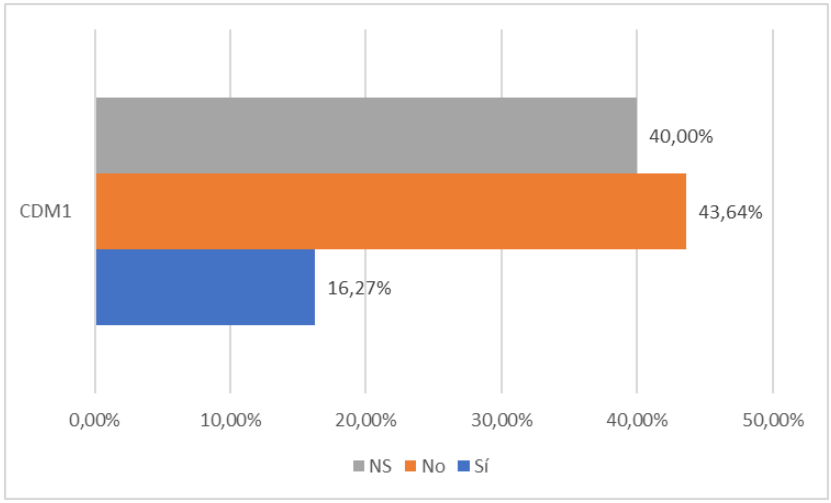

Gráfico 29. Resultados CDM1

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 27 que representan el 16,27% indicaron que los docentes, estudiantes y personal administrativo demuestran un comportamiento cumpliendo lo establecido en las normas y estándares de gobierno de seguridad de la información, el 43,34% que representa a 72 instituciones de educación superior indicaron que docentes, estudiantes y personal administrativo no cumplen lo establecido en las normas y estándares de gobierno de seguridad de la información y 66 instituciones de educación superior desconocen y representa el 40,00%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior los docentes, estudiantes y personal administrativo no cumplen lo establecido en las normas y estándares de gobierno de seguridad de la información.

CDM2: ¿Conocen los estudiantes, docentes y administrativos cuales son las políticas relacionadas con la seguridad de la información de la institución gracias a los procesos de comunicación llevados a cabo?

Tabla 29. Resultados CDM2

Respuesta	Porcentaje	Cantidad
SI	22,89%	38
NO	50,30%	83
(NS)	26,67%	44

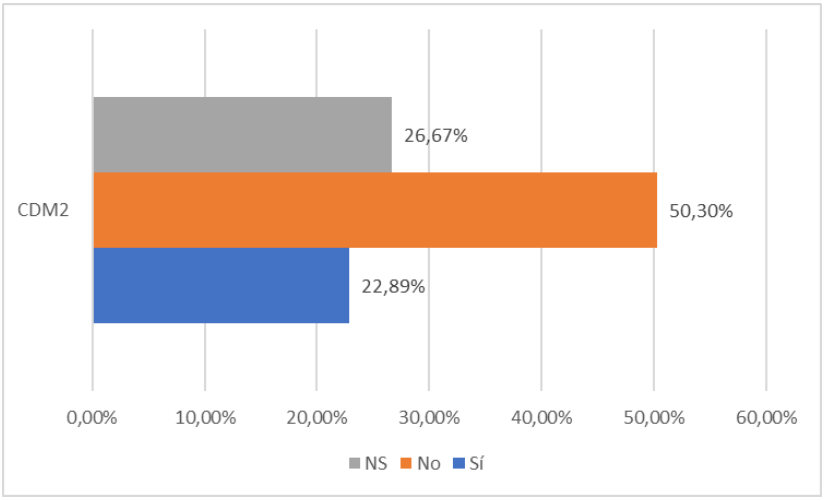

Gráfico 30. Resultados CDM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 38 que representan el 22,89% indicaron que los estudiantes, docentes y administrativos conocen cuales son las políticas relacionadas con la seguridad de la información de la institución gracias a los procesos de comunicación llevados a cabo, el 50,30% que representa a 83 instituciones de educación superior indicaron que indicaron que los indicaron que los estudiantes, docentes y administrativos no conocen cuales son las políticas relacionadas con la seguridad de la información de la institución gracias a los procesos de comunicación llevados a cabo y 44 instituciones de educación superior desconocen y representa el 26,67%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior indicaron que los estudiantes, docentes y administrativos no conocen cuales son las políticas relacionadas con la seguridad de la información de la institución gracias a los procesos de comunicación llevados a cabo.

CDM3: ¿Se han diseñado normas y procedimientos internos, basados en las políticas, cuyo objetivo es alcanzar una adecuada gestión del gobierno de seguridad de la información?

Tabla 30. Resultados CDM3

Respuesta	Porcentaje	Cantidad
SI	19,28%	32
NO	58,79%	97
(NS)	21,82%	36

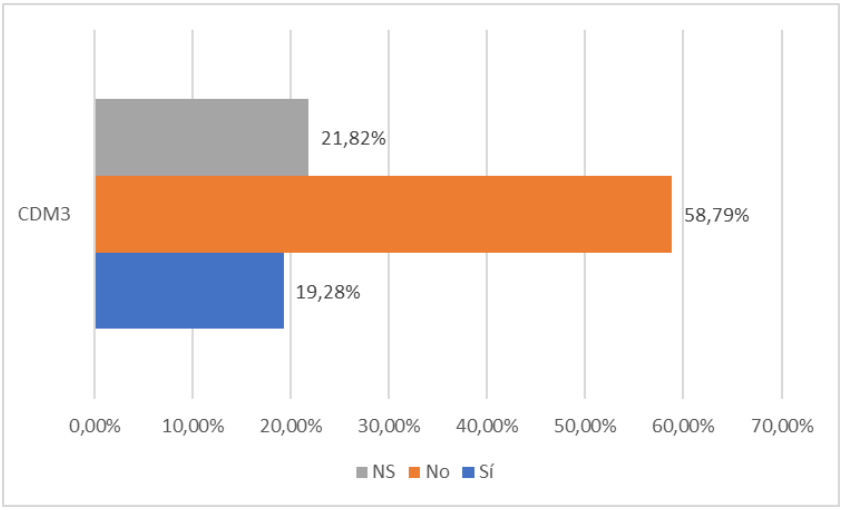

Gráfico 31. Resultados CDM3

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 32 que representan el 19,28% indicaron que se han diseñado normas y procedimientos internos, basados en las políticas, cuyo objetivo es alcanzar una adecuada gestión del gobierno de seguridad de la información, el 58,79% que representa a 97 instituciones de educación superior indicaron que los indicaron que no se han diseñado normas y procedimientos internos, basados en las políticas, cuyo objetivo es alcanzar una adecuada gestión del gobierno de seguridad de la información y 36 instituciones de educación superior desconocen y representa el 21,82%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior indicaron que no se han diseñado normas y procedimientos internos, basados en las políticas, cuyo objetivo es alcanzar una adecuada gestión del gobierno de seguridad de la información.

CMM2: ¿La institución de educación superior comprueba bajo indicadores el cumplimiento de las políticas, normas y estándares del gobierno de seguridad de la información?

Tabla 31 Resultados CMM2

Respuesta	Porcentaje	Cantidad
SI	10,84%	18
NO	68,48%	113
(NS)	20,61%	34

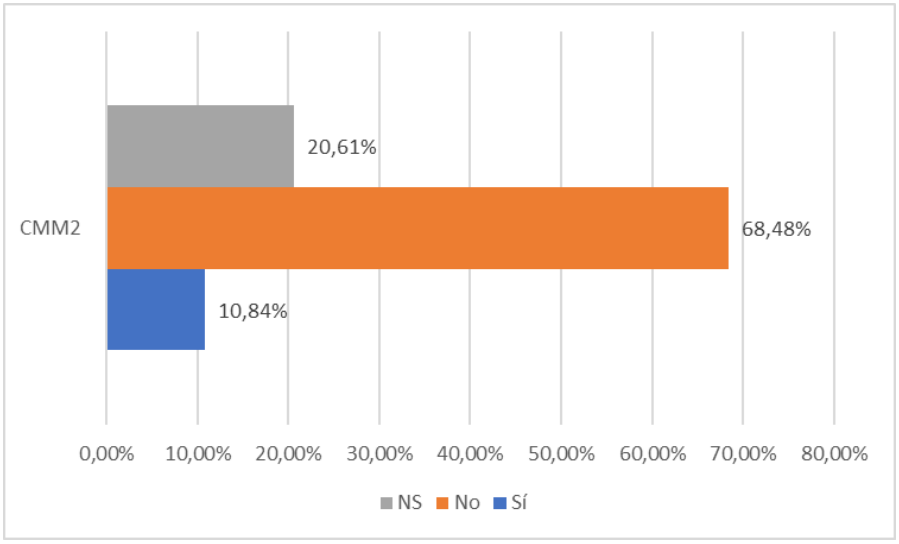

Gráfico 32. Resultados CMM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 18 que representan el 10,84% indicaron que la institución de educación superior comprueba bajo indicadores el cumplimiento de las políticas, normas y estándares del gobierno de seguridad de la información, el 68,48% que representa a 113 instituciones de educación superior indicaron que la institución de educación superior no comprueba bajo indicadores el cumplimiento de las políticas, normas y estándares del gobierno de seguridad de la información y 34 instituciones de educación superior desconocen y representa el 20,61%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que la institución de educación superior no comprueba bajo indicadores el cumplimiento de las políticas, normas y estándares del gobierno de seguridad de la información.

HEM4: ¿El cuerpo directivo de la institución de educación superior es consciente de los riesgos, amenazas y vulnerabilidad al cual están sujetos los activos de información debido a que no existen procesos de gobernanza de seguridad de la información?

Tabla 32. Resultados HEM4

Respuesta	Porcentaje	Cantidad
SI	8,43%	14
NO	69,70%	115
(NS)	21,82%	36

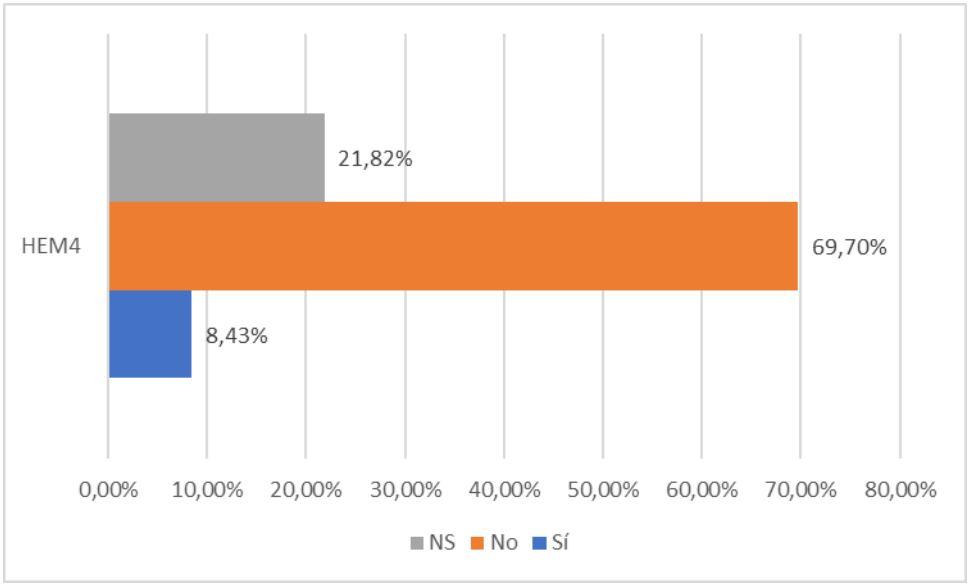

Gráfico 33. Resultados HEM4

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 14 que representan el 8,43% indicaron que el cuerpo directivo de la institución de educación superior es consciente de los riesgos, amenazas y vulnerabilidad al cual están sujetos los activos de información debido a que no existen procesos de gobernanza de seguridad de la información, el 69,70% que representa a 115 instituciones de educación superior indicaron el cuerpo directivo de la institución de educación superior no es consciente de los riesgos, amenazas y vulnerabilidad al cual están sujetos los activos de información y 36 instituciones de educación superior desconocen y representa el 21,82%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior indicaron que el cuerpo directivo de la institución de educación superior no es consciente de los riesgos, amenazas y vulnerabilidad al cual

están sujetos los activos de información debido a que no existen procesos de gobernanza de seguridad de la información.

HDM2: ¿La institución de educación superior informa a docentes, estudiantes y personal administrativo de los procesos y procedimientos de gobernanza de seguridad de la información?

Tabla 33. Resultados HDM2

Respuesta	Porcentaje	Cantidad
SI	13,86%	23
NO	66,67%	110
(NS)	19,39%	32

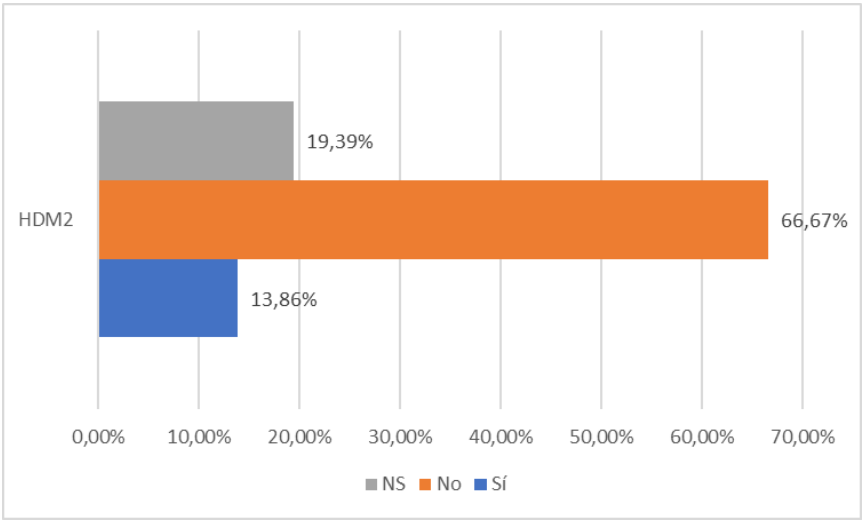

Gráfico 34. Resultados HDM2

ANÁLISIS. – En las encuestas realizadas a 165 instituciones de educación superior, 23 que representan el 13,86% indicaron que se informa a docentes, estudiantes y personal administrativo de los procesos y procedimientos de gobernanza de seguridad de la información, el 66,67% que representa a 110 instituciones de educación superior indicaron no informa a docentes, estudiantes y personal administrativo de los procesos y procedimientos de gobernanza de seguridad de la información y 32 instituciones de educación superior desconocen y representa el 19,39%.

INTERPRETACIÓN. – En función de los resultados presentados se determina que en las instituciones de educación superior no informa a docentes, estudiantes y personal administrativo de los procesos y procedimientos de gobernanza de seguridad de la información.

4.2 Verificación de Hipótesis

Luego de haber realizado el análisis estadístico de validez mediante el coeficiente V de Aiken, los resultados obtenidos apoyan verificación de la hipótesis planteada en la investigación, los valores de la validez de los expertos al modelo de gobierno de seguridad de la información con un error de 5%, establece un nivel de validez del modelo del 90%. Lo que significa, de acuerdo a Escurra Mayaute (1988) que se tiene un nivel de validez fuerte en todos en todos los elementos que constituyen el modelo de gobierno de seguridad de la información para instituciones de educación superior. Cada elemento tiene una validez de claridad de 91%, coherencia 89% y de relevancia 88,67%.

Los valores, resultado del análisis de la relevancia del contenido, superaron en todas las dimensiones el valor mínimo que exige (Aiken, 1980) que es de 0.86.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- De acuerdo a los resultados presentados se puede identificar que las instituciones de educación desconocen los roles y responsabilidades relacionadas con el gobierno de seguridad de la información, así como los procesos de gobernanza para la generación de estrategias basadas en un análisis de riesgos.
- Las instituciones de educación superior desconocen la importancia de contar con los niveles de seguridad de la información que permita garantizar el funcionamiento de los procesos de la institución y el resguardo de los activos de información que se genera en la articulación de las funciones sustantivas y de esta manera apoyar en la toman de decisiones a los directivos de la institución.
- Las instituciones de educación superior no tienen estrategias, políticas relacionadas con seguridad de la información aplicándose en las unidades administrativas y de gestión institucional que permitan garantizar que las principales operaciones de los servicios institucionales y los recursos tecnológicos bajo principios, objetivos y procesos de gobernanza de seguridad de la información.
- Las instituciones de educación superior tienen un desconocimiento de los principales estándares relacionados con el gobierno de seguridad de la información, esto no permite que los estudiantes, docentes y administrativos no conocen como actuar ante las diferentes amenazas y vulnerabilidades a las que están expuestas.
- De los resultados que se obtuvieron al analizar la problemática planteada y los resultados del análisis situacional de las instituciones de educación superior se ve la necesidad de Diseñar un modelo que sostenga el funcionamiento del gobierno de seguridad de la información en las Instituciones de Educación Superior, realizando una armonización de los modelos de gobierno de TI ISO/IEC 38500:2015 y de Seguridad de la Información ISO/IEC 27014:2013 de la forma que permita garantizar la disponibilidad, confiabilidad e integridad de la

información que se genera en la articulación u operativización de las funciones sustantivas del sistema de educación superior del Ecuador.

5.2 Recomendaciones

- El cuerpo directivo de las instituciones de educación superior debe levantar y revisar los activos de información de los distintos niveles de gestión articulados con las funciones sustantivas y las de gestión administrativa de tal forma que les permita establecer los roles y responsabilidades de gobierno de seguridad de la información.
- Las instituciones de educación superior deben conformar un comité de seguridad de la información para sea esta quien determine la alineación estratégica entre los procesos de la institución y los de seguridad de la información y a través de estos generar las políticas y procedimiento que permitan garantizar los activos de información de la gestión y de las funciones sustantivas (investigación, vinculación y docencia).
- El cuerpo directivo de la institución de educación superior en conjunto con el comité de seguridad de la información debe conocer y seleccionar de los principales estándares de gobierno de seguridad de la información cual es el que se adoptará para su implementación, ejecución, dirección y control.
- Las instituciones de educaciones de educación superior deberán del modelo de gobierno de seguridad de la información elegido para trabajar en la articulación del mismo al modelo de gobierno corporativa, su planificación estratégica instituciones, así como la de establecer los diferentes niveles de gestión se seguridad de la información y dar a conocer a estudiantes, docentes y personal administrativo para su ejecución.

CAPÍTULO 6. PROPUESTA

6.1 Titulo

"Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador"

6.2 Datos Informativos

Institución	: Instituciones de Educación Superior del Ecuador
Beneficiarios	: Personal docente, estudiantes, administrativos de la IES
Responsable	: Ing. Hugo Heredia Mayorga
Director	: PhD. Vicente Merchán Rodríguez.

6.3 Antecedentes de la Propuesta

Gashgari, Walters, y Wills (2017) sostienen que la seguridad de la información debe estar integrada al gobierno corporativo y resguardada por un gobierno en el que se incluye reportes, responsabilidad y manejo de riesgos. Una buena implantación de un gobierno de seguridad de la información debe ofrecer una alineación estratégica, manejo de riesgos, manejo de recursos; para aquello es fundamental identificar los factores críticos que permita alcanzar el éxito a largo plazo en las organizaciones; además, de las prácticas desarrolladas por la ISO/IEC 27014, así como las áreas esenciales para la gobernabilidad.

Sin embargo, Carcary, Renaud, McLaughlin, y O'Brien, (2016) en su propuesta de un marco de Gobierno de Seguridad de la Información muestran la relevancia de adoptar y emplear un enfoque de madurez de la capacidad de administrar y controlar la seguridad de la información, fácil de usar con un lenguaje común y enfocado al negocio permitiendo a las organizaciones establecer el estándar de seguridad apropiado para cada negocio individual y aprovechar los recursos en toda la

organización para lograr un nivel de seguridad en la entrega de confianza y ventaja empresarial.

Por otra parte, Tenorio Chacón (2016) establece que los beneficios de un gobierno de seguridad de la información robusto incluyen el mejorar la confianza en las relaciones con los clientes con el propósito de proteger la reputación de la organización entregando responsabilidades por el resguardo de la información durante todas las actividades críticas para el negocio; mientras tanto, Luqman Ayodele (2018) concluye que la gobernanza inadecuada de la seguridad de la información afecta a las organizaciones ya sea que estas mantengan su inconsistencia en la configuración de sus sistemas de información.

Da Veiga y Eloff (2017) sostienen que para implementar un marco de referencia de gobierno de seguridad de la información deben generarse comportamientos y un nivel de cultura de seguridad de la información en todas las instancias de la organización, es decir, desde los altos ejecutivos hasta los niveles operativos de tal forma que permita reducir el impacto de pérdida o sustracción de la información en la organización.

Para aquello, es importante que la organización gobierne de manera efectiva la seguridad de la información, sus componentes, políticas y métricas de una manera holística desarrollando entre los actores comportamientos que van de la mano con las políticas y procedimientos del modelo de gobierno de seguridad de la información.

Si bien es cierto las vulnerabilidades de la información y las constantes amenazas a las cuales están sujetas y el daño en la confidencialidad, integridad y disponibilidad de la información y activos de TI en la actualidad han sido altos, debido a esto es sorprendente que las instituciones u organizaciones todavía piensen que esto es solamente responsabilidad de los departamentos de TI (Clark y Sitko, 2008).

Sin embargo, hasta que no se logre hacer entender a los ejecutivos de las organizaciones sobre la importancia dentro de la organización de su participación para que se alcance el éxito; Clark y Sitko (2008) aseguran que la implementación de un framework de seguridad de la información permitirá la mejora significativa de la organización en su trabajo de alinear la seguridad de la información a los procesos de Gobernanza Corporativa.

De ahí que (CGI Group, 2016), establece que la seguridad y la gobernanza no pueden estar separadas ni pueden lograrse solo con un despliegue de soluciones técnicas, para esto las organizaciones necesitan un enfoque holístico donde conjuguen los valores claves como la responsabilidad, en todos los ámbitos de la organización.

Otro de los factores relevantes en un gobierno de seguridad de la información es la participación de la alta gerencia la cual debe estar comprometida e informada, para tomar las decisiones acertadas en función de un análisis de riesgos con el fin de enfrentar las amenazas actuales.

Carcary et al. (2016) sostienen que un marco de gobierno de seguridad de la información debe estar centrado en determinar la capacidad que toda organización debe tener para dirigir, supervisar, y controlar las acciones, procesos y procedimientos necesarios para proteger la información, de la misma manera para proporcionar confidencialidad, integridad, disponibilidad, accesibilidad de los datos que se encuentran en los sistemas de información.

También afirma que, dentro de las organizaciones los interesados en el negocio y los interesados de TI deben enfocar su esfuerzo por cerrar brechas de seguridad de la información y adoptar un marco de trabajo que garantice e impulse alcanzar un nivel de madurez medido a lo largo de su implementación dentro de la organización como un proceso de mejora continua.

Es por ello que, Bowen, P., Chew, E., Hash (2007), establecen una conceptualización de lo que es gobernanza de la seguridad de la información garantizando su implementación de manera proactiva para respaldar su misión de manera rentable, al mismo tiempo que debe gestionar los riesgos en constante evolución.

6.4 Justificación

Un gobierno de seguridad de la información tiene un conjunto de requisitos, desafíos, actividades y estructuras que le permite la identificación de roles y responsabilidades claves que influyen en la aplicación de políticas y procedimientos de seguridad de la información (Bowen, P., Chew, E., Hash, 2007).

El enfoque de Asgarkhani, Correia, y Sarkar (2017) es mucho más amplio con relación al gobierno de TI, hablan de una clasificación de lo que es el gobierno de seguridad de la red y el de seguridad de la información en cuanto a vulnerabilidades y fuentes de riesgos potenciales que influyen en una efectiva gobernanza de seguridad. Finalmente, de Oliveira Alves, Rust da Costa Carmo, y Ribeiro Dustra de Almeida (2006) concluyen que si bien los conceptos de gobierno corporativo están bien conocidos, la gobernanza de seguridad de la información sigue siendo un gran desafío para las organizaciones; sin embargo, el objetivo es alinear las mejores prácticas de los Modelos de Gobierno con los modelos de Gobernanza de Seguridad de la Información visualizando claramente la Alineación Estratégica entre la seguridad de la información y objetivos de negocios.

6.5 Objetivos

6.5.1 Objetivo General

Diseñar un modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior del Ecuador.

6.5.2 Objetivo Especifico

- Determinar los criterios de armonización de los modelos de gobierno de TI ISO/IEC 38500:2015 y el modelo de gobierno de seguridad de la información ISO/IEC 27014:2013.
- Elaborar un modelo de gobierno de seguridad de la información para Instituciones de Educación Superior del Ecuador.

6.6 Análisis de Factibilidad

El trabajo de investigación realizado para determinar un modelo de Gobierno de Seguridad de la Información para las instituciones de educación superior cuenta con el presupuesto necesario para el desarrollo de la implantación del modelo de gobierno propuesto, posibilitando de esta manera asegurar el activo más importa te para la Institución que es la información.

6.6.1 Factibilidad Técnica

La investigación cuenta con los recursos tecnológicos necesarios en cuanto a infraestructura, sistemas de información, accesos a datos e información requerida.

El apoyo por parte de las autoridades de la institución de la unidad de observación es de vital importancia para la consecución de la investigación, así como también, de las direcciones de acreditación, vicerrectorados académicos y tecnológicos y cada una de las unidades académicas y departamentos como proveedores directos de los datos e información.

6.6.2 Factibilidad Económica

Podemos mencionar que económicamente el presente proyecto de investigación es factible ya que los costos que implican el análisis, estudio, tiempo empleado en estos temas son asumidos por el investigador, mientras que los tiempos del personal de la institución involucrados son asumidos por la unidad de observación de la investigación.

6.7 Fundamentación

6.7.1 ISO/IEC 38500:2015

La ISO/IEC 38500:2015 es la norma internacional que habla sobre elementos de gobierno de TI en las organizaciones, en ella se fijan estándares para un buen gobierno de los procesos, procedimientos y la toma de decisiones en términos de referencia a los sistemas y tecnologías de información, por otro lado, describe que un modelo es un conjunto de componentes que están relacionados a describir el funcionamiento de un objeto, sistema o concepto (INEN-ISO/IEC, 2019).

Para objeto de la investigación se establece como modelo de referencia la norma ISO/IEC 38500:2015 (INEN-ISO/IEC, 2019) como el modelo de Gobierno de TI bajo los cuales se establecerán los elementos de trabajo para determinar el modelo de gobierno de Seguridad de la Información para Instituciones de Educación Superior en concordancia con lo que establece la norma ISO/IEC 27014:2013.

Castro Márquez, Veláquez Pérez, y Castro Silva (2018) , concluyen que la integración de estándares y buenas prácticas de seguridad, gestión de servicios y gobierno de TI contribuyen al mejoramiento continuo de las organizaciones en un contexto propiamente corporativo.

El modelo de gobernanza de la norma ISO/IEC 38500:2015 está fundamentada en tres ejes principales, el primero evaluar el uso actual y futuro de las TI, el segundo la preparación para la implementación de políticas y estrategias para asegurar que

el uso de TI cumpla con los objeticos de negocio, y el tercer establecer el monitoreo de la conformidad con las políticas y el desempeño en relación con las estrategias establecidas, es decir muestra un modelo de gobernanza que Evalúa-Dirige y Monitorea (INEN-ISO/IEC, 2019).

El Gráfico 35 muestra el Modelo para la Gobernanza de TI propuesto por la norma ISO/IEC 38500:2015 en la que se puede apreciar tres elementos principales de evaluar, dirigir y monitorear las estrategias, políticas, planes y propósitos en la consecución de los objetivos estratégicos de la organización (Quintanilla, 2016)(INEN-ISO/IEC, 2019).

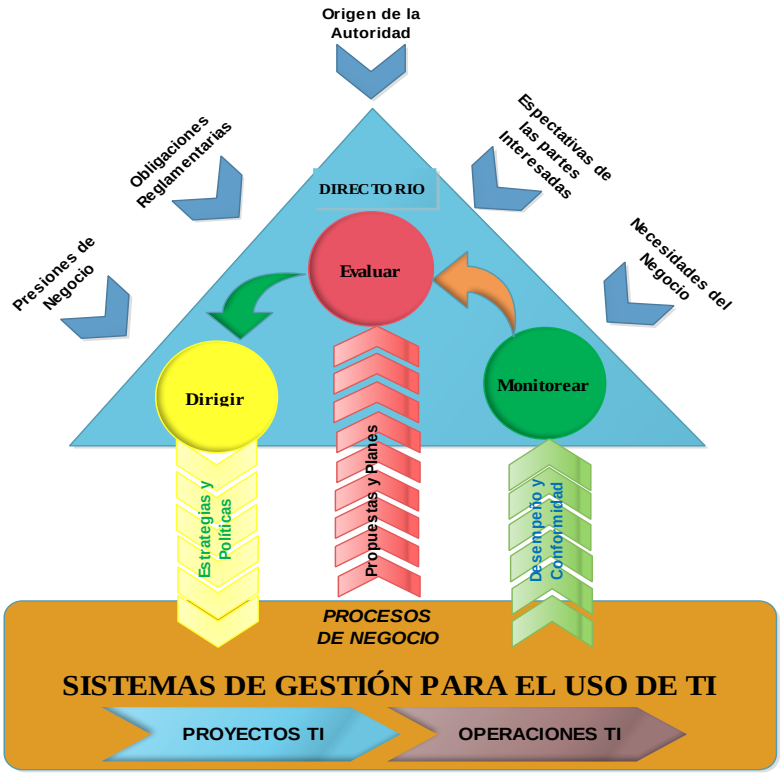

Gráfico 35. Modelo para la Gobernanza de TI.
Fuente: (INEN-ISO/IEC, 2019)

Dentro del contexto que se analiza Merchán y Rodríguez (2015) aseguran que dentro de la norma ISO/IEC 38500:2015 también se definen principios rectores, los mismos que son aplicables a cualquier organización. Estos principios

establecen la conducta mediante la cual se regirá a los directores, ejecutivos y guiará en la mejor toma de decisiones (Ver Tabla 34).

Tabla 34. Principios del estándar ISO/IEC 38500:2015

PRINCIPIOS	DESCRIPCIÓN
RESPONSABILIDAD	Los individuos y grupos dentro de la organización entienden y aceptan sus responsabilidades con respecto, tanto a la oferta como a la demanda de TI. Quienes tienen la responsabilidad de las acciones también tienen la autoridad para realizar esas acciones.
ESTRATEGIAS	La estrategia de negocios de la organización toma en cuenta las capacidades actuales y futuras de TI; los planes para el uso de TI satisfacen las necesidades actuales y continuas de la estrategia de los negocios de la organización.
ADQUISICIÓN	Las adquisiciones de TI se realizan por razones válidas, sobre la base del análisis apropiado y en curso, con una toma de decisiones clara y transparente. Existe un equilibrio adecuado entre los beneficios, las oportunidades, los costos y los riesgos, tanto a corto como a largo plazo.
DESEMPEÑO	TI es adecuada para el propósito de apoyar a la organización que brindan los servicios, los niveles de servicio y la calidad de servicio requeridos para cumplir con los requisitos de negocios actuales y futuros
CONFORMIDAD	El uso de TI cumple con todas las leyes y reglamentos obligatorios. Las políticas y prácticas están claramente definidas, implementadas y aplicadas
COMPORTAMIENTO HUMANO	Las políticas, prácticas y decisiones de TI demuestran respeto por el Comportamiento Humano, incluidas las necesidades actuales y cambiantes de todas las 'personas en el proceso'

Fuente: (INEN-ISO/IEC, 2019)

Como se señala en INEN-ISO/IEC (2019) el modelo de referencia está compuesto de tres actividades principales que son la dirección (Dirigir), la evaluación (Evaluar) y el seguimiento (Monitorear), los mismos que se resumen en la Tabla 35.

Tabla 35. Modelo del estándar ISO/IEC 38500:2015

ACTIVIDADES	DESCRIPCIÓN
EVALUAR	Al evaluar el uso de TI, el directorio debe considerar las presiones externas o internas que actúan sobre la organización como el cambio tecnológico, las tendencias económicas y sociales, las obligaciones reglamentarias, las expectativas legítimas de las partes interesadas y las influencias políticas, mediante evaluaciones continuas a medida que cambien las circunstancias de las necesidades de negocios actuales y futuras, los objetivos institucionales actuales y futuros que tienen que alcanzar, así como mantener la ventaja competitiva, para alcanzar los objetivos específicos de los planes y las propuestas que se evalúan (INEN-ISO/IEC, 2019).
DIRIGIR	El directorio debe asignar la responsabilidad y la preparación directa, y la implementación de estrategias y políticas. Las estrategias deberían establecer la dirección de las inversiones en TI y lo que TI debería lograr. Las políticas deberían establecer un buen comportamiento en el uso de TI, fomentando una cultura de buena gobernanza de las TI en su organización al exigir a los administradores que proporcionen información oportuna, que cumplan con la dirección y que se ajusten a los seis principios de buena gobernanza de ser necesario deben dirigir la presentación de propuestas para su aprobación a fin de abordar las necesidades identificadas (INEN-ISO/IEC, 2019).
MONITOREAR	El directorio debe monitorear, a través de sistemas de medición apropiados, el desempeño de TI asegurando que de acuerdo con las estrategias y particularmente con respecto a los objetivos de negocio y que se ajuste a las obligaciones externas (reglamentos, de legislación y contractuales) y las prácticas de trabajo internas (INEN-ISO/IEC, 2019).

6.7.2 ISO/IEC 27014:2013

La norma ISO/IEC 27014:2013 (INEN-ISO/IEC, 2016) pretende ser una guía sobre la gobernanza de seguridad de la información, proporciona conceptos y principios mediante los cuales las organizaciones pueden evaluar, dirigir, monitorear y comunicar las actividades relacionadas con seguridad de la información. Como manifiesta la norma es importante para el directorio de la organización desarrollar una visión holística de un modelo de gobierno dentro del cual el gobierno de seguridad debe ser una parte importante, los mismos que se superponen en sus alcances.

Sin embargo, la ISO/IEC 27014:2013 establece ciertos resultados que deben evaluarse al momento de implantar el gobierno de seguridad de la información, entre los cuales incluyen la visibilidad del directorio sobre el estado de la seguridad, un enfoque ágil para la toma de decisiones y los riesgos de la información así como las inversiones eficientes y eficaces en la seguridad de la información. Al igual como la ISO/IEC 38500:2015 para el cumplimiento de los requisitos externos (legales, reglamentarios o contractuales).

Es importante recalcar la relación que existe entre el Gobierno de TI y el Gobierno de Seguridad de la Información, tal como se observa en la Gráfico 36.

Gráfico 36. Gobierno de SI y TI.

Fuente: (INEN-ISO/IEC, 2016)

De manera similar, en la norma ISO/IEC 38500:2015, las definiciones de entorno de gobierno organizativo y las diferencias entre gobierno y administración se encuentran en la norma, enfatizando que la construcción de un puente de comunicación beneficiará el logro de los objetivos empresariales.

La ISO/IEC 27014:2013 presenta seis principios a través de los cuales el gobierno corporativo puede diseñar e implementar su marco de gobierno de seguridad de la información, enumerando las responsabilidades que deben tener en cuenta. Tal como se muestra en la Tabla 36.

Tabla 36. Principios del estándar ISO/IEC 27014:2013

PRINCIPIOS	DESCRIPCIÓN
Establecer la seguridad de la información en toda la organización	El gobierno de seguridad de la información debe garantizar que las actividades de seguridad de la información sean comprensivas e integradas, debe ser manejada a nivel organizativo con la toma de decisiones teniendo en cuenta los negocios, seguridad de la información y todas las actividades relacionadas con la seguridad física y lógica deberían estar estrechamente coordinadas.
Adoptar un enfoque basado en riesgos	El gobierno de seguridad de la información debe basarse en decisiones basadas en el riesgo. La determinación de cuánta seguridad es aceptable debe estas basada sobre el nivel del riesgo de una organización, incluyendo la pérdida de la ventaja competitiva, los riesgos de cumplimiento y responsabilidad, las interrupciones operativas, daño a la reputación y la pérdida financiera. Para adoptar una gestión de riesgos de la información apropiada para la organización, se tomará en cuenta que la misma sea consistente e integrado con el enfoque general de gestión de riesgos de la organización.
Establecer la dirección de las decisiones de inversión	El gobierno de seguridad de la información debe establecer una estrategia de inversión de seguridad de la información basado en los resultados de negocios alcanzados, lo que resulta en la armonización entre los requisitos de negocios y seguridad de la información, tanto en corto como a largo plazo, cumpliendo así con las necesidades actuales y futuras de las partes interesadas
Asegurar la conformidad con los requisitos internos y externos	El gobierno de seguridad de la información debería garantizar que las políticas y prácticas de seguridad de la información deben ajustarse conforme a la legislación y regulaciones relevantes obligatorias, así como los negocios comprometidos o requisitos contractuales y otros requisitos externos o internos.
Fomentar un entorno de seguridad positiva	El gobierno de seguridad de la información debe basarse en el comportamiento humano, incluyendo las necesidades cambiantes de todas las partes interesadas ya que el comportamiento humano es uno de los elementos fundamentales para apoyar el nivel adecuado de seguridad de la información. Si no están coordinados adecuadamente los objetivos, las funciones, responsabilidades y recursos pueden entrar en conflicto entre sí, lo que resulta en el incumplimiento de los objetivos de negocios. Por lo tanto, la armonización y la orientación concertada entre los diferentes actores es muy importante
Desempeño de la opinión en relación a los resultados de negocio	El gobierno de seguridad de la información debe garantizar que el enfoque adoptado para proteger la información es apto para el propósito de apoyar la organización, proporcionando niveles acordados de seguridad de la información. El desempeño de seguridad debe ser mantenido a niveles requeridos para satisfacer las necesidades de negocios actuales y futuros. Esto se puede hacer mediante la realización de exámenes prescritos de un programa de medición del desempeño para el seguimiento, auditoría y mejora, y por lo tanto vincular el desempeño de seguridad de información para el desempeño de negocios.

Fuente: (INEN-ISO/IEC, 2016)

A diferencia de ISO/IEC 38500:2015, que presenta un modelo Evaluar-Dirigir-Monitorear y deja al comité para crear su propio marco de gobierno particular; ISO/IEC 27014 muestra un marco proporcionado para el manejo de la seguridad de la información destacando el proceso para su implementación (Ver Gráfico 37).

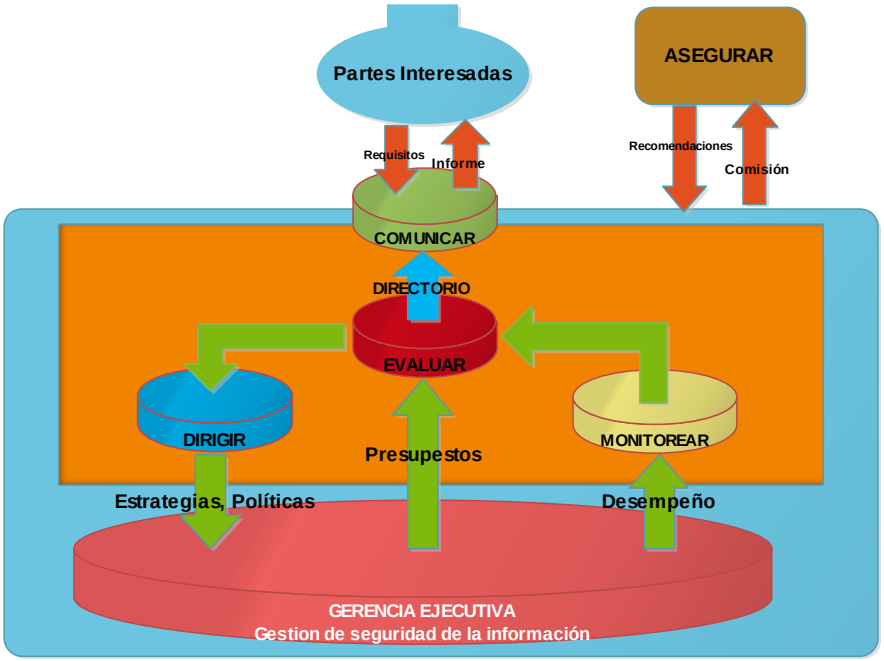

Gráfico 37. Implementación del modelo de seguridad de la información.

Fuente: (INEN-ISO/IEC, 2016)

Los procesos gobernantes que enfoca la ISO/IEC 27014 están definidos en cinco áreas con un flujo de comunicación, entre ellas, enfocado al monitoreo, evaluación, comunicación, dirección y, por último, el aseguramiento; es decir, Evaluar – Dirigir – Monitorear – Comunicar – Asegurar (Ver Tabla 37).

Tabla 37. Modelo del estándar ISO/IEC 27014:2013

MODELO	DESCRIPCIÓN
EVALUAR	Evaluar" es el proceso de gobierno que considera el logro actual y previsión de los objetivos de seguridad basados en los procesos actuales y los cambios previstos y determina donde se requieren ajustes para optimizar el logro de los objetivos estratégicos en el futuro.
DIRIGIR	"Dirigir" es el proceso de gobierno por el cual el directorio da la directriz acerca de los objetivos de seguridad de la información y la estrategia que necesitan ser implementadas. La directriz puede incluir cambios en los niveles de dotación de recursos, asignación de recursos, el establecimiento de prioridades de las actividades y las aprobaciones de las políticas, la aceptación de riesgos materiales y planes de gestión de riesgos.
MONITOREAR	"Monitorear" es el proceso de gobierno que permite al directorio evaluar el logro de los objetivos estratégicos
COMUNICAR	Comunicar" es el proceso de gobierno bidireccional mediante el cual el directorio y las partes interesadas intercambian información sobre seguridad de la información adecuada a sus necesidades específicas.
ASEGURAR	"Asegurar" es el proceso de gobierno mediante el cual se audita, revisa o certifica las actividades de gobierno y operativas con el fin de alcanzar el nivel deseado de seguridad de la información.

Fuente: (INEN-ISO/IEC, 2016)

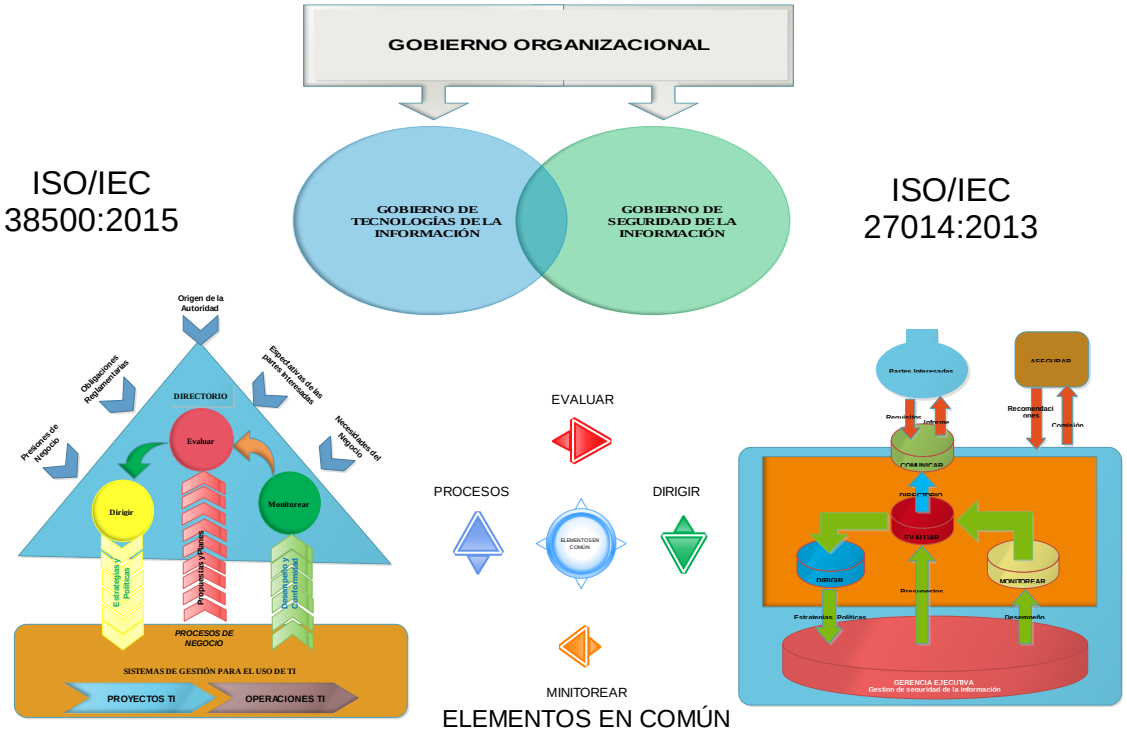

Gráfico 38. Elementos Comunes ISO/IEC 27014:2013 e ISO/IEC 35800:2015

6.7.3 Armonización de la norma ISO 38500:2015 e ISO 27014:2013

Para realizar la armonización de los Modelos de Gobierno que proponen las norma ISO/IEC 38500:2015 y la ISO/IEC 27014:2013, se establecerán e identificar las dificultades y a través de la comparación de los objetivos, políticas, modelos, procesos de acuerdo al modelo propuesto por (Baldassarre, Caivano, Pino, Piattini, y Visaggio, 2012)(Pardo, Pino, Garcia, Baldassarre, y Piattini, 2013) (Serrano et al., 2018).

Para ello se mostrará la similitud de los dos estándares determinando qué elementos de la ISO/IEC 27014 están incluidas en la ISO/IEC 38500, con el propósito de homogeneizar, mapear e integrar, como parte de las técnicas y métodos utilizadas por los procesos de armonización (Serrano et al., 2018) como primer paso para realizar el mapeo de los estándares.

Para el mapeo comparativo se ejecutó los siguientes pasos:

1. Se estableció los diferentes elementos a comparar entre ISO/IEC 38500:2015 e ISO/IEC 27014:2013.

2. Se diseñó el mapeo entre los dos estándares, para ello se tomó como referencia el trabajo de (Serrano et al., 2018), en los términos siguientes:

A. Obtener los elementos identificados en el paso anterior que serán sujetos a comparación;
B. Definir una escala de comparación, para mostrar el grado de similitud entre ambos estándares; y.
C. Definir la plantilla de comparación a través de la cual se determinan si los valores de la escala representan la relación de ISO/IEC 27014 en ISO/IEC 38500.

3. El mapeo realizado establece un proceso de valoración de los elementos y componentes principales de las dos normas ISO mostrado en una tabla. En donde las filas están los elementos de la norma ISO/IEC 38500:2015 y en las columnas se encontrarán los elementos de la norma ISO/IEC 27014:2013.

Para ello se consideró los elementos seleccionados en el paso 1 para analizar la relación que existe entre ambas normas (Serrano et al., 2018).

1. Selección de los Elementos y/o componentes de la ISO/IEC 38500:2015 y de la ISO/IEC 27014:2013

Para el análisis se consideraron los siguientes elementos de comparación:

- Objetivos de gobierno.
- Principios de gobierno.
- Modelos de Gobierno.
- Actividades de Gobernanza.

En la Tabla 28 se muestran los objetivos del gobierno de seguridad de la información y los objetivos del gobierno de tecnologías de la información. El

orden en que se presentan los objetivos no significa que exista un vínculo específico entre ellos, los objetivos del gobierno de seguridad de la información y el gobierno de tecnologías de la información están relacionados entre sí.

Tabla 38. Objetivos de gobierno

Gobierno de TI (ISO/IEC 38500:2015)	**Gobierno de Seguridad de la Información (ISO/IEC 27014:2013)**
• Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI. • Mitigar el riesgo de los directores no cumpliendo con sus obligaciones • Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI. • Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	• Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias • Agregar valor al tablero. de directores y partes interesadas • Asegurar que la información los riesgos están siendo adecuadamente tratado

La Tabla 39 se puede observar que los principios del gobierno de seguridad de la información y el gobierno de tecnologías de la información están más orientados a la organización.

Tabla 39. Principios de gobierno

Gobierno de TI (ISO/IEC 38500:2015)	**Gobierno de Seguridad de la Información (ISO/IEC 27014:2013)**
• Responsabilidad • Estrategias • Adquisición • Desempeño • Conformidad • Comportamiento humano	• Establecer la seguridad de la información en toda la organización • Adoptar un enfoque basado en riesgos • Establecer la dirección de las decisiones de inversión • Asegurar la conformidad con los requisitos internos y externos • Fomentar un entorno de seguridad positiva • Desempeño de la opinión en relación a los resultados de negocio

Como se puede observar en la Tabla 40, en los dos modelos existe la adopción de un sistema de dos niveles, como una forma de aumentar la confiabilidad del proceso de gobierno por segregación de funciones.

Tabla 40. Modelos de gobernanza

Gobierno de TI (ISO/IEC 38500:2015)	**Gobierno de Seguridad de la Información (ISO/IEC 27014:2013)**
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)

Si se observan las actividades de cada una de las normas ISO/IEC 38500 e ISO/IEC 27014 están determinadas por la evaluación, dirección y monitoreo, como elementos comunes, sin embargo, la comunicación se encuentra explicita en la ISO/IEC 38500:2015 mientras que en la ISO/IEC 27014:2013 se encuentra como parte esencial del modelo la Comunicación y el Aseguramiento hacia el cumplimiento de los objetivos organizacionales (Ver Tabla 41).

Tabla 41. Actividades de gobernanza

Gobierno de TI (ISO/IEC 38500:2015)	Gobierno de Seguridad de la Información (ISO/IEC 27014:2013)
Evaluar el uso de TI incluidas las estrategias, propuestas y acuerdos de suministros	Evaluar el logro de los objetivos de seguridad y determinar los ajustes.
Dirigir la planificación e implementación de planes y políticas, incluidas las transiciones de proyectos a estados operativos y prestaciones propuestas para la aprobación para abordar las necesidades identificadas.	Dirigir objetivos, estrategias, recursos, prioridades y aprobaciones de inversiones.
Monitorear el desempeño de TI y su cumplimiento con obligaciones externas y prácticas de trabajo internas	Monitorear el logro de objetivos estratégicos
Si bien no existe un proceso de comunicación explícito en el gobierno de TI ISO 38500, hay aspectos relacionados con la responsabilidad de los directores que requieren que los gerentes proporcionen información oportuna.	Comunicar la seguridad de la información al cuerpo directivo y las partes interesadas
	Asegurar, mediante auditorías independientes y objetivas, revisiones y certificaciones, la validez de los objetivos y acciones relacionadas con el gobierno y las operaciones de seguridad de la información

2. Diseño del mapeo

Una vez que han identificados los elementos de cada uno de los estándares, se procedió a determinar el nivel de relación que existe entre cada uno de ellos mediante el uso de la escala de similitud.

Para el trabajo se utilizó la matriz de Holmes como herramienta de comparación, análisis y priorización de cada uno de los criterios en base a una escala valorativa (ver Tabla 42) considerada para establecer la importancia que tienen los elementos de los modelos de gobierno, tanto de TI como de Seguridad de la Información establecidos en las normas ISO 38500:2015 e ISO 27014:2013, respectivamente (Albán y Saavedra, 2009).

Con los parámetros o criterios establecidos y definidos, la matriz de Holmes permitió la toma de decisiones en función de los criterios y juicios de valor de acuerdo con la escala determinada con base a la cuantificación respecto a cada

elemento (ver Tabla 43). La comparación se la realiza considerando una matriz triangular superior y se completa con los opuestos a la escala según corresponda al análisis obteniendo al final una matriz tipo L.

Tabla 42. Escala de ponderación Matriz de Holmes

Escala	Escala Verbal
0.5	Corresponde al valor de la diagonal principal de la matriz considerando la comparación del criterio consigo mismo.
1	Si el criterio es más importante que los otros criterios
0	Si el criterio es menos importante que los otros criterios

Tabla 43. Criterios para el análisis

Criterio	Definición
Eficacia	Se refiere a qua información generada sea relevante y pertinente al negocio, permitiendo lograr las metas estratégicas y mejoras a los procesos de negocio.
Eficiencia	La eficiencia trata de entregar o proveer la información de calidad a los servicios de manera más rápida permitiendo a los departamentos de TI buscar las maneras de lograrlo, con estrategias que aporten a este objetivo.
Confidencialidad	Se relaciona con la característica de protección, privacidad y acceso a la información y a las directivas y acciones necesarias para garantizarlo.
Integridad	Se refiere a la integridad de los datos que son tratados para generar información, estos deben ser precisos, válidos y coherentes con mecanismos que impidan la eliminación, modificación y eliminación no autorizada (Gelbstein, 2011a)
Disponibilidad	Se refiere a que la información debe estar disponible en el momento que sea requerida por cualquier unidad de negocio, así como a los servicios de TI que los requerimientos del negocio necesiten.
Confiabilidad	Fernández y Llorens (2011) la trabajan como la provisión de información apropiada que los servicios de TI proporcionan para ser considerados dentro de la toma de decisiones (Fernandez y Llorenz, 2014)
Alineamiento Estratégico	Son las estrategias de gobernanza de TI como de seguridad de la información apoyen a la estrategia empresarial.
Satisfacer las necesidades de los interesados	Se entiende como las necesidades de información que cada uno de los interesados busca obtener para la toma de decisiones evaluando el beneficio y riesgos asociados.
Cubrir la organización de forma integral.	Se contempla todos los procesos y funciones necesarios para la gobernabilidad y administración de toda la organización incluyendo los servicios de TI
Estructuras organizativas	Define las responsabilidades que tiene con el gobierno de TI y de seguridad de la información con el propósito de asegurar los objetivos planteados.
Manejo de riesgos	Se considera como el manejo adecuado de los riesgos asociados al uso y generación de información por parte de TI y cada unidad de negocio de la organización
Medir el rendimiento	Es el valor que genera las TI y las estrategias de gobernanza de seguridad de la información en la ejecución y control de los proyectos, desempeños enfocados al costo beneficio.
Manejo de recursos.	Se define como el manejo adecuado que debe tener cada uno de los recursos disponibles que tenga la organización para garantizar el cumplimiento de las estrategias organizacionales.
Entrega de Valor	Mide si la información generada por cada una de las unidades organizaciones responde a las necesidades y cumplimiento de los objetivos organizaciones, es decir es el valor de uso que se puede dar a la información generada para la toma de decisiones.

Posteriormente se realizó la suma para cada uno de los criterios o parámetros con el fin de determinar cuantitativamente la importancia del criterio o parámetro que ordenándolos de mayor a menor permitirá observar cuales son los más importantes (ver Tabla 44).

Tabla 44. Matriz de Holmes de comparación de parámetros

Parámetros de comparación de las Normas ISO 38500:2015 e ISO 27014:2013	**Eficacia**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Confiabilidad**	**Alineamiento Estratégico**	**Satisfacer las necesidades de los interesados**	**Cubrir la organización de forma integral**	**Estructuras organizativas**	**Manejo de riesgos**	**Medir el rendimiento**	**Manejo de recursos.**	**Entrega de Valor**	**SUMA**
Eficacia	0,5	1	1	1	1	1	0	0	1	0	1	0	0	0	7,5
Eficiencia	0	0,5	0	0	0	0	0	0	0	1	1	1	1	1	5,5
Confidencialidad	0	1	0,5	1	1	1	0	1	1	1	1	1	1	1	11,5
Integridad	0	1	0	0,5	1	1	1	1	1	1	1	1	1	0	10,5
Disponibilidad	0	1	0	0	0,5	1	1	1	1	1	1	1	1	1	10,5
Confiabilidad	0	1	0	0	0	0,5	1	0	1	1	1	1	0	0	6,5
Alineamiento Estratégico	1	1	1	0	0	0	0,5	1	1	1	1	1	1	1	10,5
Satisfacer las necesidades de los interesados	1	1	0	0	0	1	0	0,5	1	1	1	0	1	0	7,5
Cubrir la organización de forma integral.	0	1	0	0	0	0	0	0	0,5	0	1	1	1	0	4,5
Estructuras organizativas	1	0	0	0	0	0	0	0	1	0,5	0	0	0	0	2,5
Manejo de riesgos	0	0	0	0	0	0	0	0	0	1	0,5	1	1	0	3,5
Medir el rendimiento	1	0	0	0	0	0	0	1	0	1	0	0,5	1	0	4,5
Manejo de recursos.	1	0	0	0	0	1	0	0	0	1	0	0	0,5	0	3,5
Entrega de Valor	1	0	0	1	0	1	0	1	1	1	1	1	1	0,5	9,5

Una vez obtenidos los resultados se aplicó la regla de Pareto a los resultados obtenidos, ordenando~~s~~ y calculando el porcentaje, la suma y el porcentaje

acumulados.-Con esto se hace visible la elección de los criterios o parámetros bajo los cuales se realizó el análisis de los dos modelos de gobierno (Ver Tabla 45).

Tabla 45. Aplicación de la regla de Pareto

Parámetros	Importancia	Importancia Acumulada	% del Total	% del Total Acumulado
Confidencialidad	11,5	11,50	12%	12%
Integridad	10,5	22,00	11%	22%
Disponibilidad	10,5	32,50	11%	33%
Alineamiento Estratégico	10,5	43,00	11%	44%
Entrega de Valor	9,5	52,50	10%	54%
Eficacia	7,5	60,00	8%	61%
Satisfacer las necesidades de los interesados	7,5	67,50	8%	69%
Confiabilidad	6,5	74,00	7%	76%
Eficiencia	5,5	79,50	6%	81%
Cubrir la organización de forma integral.	4,5	84,00	5%	86%
Medir el rendimiento	4,5	88,50	5%	90%
Manejo de riesgos	3,5	92,00	4%	94%
Manejo de recursos.	3,5	95,50	4%	97%
Estructuras organizativas	2,5	98,00	3%	100%

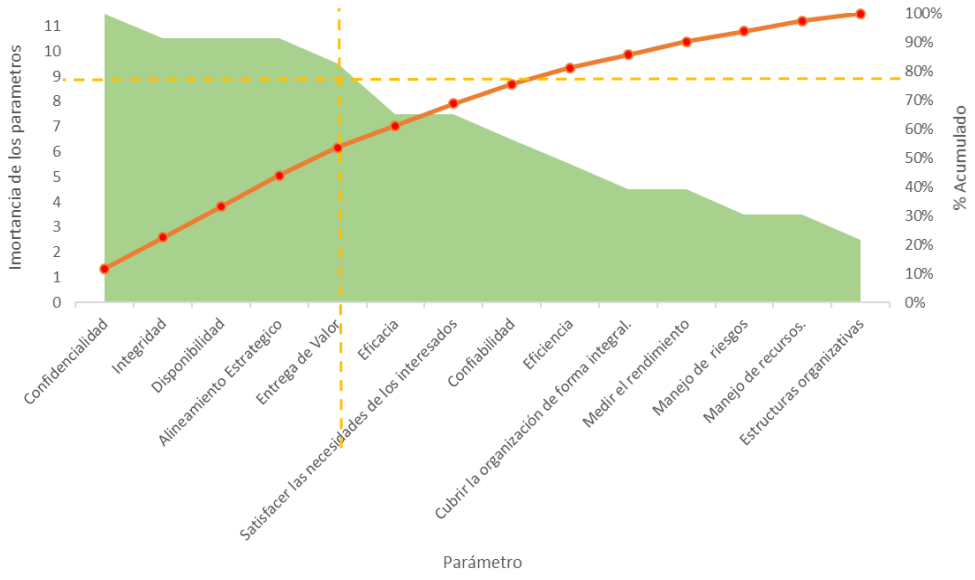

Gráfico 39. Selección de criterios ISO/IEC 27014:2013 e ISO/IEC 35800:2015

Como resultado de aplicar la regla de Pareto los parámetros mayor valor de ponderación es la Confidencialidad, Integridad, Disponibilidad y Alineamiento Estratégico; es decir, los cuatro criterios o parámetros tienen mayor importancia para evaluar la relación entre las normas estudiadas.

Los cuatro criterios o parámetros constituyen en los elementos mínimos deseables en un modelo de Gobierno de Seguridad de la información, la matriz de Holmes (Tabla 46) permitió determinar valores categóricos y numéricos para cada uno de los criterios obteniendo cuatro niveles de calificación que van de 1 a 4 como se detalla en la Tabla 47.

Tabla 46. Matriz de Holmes criterios seleccionados

CRITERIOS	Confidencialidad	Integridad	Disponibilidad	Alineamiento Estratégico	SUMA	Factor de ponderación
Confidencialidad	0,5	1	1	1	4	0,44
Integridad	0	0,5	1	0	2	0,19
Disponibilidad	0	0	0,5	1	2	0,19
Alineamiento Estratégico	0	1	0	1	2	0,19

Tabla 47. Métrica, rangos y categorías

	ESCALA DE VALORACIÓN			
CRITERIO	1-NR	2 -PR	3-MR	4 - FR
Confidencialidad	No facilita la confidencialidad de la información	Facilita un poco la confidencialidad de la información	Facilita medianamente la confidencialidad de la información	Facilita totalmente la confidencialidad de la información
Integridad	No toma en cuenta ningún elemento de integridad de la información	Toma en cuenta algunos elementos que garanticen la integridad de la información	Toma en cuenta la mayoría de los elementos que garantice la integridad de la información	Toma en cuenta todos los elementos que garantizan la integridad de la información
Disponibilidad	No cumple con las políticas de disponibilidad de la información	Cumple con algunas políticas de disponibilidad de la información	Cumple con la mayoría de las políticas de disponibilidad de la información	Cumple con todas las políticas de disponibilidad de la información
Alineamiento Estratégico	No facilita el alineamiento estratégico	Facilita en pocos aspectos el alineamiento estratégico	Facilita en varios aspectos el alineamiento estratégico	Facilita totalmente el alineamiento estratégico

Para facilitar el trabajo del análisis se estableció una nomenclatura para cada uno de los aspectos de la norma ISO/IEC 38500:2015 y la norma ISO/IEC 27014:2013 (ver Tabla 48, Tabla 49).

Tabla 48. Elementos de la norma ISO/IEC 38500:2015

Elementos	Nomenclatura
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	MOGTI
Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	OGTI_1
Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	OGTI_2
Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	OGTI_3
Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	OGTI_4
Evaluar	AGTI_1
Dirigir	AGTI_2
Monitorear	AGTI_3
Responsabilidad	PGTI_1
Estrategia	PGTI_2
Adquisición	PGTI_3
Desempeño	PGTI_4
Conformidad	PGTI_5
Comportamiento Humano	PGTI_6

Tabla 49. Elementos de la norma ISO/IEC 27014:2013

Elementos	Nomenclatura
Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Mogo TI
Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	OGoSI_1
Agregar valor al tablero. de directores y partes interesadas	OGoSI_2
Asegurar que la información los riesgos están siendo adecuadamente tratado	OGoSI_3
Evaluar	AGoSI_1
Dirigir	AGoSI_2
Monitorear	AGoSI_3
Comunicar	AGoSI_4
Asegurar	AGoSI_5
Establecer la seguridad de la Información en toda la organización	PGoSI_1
Adoptar un enfoque basado en riesgos	PGoSI_2
Establecer la dirección de las decisiones de inversión	PGoSI_3
Asegurar la conformidad con los requisitos internos y externos	PGoSI_4
Fomentar un entorno de seguridad positiva	PGoSI_5
Desempeño de la opinión en relación a los resultados de negocio	PGoSI_6

Con la escala definida se procedió a estructurar la matriz que sirvió para establecer el mapeo entre los dos estándares. Esta matriz contiene en las filas los elementos de la norma ISO y en las columnas-los elementos de(Serrano et al., 2018).

3. Ejecución de la Armonización

Criterio de Confidencialidad

Los elementos fuertemente relacionados de la norma ISO/IEC 38500:2015 frente a la norma ISO/IEC 27014:2013 son el sistema de dos niveles: organismo de gestión y gobierno corporativo, los cuales buscan: mitigar el riesgo de los directores que no cumplen con sus obligaciones, estrategias, desempeños, comportamiento humano, responsabilidad, conformidad, gobernar TI, para equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI, así como, para establecer y sostener un entorno apto y monitoreado como se puede observar en el Gráfico 4, en las Tabla 50 y Tabla 51.

Tabla 50. Comparativa ISO/IEC 38500 e ISO/IEC 27014

		ISO/IEC 27014:2013														
		Modelo	**Objetivos**			**Actividades**					**Principios**					
	ISO/IEC 38500:2015	Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios	Agregar valor al tablero. de directores y partes	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación con los resultados de negocio
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**4**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**3**	**2**	**4**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**4**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**3**	**2**	**2**	**3**	**3**	**2**	**4**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**4**	**3**	**2**	**3**	**2**
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**1**	**1**	**1**	**1**	**1**
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	**1**	**4**	**3**	**2**	**1**	**1**	**1**	**3**	**3**	**4**	**3**	**4**	**3**	**3**	**4**
Actividades	*Evaluar*	**4**	**2**	**2**	**3**	**4**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**4**
	Dirigir	**4**	**3**	**3**	**1**	**3**	**4**	**2**	**2**	**3**	**4**	**1**	**3**	**3**	**1**	**1**
	Monitorear	**3**	**3**	**4**	**4**	**3**	**3**	**4**	**2**	**2**	**2**	**4**	**3**	**2**	**2**	**1**
Principios	**Responsabilidad**	**1**	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**
	Estrategia	**3**	**3**	**4**	**3**	**4**	**4**	**4**	**3**	**4**	**3**	**3**	**3**	**3**	**3**	**2**
	Adquisición	**3**	**2**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**4**	**3**	**3**	**2**
	Desempeño	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**2**	**3**	**4**	**3**	**3**
	Conformidad	**2**	**4**	**4**	**3**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
	Comportamiento Humano	**2**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**
ISO/IEC 38501:2015																
Establecer y sostener un entorno apto		**3**	**1**	**4**	**3**	**4**	**4**	**2**	**4**	**4**	**4**	**3**	**3**	**1**	**1**	**4**
Gobernar TI		**4**	**4**	**2**	**4**	**3**	**3**	**3**	**4**	**4**	**3**	**4**	**2**	**2**	**2**	**2**
Revisión Continua		**1**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Tabla 51. Resultado principio de Pareto norma ISO/IEC 38500:2015

Elementos Norma ISO 38500:2015	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	MOGTI	51	7%	51	7%
Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	OGTI_2	48	7%	99	14%
Estrategia	PGTI_2	48	7%	147	20%
Desempeño	PGTI_4	48	7%	195	27%
Comportamiento Humano	PGTI_6	48	7%	243	33%
Responsabilidad	PGTI_1	47	6%	290	40%
Conformidad	PGTI_5	47	6%	337	46%
Adquisición	PGTI_3	46	6%	383	52%
Gobernar TI	GoTI	46	6%	429	59%
Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	OGTI_1	45	6%	474	65%
Establecer y sostener un entorno apto	EA	43	6%	517	71%
Monitorear	AGTI_3	42	6%	559	76%
Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	OGTI_4	40	5%	599	82%
Dirigir	AGTI_2	38	5%	637	87%
Evaluar	AGTI_1	34	5%	671	92%
Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	OGTI_3	31	4%	702	96%
Revisión Continua	RC	30	4%	732	100%

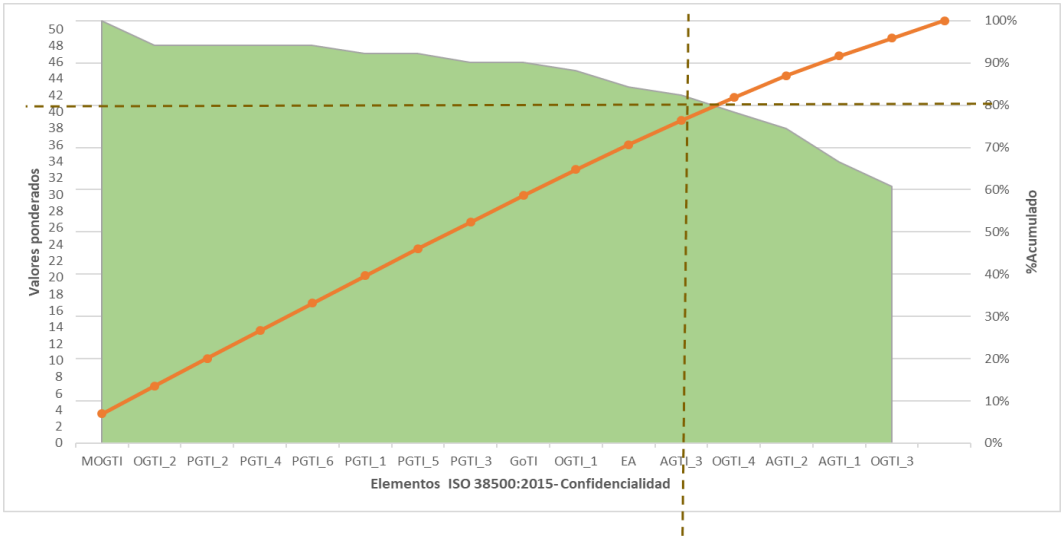

Gráfico 40. Diagrama de Pareto ISO/IEC 35800:2015 - Confidencialidad

De la misma manera, como resultados del mapeo de la norma ISO 27014:2013 frente a la norma ISO/IEC 38500:2015 los elementos de mayor importancia relativa son: evaluar, dirigir, agregar valor al tablero de directores y partes interesadas, monitorear, proporcionar alineación entre las estrategias y objetivos de seguridad de la información con las estrategias y objetivos de negocio para asegurar que la información y los riesgos están siendo adecuadamente tratados, mediante una comunicación asertiva (ver Tabla 52, Tabla 53 y Gráfico 41).

Tabla 52. Principio de Pareto norma ISO/IEC 27014:2013

Elementos Norma ISO 27014:2013	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Evaluar	AGoSI_1	59	8%	59	8%
Dirigir	AGoSI_2	58	8%	117	16%
Agregar valor al tablero. de directores y partes interesadas	OGoSI_2	55	8%	172	23%
Monitorear	AGoSI_3	55	8%	227	31%
Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	OGoSI_1	53	7%	280	38%
Asegurar que la información los riesgos están siendo adecuadamente tratado	OGoSI_3	53	7%	333	45%
Comunicar	AGoSI_4	49	7%	382	52%
Asegurar	AGoSI_5	48	7%	430	59%
Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	MOGoTI	47	6%	477	65%
Establecer la seguridad de la Información en toda la organización	PGoSI_1	46	6%	523	71%
Establecer la dirección de las decisiones de inversión	PGoSI_3	45	6%	568	78%
Desempeño de la opinión en relación a los resultados de negocio	PGoSI_6	44	6%	612	84%
Adoptar un enfoque basado en riesgos	PGoSI_2	43	6%	655	89%
Asegurar la conformidad con los requisitos internos y externos	PGoSI_4	41	6%	696	95%
Fomentar un entorno de seguridad positiva	PGoSI_5	36	5%	732	100,00%

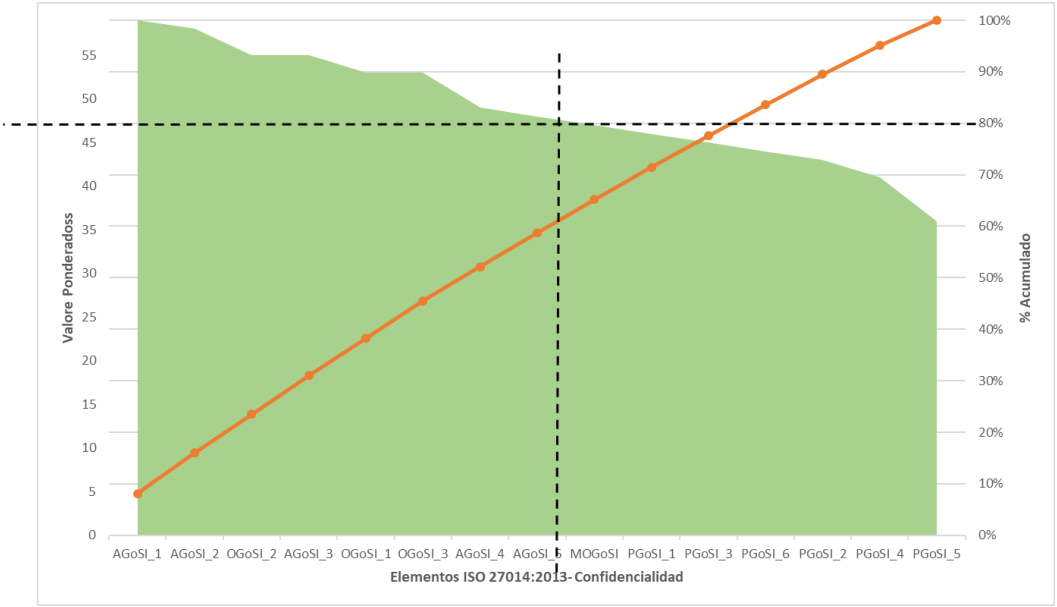

Gráfico 41. Diagrama de Pareto ISO/IEC 27014:2013 - Confidencialidad

Criterio de Integridad

El mapeo bajo la integridad determino que en un sistema de dos niveles que conjuga los organismos de gestión y gobierno corporativo debe estar enfocado en el desempeño, responsabilidad, estrategia tratando de mitigar el riesgo de los directores que no cumplieron con sus obligaciones, en la adquisición y sobre todo en el comportamiento humano para buscar la conformidad en el gobierno de TI, equilibrando los riesgos y fomentando las oportunidades derivadas del uso de TI para establecer y sostener un entorno apto, asegurando el cumplimiento de las obligaciones relativas al uso aceptable de TI con un monitoreo de las actividades como lo indican la Tabla 53, Tabla 54 y el Gráfico 42.

Tabla 53. Comparativa ISO/IEC 38500 e ISO/IEC 27014- Integridad

		ISO/IEC 27014:2013														
		Modelo	**Objetivos**			**Actividades**					**Principios**					
ISO/IEC 38500:2015		Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	Agregar valor al tablero. de directores y partes interesadas	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de negocio
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**4**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**3**	**2**	**4**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**4**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**3**	**2**	**2**	**3**	**3**	**2**	**4**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**4**	**3**	**2**	**3**	**2**
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**1**	**1**	**1**	**1**	**1**
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	**1**	**4**	**3**	**2**	**1**	**1**	**1**	**3**	**3**	**4**	**3**	**4**	**3**	**3**	**4**
Actividades	*Evaluar*	**4**	**2**	**2**	**3**	**4**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**4**
	Dirigir	**4**	**3**	**3**	**1**	**3**	**4**	**2**	**2**	**3**	**4**	**1**	**3**	**3**	**1**	**1**
	Monitorear	**3**	**3**	**4**	**4**	**3**	**3**	**4**	**2**	**2**	**2**	**4**	**3**	**2**	**2**	**1**
Principios	**Responsabilidad**	**1**	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**
	Estrategia	**3**	**3**	**4**	**3**	**4**	**4**	**4**	**3**	**4**	**3**	**3**	**3**	**3**	**3**	**2**
	Adquisición	**3**	**2**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**4**	**3**	**3**	**2**
	Desempeño	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**2**	**3**	**4**	**3**	**3**
	Conformidad	**2**	**4**	**4**	**3**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
	Comportamiento Humano	**2**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**
ISO/IEC 38501:2015																
Establecer y sostener un entorno apto		**3**	**1**	**4**	**3**	**4**	**4**	**2**	**4**	**4**	**4**	**3**	**3**	**1**	**1**	**4**
Gobernar TI		**4**	**4**	**2**	**4**	**3**	**3**	**3**	**4**	**4**	**3**	**4**	**2**	**2**	**2**	**2**
Revisión Continua		**1**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Tabla 54. Principio de Pareto norma ISO/IEC 38500:2015- Integridad

Elementos Norma ISO 38500:2015	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	*MOGTI*	*51*	*7%*	*51*	*7%*
Desempeño	*PGTI_4*	*51*	*7%*	*102*	*14%*
Responsabilidad	*PGTI_1*	*50*	*7%*	*152*	*20%*
Estrategia	*PGTI_2*	*49*	*6%*	*201*	*27%*
Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	*OGTI_2*	*48*	*6%*	*249*	*33%*
Adquisición	*PGTI_3*	*48*	*6%*	*297*	*39%*
Comportamiento Humano	*PGTI_6*	*48*	*6%*	*345*	*46%*
Conformidad	*PGTI_5*	*47*	*6%*	*392*	*52%*
Gobernar TI	*GoTI*	*46*	*6%*	*438*	*58%*
Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	*OGTI_1*	*45*	*6%*	*483*	*64%*
Establecer y sostener un entorno apto	*EA*	*45*	*6%*	*528*	*70%*
Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	*OGTI_3*	*43*	*6%*	*571*	*76%*
Monitorear	*AGTI_3*	*42*	*6%*	*613*	*81%*
Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	*OGTI_4*	*40*	*5%*	*653*	*86%*
Dirigir	*AGTI_2*	*38*	*5%*	*691*	*92%*
Evaluar	*AGTI_1*	*34*	*5%*	*725*	*96%*
Revisión Continua	*RC*	*30*	*4%*	*755*	*100%*

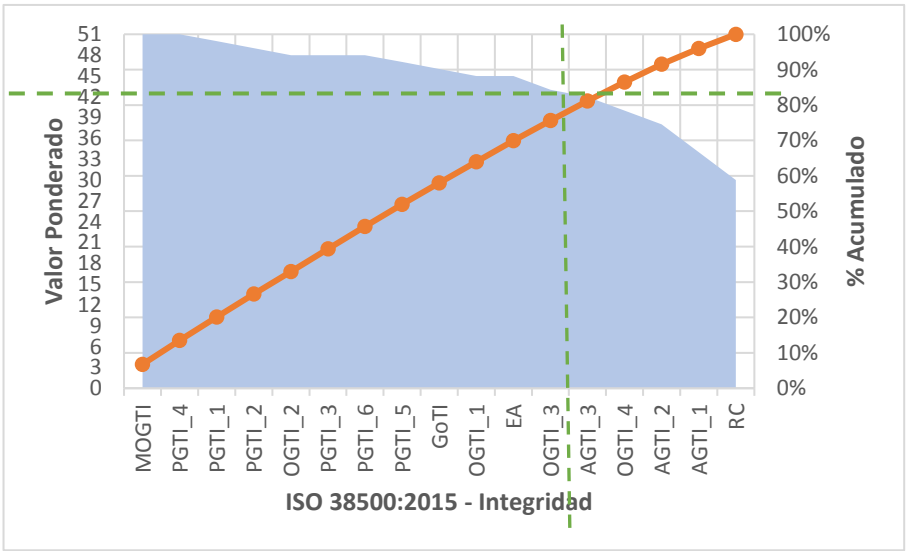

Gráfico 42. Diagrama de Pareto ISO/IEC 38500:2015 - Integridad

De la misma manera, los resultados analizados desde la norma ISO 27014:2013 determinan que evaluar, dirigir, monitorear agregará valor al tablero de directores

y de las partes interesadas asegurando que la información en base a los riesgos está siendo adecuadamente tratada, asegurando así la integridad de la información para proporcionar una alineación entre las estrategias y objetivos de seguridad de la información con las estrategias y objetivos del negocio por medio de una comunicación eficiente como lo indican la Tablas 55 y el Gráfico 43.

Tabla 55. Principio de Pareto norma ISO/IEC 27014:2013 - Integridad

Elementos Norma ISO 27014:2013	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Evaluar	*AGoSI_1*	*62*	*8%*	*62*	*8%*
Dirigir	*AGoSI_2*	*61*	*8%*	*123*	*16%*
Monitorear	*AGoSI_3*	*58*	*8%*	*181*	*24%*
Agregar valor al tablero. de directores y partes interesadas	*OGoSI_2*	*57*	*8%*	*238*	*32%*
Asegurar que la información los riesgos están siendo adecuadamente tratado	*OGoSI_3*	*55*	*7%*	*293*	*39%*
Asegurar	*AGoSI_5*	*55*	*7%*	*348*	*46%*
Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	*OGoSI_1*	*52*	*7%*	*400*	*53%*
Comunicar	*AGoSI_4*	*51*	*7%*	*451*	*60%*
Establecer la seguridad de la Información en toda la organización	*PGoSI_1*	*48*	*6%*	*499*	*66%*
Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	*MOGoTI*	*47*	*6%*	*546*	*72%*
Establecer la dirección de las decisiones de inversión	*PGoSI_3*	*45*	*6%*	*591*	*78%*
Desempeño de la opinión en relación a los resultados de negocio	*PGoSI_6*	*44*	*6%*	*635*	*84%*
Adoptar un enfoque basado en riesgos	*PGoSI_2*	*43*	*6%*	*678*	*90%*
Asegurar la conformidad con los requisitos internos y externos	*PGoSI_4*	*41*	*5%*	*719*	*95%*
Fomentar un entorno de seguridad positiva	*PGoSI_5*	*36*	*5%*	*755*	*100%*

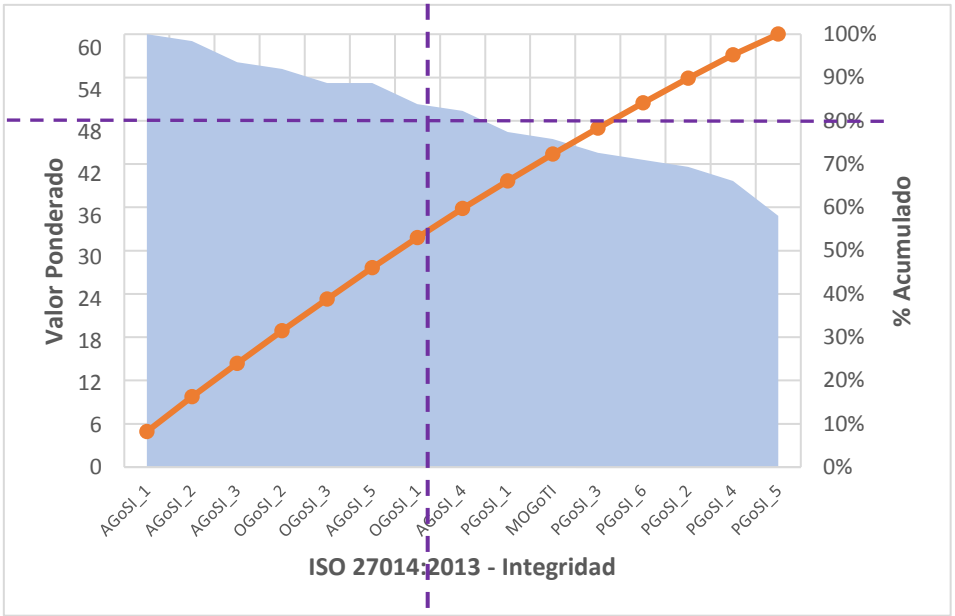

Gráfico 43. Diagrama de Pareto ISO/IEC 27014:2013 - Integridad

Criterio de Disponibilidad

Para garantizar la disponibilidad de la información el modelo de gobierno de seguridad debe estar conformado por un sistema de dos niveles que conjuga los organismos de gestión y gobierno corporativo, que permita definir la estrategias a través de la mitigación delos riesgos con responsabilidad y midiendo su desempeño, en el cumplimiento de sus obligaciones, así como también debe buscar medir la conformidad del gobierno de TI a mediante un comportamiento humano adecuado y la adquisición de herramientas que permitan establecer y sostener un entorno seguro para sus activos de información como se puede observar en la Tabla 56, Tabla 57 y el Gráfico 43.

Tabla 56. Comparativa ISO/IEC 38500 e ISO/IEC 27014 - Disponibilidad

		ISO/IEC 27014:2013														
		Modelo	**Objetivos**			**Actividades**					**Principios**					
	ISO/IEC 38500:2015	Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	Agregar valor al tablero. de directores y partes	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de negocio
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**4**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**3**	**2**	**4**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**4**	**4**	**2**	**4**	**3**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	**2**	**4**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**2**	**3**	**1**	**1**	**4**	**4**	**4**	**3**	**3**	**3**	**4**	**3**	**2**	**3**	**2**
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**4**	**3**	**4**	**2**	**2**	**2**	**2**	**2**	**2**	**3**	**1**	**1**	**1**	**1**	**1**
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	**1**	**4**	**3**	**1**	**1**	**1**	**1**	**3**	**3**	**4**	**3**	**4**	**3**	**3**	**4**
Actividades	*Evaluar*	**4**	**2**	**2**	**4**	**4**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**4**
	Dirigir	**4**	**3**	**3**	**1**	**3**	**4**	**2**	**2**	**3**	**4**	**1**	**3**	**3**	**1**	**1**
	Monitorear	**3**	**3**	**4**	**4**	**3**	**3**	**4**	**2**	**2**	**2**	**4**	**3**	**2**	**2**	**1**
Principios	**Responsabilidad**	**1**	**4**	**3**	**2**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
	Estrategia	**2**	**3**	**4**	**3**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**4**
	Adquisición	**2**	**3**	**3**	**3**	**4**	**4**	**4**	**3**	**3**	**2**	**3**	**3**	**3**	**3**	**4**
	Desempeño	**2**	**3**	**3**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**2**	**3**	**4**	**3**	**3**
	Conformidad	**1**	**4**	**4**	**3**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
	Comportamiento Humano	**1**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**
	ISO/IEC 38501:2015															
Establecer y sostener un entorno apto		**3**	**2**	**4**	**3**	**4**	**4**	**2**	**4**	**4**	**2**	**3**	**3**	**1**	**1**	**4**
Gobernar TI		**4**	**4**	**2**	**4**	**3**	**3**	**3**	**4**	**4**	**3**	**4**	**2**	**2**	**2**	**2**
Revisión Continua		**1**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Tabla 57. Diagrama de Pareto ISO/IEC 38500 e ISO/IEC 27014 - Disponibilidad

Elementos Norma ISO 38500:2015	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	MOGTI	51	7%	51	7%
Estrategia	PGTI_2	49	7%	100	14%
Desempeño	PGTI_4	48	7%	148	20%
Adquisición	PGTI_3	47	6%	195	27%
Comportamiento Humano	PGTI_6	47	6%	242	33%
Responsabilidad	PGTI_1	46	6%	288	40%
Conformidad	PGTI_5	46	6%	334	46%
Gobernar TI	*GoTI*	46	6%	380	52%
Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	OGTI_1	45	6%	425	59%
Establecer y sostener un entorno apto	*EA*	44	6%	469	65%
Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	OGTI_2	42	6%	511	70%
Monitorear	AGTI_3	42	6%	553	76%
Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	OGTI_4	39	5%	592	82%
Dirigir	AGTI_2	38	5%	630	87%
Evaluar	AGTI_1	35	5%	665	92%
Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	OGTI_3	31	4%	696	96%
Revisión Continua	*RC*	30	4%	726	100%

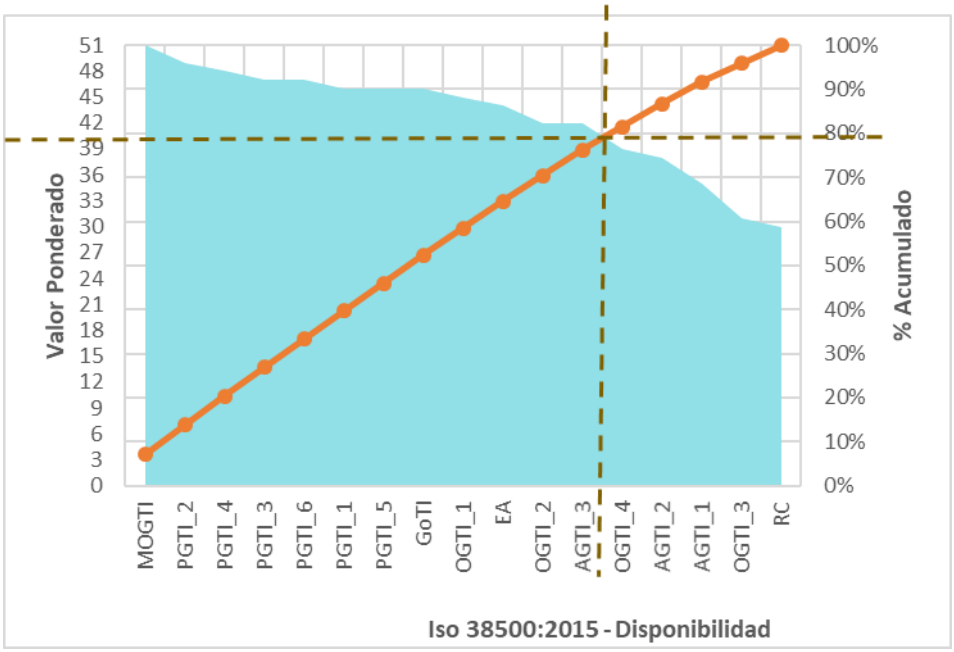

Gráfico 44. Diagrama de Pareto ISO/IEC 38500:2015 - Disponibilidad

La norma ISO 27014:2013 determina que evaluar, dirigir y monitorear agregará valor al tablero de directores y al de las partes interesadas, lo que asegura que la información en base a los riesgos está siendo adecuadamente tratada. Se debe asegurar así, la integridad de la información al alinear las estrategias y objetivos de seguridad de la información con las estrategias y objetivos del negocio por medio de una comunicación eficiente. Estos elementos se marcan como los de mayor importancia relativa, como se puede apreciar en la Tabla 58 y el Gráfico 45.

Tabla 58. Diagrama de Pareto ISO/IEC 27014 - Disponibilidad

Elementos Norma ISO 27014:2013	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Evaluar	AGoSI_1	59	8%	59	8%
Dirigir	AGoSI_2	58	8%	117	16%
Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	OGoSI_1	55	8%	172	24%
Monitorear	AGoSI_3	55	8%	227	31%
Agregar valor al tablero. de directores y partes interesadas	OGoSI_2	52	7%	279	38%
Asegurar que la información los riesgos están siendo adecuadamente tratado	OGoSI_3	49	7%	328	45%
Asegurar	AGoSI_5	49	7%	377	52%
Comunicar	AGoSI_4	48	7%	425	59%
Desempeño de la opinión en relación a los resultados de negocio	PGoSI_6	48	7%	473	65%
Establecer la seguridad de la Información en toda la organización	PGoSI_1	46	6%	519	71%
Establecer la dirección de las decisiones de inversión	PGoSI_3	44	6%	563	78%
Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	MOGoTI	43	6%	606	83%
Adoptar un enfoque basado en riesgos	PGoSI_2	43	6%	649	89%
Asegurar la conformidad con los requisitos internos y externos	PGoSI_4	41	6%	690	95%
Fomentar un entorno de seguridad positiva	PGoSI_5	36	5%	726	100%

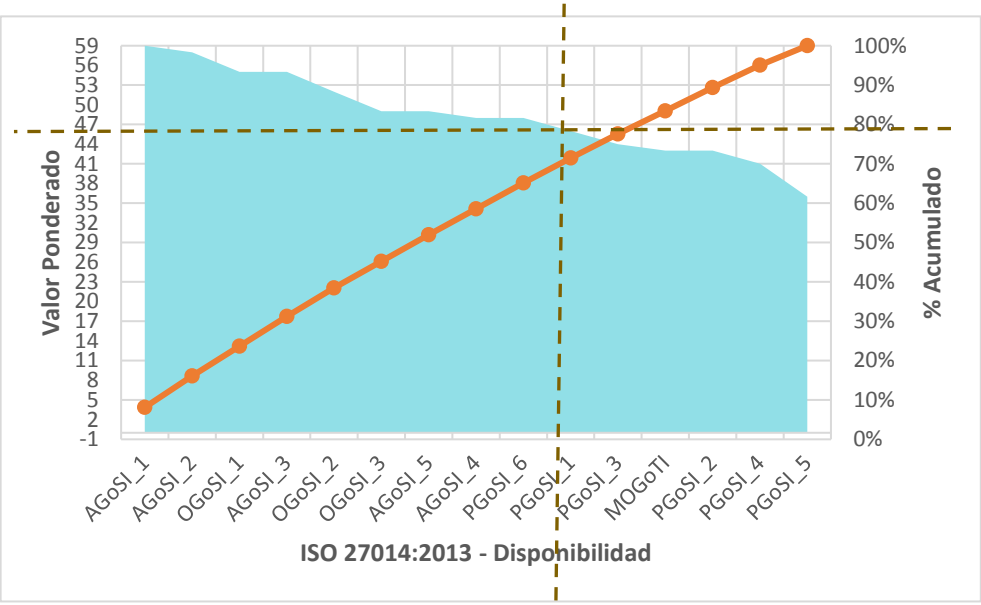

Gráfico 45. Diagrama de Pareto ISO/IEC 27014:2013 - Disponibilidad

Criterio Alineamiento Estratégico

El alineamiento estratégico es uno de los criterios más importantes para establecer un modelo de seguridad de la información, las estrategias que se establezcan entre el gobierno de TI y el de seguridad permitirá asegurar un sistema de gobierno que gestione la seguridad desde el gobierno corporativo basados en un análisis de riesgos sobre los activos de información.

Este alineamiento estratégico permitirá monitorear los activos de información y a través de ello medir el desempeño de las obligaciones que tiene los departamentos o áreas de TI sobre los servicios que prestan en la organización. el equilibrio que se logre fomentará las oportunidades y establecerá un ambiente de seguridad que permita el cumplimiento de las estrategias institucionales, así como sus principios y valores. (ver Tabla 59, Tabla 60 y Gráfico 46).

Tabla 59. Comparativo ISO/IEC 38500 e ISO/IEC 27014 - Alineamiento Estratégico

		ISO/IEC 27014:2013															
		Modelo	**Objetivos**			**Actividades**					**Principios**						
ISO/IEC 38500:2015		Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	Agregar valor al tablero. de directores y partes	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de negocio	
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**4**	**4**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**3**	**2**	**4**	
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**4**	**3**	**4**	**3**	**4**	**4**	**4**	**1**	**3**	**3**	**2**	**3**	**3**	**2**	**4**	
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**4**	**3**	**2**	**3**	**2**	
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**1**	**1**	**1**	**1**	**1**	
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	**1**	**4**	**3**	**2**	**1**	**1**	**1**	**3**	**3**	**4**	**3**	**4**	**3**	**3**	**4**	
Actividades	*Evaluar*	**4**	**2**	**2**	**3**	**4**	**2**	**3**	**3**	**2**	**1**	**2**	**1**	**2**	**1**	**4**	
	Dirigir	**4**	**3**	**3**	**1**	**3**	**4**	**3**	**3**	**3**	**4**	**1**	**3**	**3**	**1**	**1**	
	Monitorear	**3**	**3**	**4**	**4**	**3**	**3**	**4**	**2**	**3**	**2**	**4**	**3**	**2**	**2**	**1**	
Principios	**Responsabilidad**	**1**	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**	
	Estrategia	**3**	**3**	**4**	**3**	**4**	**4**	**4**	**3**	**4**	**3**	**3**	**3**	**3**	**3**	**2**	
	Adquisición	**3**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**2**	**3**	**4**	**3**	**3**	**2**	
	Desempeño	**2**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**2**	**3**	**4**	**3**	**3**	
	Conformidad	**3**	**4**	**4**	**3**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	
	Comportamiento Humano	**2**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**	
ISO/IEC 38501:2015																	
Establecer y sostener un entorno apto		**3**	**1**	**4**	**3**	**4**	**4**	**2**	**4**	**4**	**4**	**3**	**3**	**1**	**1**	**4**	
Gobernar TI		**4**	**4**	**2**	**4**	**3**	**3**	**3**	**4**	**4**	**3**	**4**	**2**	**2**	**2**	**2**	
Revisión Continua		**1**	**3**	**3**	**3**	**4**	**4**	**4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	

Tabla 60. Diagrama de Pareto ISO/IEC 38500 - Alineamiento Estratégico

Elementos Norma ISO 38500:2015	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Sistema de dos niveles (organismo de gestión y gobierno corporativo)	*MOGTI*	*52*	*7%*	*52*	*7%*
Desempeño	*PGTI_4*	*51*	*7%*	*103*	*13%*
Responsabilidad	*PGTI_1*	*50*	*7%*	*153*	*20%*
Estrategia	*PGTI_2*	*49*	*6%*	*202*	*26%*
Adquisición	*PGTI_3*	*49*	*6%*	*251*	*33%*
Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	*OGTI_2*	*48*	*6%*	*299*	*39%*
Conformidad	*PGTI_5*	*48*	*6%*	*347*	*45%*
Comportamiento Humano	*PGTI_6*	*48*	*6%*	*395*	*52%*
Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	*OGTI_1*	*47*	*6%*	*442*	*58%*
Gobernar TI	*GoTI*	*46*	*6%*	*488*	*64%*
Establecer y sostener un entorno apto	*EA*	*45*	*6%*	*533*	*70%*
Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	*OGTI_3*	*43*	*6%*	*576*	*75%*
Monitorear	*AGTI_3*	*43*	*6%*	*619*	*81%*
Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	*OGTI_4*	*40*	*5%*	*659*	*86%*
Dirigir	*AGTI_2*	*40*	*5%*	*699*	*91%*
Evaluar	*AGTI_1*	*36*	*5%*	*735*	*96%*
Revisión Continua	*RC*	*30*	*4%*	*765*	*100%*

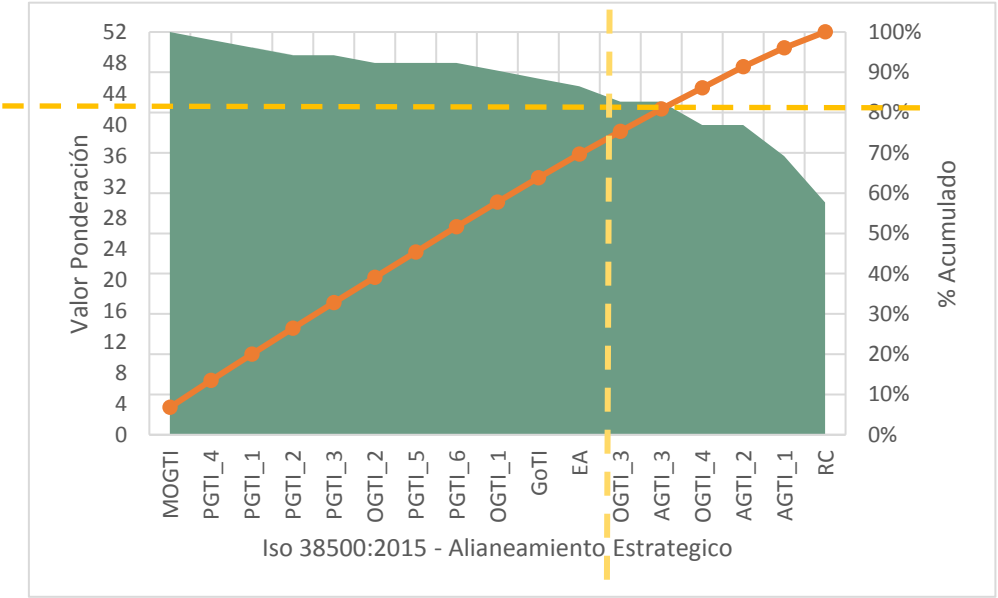

Gráfico 46. Diagrama de Pareto ISO/IEC 38500:2015 – Alineamiento Estratégico

En el alineamiento estratégico visto desde el enfoque de la norma ISO 27014:2013 permitió identificar elementos superpuestos y proporcionar cierta coordinación a través de un modelo de gobierno de seguridad con el gobierno de TI. Esta coordinación establece un proceso de dirección, evaluación y monitorización de los activos de información en base al análisis de riesgos para asegurar la integridad de la información mediante las estrategias y objetivos de seguridad de la información que permiten lograr que las estrategias y objetivos organizacionales se cumplan y permitan establecer un conjunto de políticas y métricas que deben ser comunicados eficientemente a todos los miembros de la organización (ver Tabla 61 y Gráfico 47).

Tabla 61. Diagrama de Pareto ISO/IEC 27014 - Alineamiento Estratégico

Elementos Norma ISO 27014:2013	Nomenclatura	Valor Ponderación	%	Valor Acumulado	% Acumulado
Evaluar	*AGoSI_1*	*62*	*8%*	*62*	*8%*
Dirigir	*AGoSI_2*	*61*	*8%*	*123*	*16%*
Monitorear	*AGoSI_3*	*60*	*8%*	*183*	*24%*
Agregar valor al tablero. de directores y partes interesadas	*OGoSI_2*	*58*	*8%*	*241*	*32%*
Asegurar	*AGoSI_5*	*56*	*7%*	*297*	*39%*
Asegurar que la información los riesgos están siendo adecuadamente tratado	*OGoSI_3*	*55*	*7%*	*352*	*46%*
Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	*OGoSI_1*	*54*	*7%*	*406*	*53%*
Comunicar	*AGoSI_4*	*53*	*7%*	*459*	*60%*
Establecer la seguridad de la Información en toda la organización	*PGoSI_1*	*49*	*6%*	*508*	*66%*
Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	*MOGoTI*	*48*	*6%*	*556*	*73%*
Establecer la dirección de las decisiones de inversión	*PGoSI_3*	*45*	*6%*	*601*	*79%*
Desempeño de la opinión en relación a los resultados de negocio	*PGoSI_6*	*44*	*6%*	*645*	*84%*
Adoptar un enfoque basado en riesgos	*PGoSI_2*	*43*	*6%*	*688*	*90%*
Asegurar la conformidad con los requisitos internos y externos	*PGoSI_4*	*41*	*5%*	*729*	*95%*
Fomentar un entorno de seguridad positiva	*PGoSI_5*	*36*	*5%*	*765*	*100%*

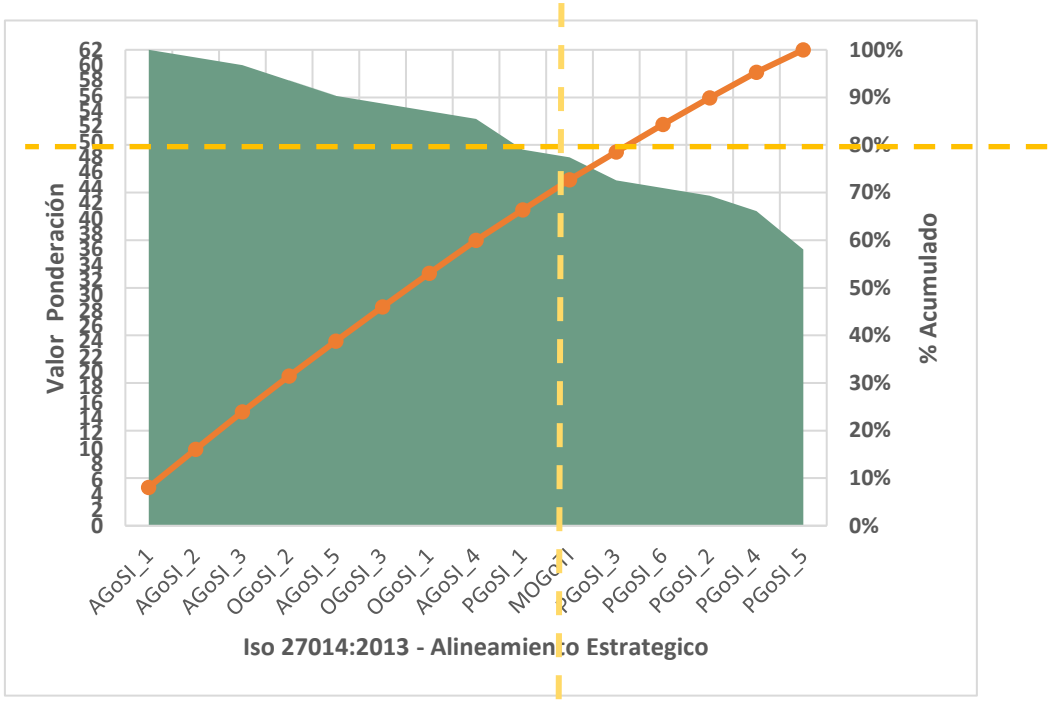

Gráfico 47. Diagrama de Pareto ISO/IEC 27014:2013 – Alineamiento Estratégico

6.8 Interpretación de datos

Para lograr un mapeo de integración entre la ISO 38500:2015 e ISO 27014:2013 y en concordancia con los resultados anteriores por cada uno de sus elementos se establece una matriz de mapeo consolidada que permite ver la relación que existe en base a los criterios seleccionados y las ponderaciones establecidas.

En la Tabla 63 se muestra la integración de los cuatro criterios con el único objetivo de poder determinar si existe una fuerte, mediana, poca o ninguna relación entre las actividades, principios y modelo de las normas.

El establecimiento de la relación se trabajó con una escala de fuerte, ninguna, poca, ninguna importancia de un elemento de la norma ISO 38500:2015 e ISO 27014:2013, las demás combinaciones son valores intermedios que para efectos del análisis no se consideraron.

Tabla 62. Escala de relación entre ISO 38500:2015 e ISO 27014:2013

Escala Difusa	Representación	Escala Verbal
(4,4,4,4)	FR	Fuerte importancia de un elemento sobre el otro
(3,3,3,3)	MR	Moderada importancia de un elemento sobre el otro
(2,2,2,2)	PR	Poca importancia de un elemento sobre el otro
(1,1,1,1)	NR	Ninguna importancia de un elemento sobre el otro

Los resultados de la integración se pueden observar en la Tabla 63.

Tabla 63. Relación ISO 38500:2015 e ISO 27014:2013

		ISO/IEC 27014:2013														
		Modelo	**Objetivos**			**Actividades**								**Principios**		
ISO/IEC 38500:2015		Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y	Agregar valor al tablero, de directores y partes interesadas	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de negocio
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**(4,4,4,4)**	**(3,3,3,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(2,2,2,2)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,2,2)**	**(4,4,4,4)**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**(4,4,4,4)**	**(4,3,4,3)**	**(2,3,2,4)**	**(4,3,4,3)**	**(3,4,3,4)**	**(3,4,3,4)**	**(3,4,3,4)**	**(3,1,3,1)**	**(3,3,3,3)**	**(2,2,2,3)**	**(2,2,2,2)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,2,2)**	**(4,4,4,4)**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**(2,2,2,2)**	**(3,3,3,3)**	**(4,4,1,4)**	**(4,4,1,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(3,3,3,3)**	**(2,2,3,2)**	**(3,3,2,3)**	**(2,2,2,2)**
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(2,4,2,4)**	**(2,4.2,4)**	**(2,4,2,4)**	**(2,4,2,4)**	**(2,4,2,4)**	**(2,4,2,4)**	**(3,3,3,3)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización	**(1,1,1,1)**	**(4,4,4,4)**	**(3,3,3,3)**	**(2,2,1,2)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**
Actividades	*Evaluar*	**(4,4,4,4)**	**(2,2,2,2)**	**(2,2,2,2)**	**(3,3,4,3)**	**(4,4,4,4)**	**(2,2,2,2)**	**(2,2,2,3)**	**(2,2,2,3)**	**(2,2,2,2)**	**(1,1,1,1)**	**(2,2,2,2)**	**(1,1,1,1)**	**(2,2,2,2)**	**(1,1,1,1)**	**(4,4,4,4)**
	Dirigir	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(1,1,1,1)**	**(3,3,3,3)**	**(4,4,4,4)**	**(2,2,2,3)**	**(2,2,2,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(1,1,1,1)**	**(3,3,3,3)**	**(3,3,3,3)**	**(1,1,1,1)**	**(1,1,1,1)**
	Monitorear	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(2,2,2,2)**	**(2,2,2,3)**	**(2,2,2,2)**	**(4,4,4,4)**	**(3,3,3,3)**	**(2,2.2,2)**	**(2,2,2,2)**	**(1,1,1,1)**
Principios	**Responsabilidad**	**(1,1,1,1)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,4,2,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,4,3,4)**	**(3,4,3,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**
	Estrategia	**(3,3,2,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,4,3,4)**	**(3,3,2,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,4,2)**
	Adquisición	**(3,3,2,3)**	**(2,2,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,4,3,4)**	**(3,4,3,4)**	**(2,2,2,2)**	**(3,3,3,3)**	**(3,3,3,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,4,2)**
	Desempeño	**(2,2,2,2)**	**(3,3,3,3)**	**(3,4,3,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,4,3,4)**	**(3,4,3,4)**	**(3,3,3,3)**	**(2,2,2,2)**	**(3,3,3,3)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**
	Conformidad	**(2,2,1,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,2,2)**	**(2,2,2,2)**	**(3,3,3,3)**	**(3,3,3,3)**
	Comportamiento Humano	**(2,2,1,2)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,2)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,2,2)**	**(3,3,3,3)**	**(3,3,3,3)**	**(2,2,2,2)**	**(3,3,3,3)**
ISO/IEC 38501:2015																
Establecer y sostener un entorno apto		**(3,3,3,3)**	**(1,1,2,1)**	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(2,2,2,2)**	**(4,4,4,4)**	**(4,4,4,4)**	**(2,4,2,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(1,1,1,1)**	**(1,1,1,1)**	**(4,4,4,4)**
Gobernar TI		**(4,4,4,4)**	**(4,4,4,4)**	**(2,2,2,2)**	**(4,4,4,4)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(3,3,3,3)**	**(4,4,4,4)**	**(2,2,2,2)**	**(2,2,2,2)**	**(2,2,2,2)**	**(2,2,2,2)**
Revisión Continua		**(1,1,1,1)**	**(3,3,3,3)**	**(3,3,3,3)**	**(3,3,3,3)**	**(4,4,4,4)**	**(4,4,4,4)**	**(4,4,4,4)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**	**(1,1,1,1)**

Aplicando la representación de la escala para medir el grado de relación entre las dos normas se obtuvo los resultados presentados en la Tabla 64.

Tabla 64. Armonización entre ISO 38500:2015 e ISO 27014:2013

		ISO/IEC 27014:2013														
		Modelo	**Objetivos**			**Actividades**					**Principios**					
	ISO/IEC 38500:2015	Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios	Agregar valor al tablero. de directores y partes interesadas	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la organización	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de negocio
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**FR**		**MR**	**MR**	**FR**	**FR**	**FR**	**FR**	**FR**	**FR**	**PR**	**MR**	**MR**	**PR**	**FR**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**FR**								**MR**		**PR**	**MR**	**MR**	**PR**	**FR**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones	**PR**	**MR**			**FR**	**FR**	**FR**	**MR**	**MR**	**MR**	**FR**	**MR**			**PR**
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**FR**	**MR**	**FR**							**MR**					
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización		**FR**	**MR**					**MR**	**MR**	**FR**	**MR**	**FR**	**MR**	**MR**	**FR**
Actividades	*Evaluar*	**FR**	**PR**	**PR**		**FR**	**PR**			**PR**		**PR**		**PR**		**FR**
	Dirigir	**FR**	**MR**	**MR**		**MR**	**FR**			**MR**	**FR**		**MR**	**MR**		
	Monitorear	**MR**	**MR**	**FR**	**FR**	**MR**	**MR**	**FR**	**PR**		**PR**	**FR**	**MR**		**PR**	
Principios	**Responsabilidad**		**FR**	**MR**		**FR**	**FR**	**FR**			**MR**	**MR**	**MR**	**MR**	**MR**	**MR**
	Estrategia		**MR**	**FR**	**MR**	**FR**	**FR**	**FR**	**MR**			**MR**	**MR**	**MR**	**MR**	
	Adquisición			**MR**	**MR**	**FR**	**FR**	**FR**			**PR**	**MR**		**MR**	**MR**	
	Desempeño	**PR**	**MR**		**FR**	**FR**	**FR**	**FR**			**MR**	**PR**	**MR**	**FR**	**MR**	**MR**
	Conformidad		**FR**	**FR**	**MR**	**FR**	**FR**	**FR**	**MR**	**MR**	**MR**	**MR**	**PR**	**PR**	**MR**	**MR**
	Comportamiento Humano		**FR**	**FR**	**FR**	**FR**	**FR**	**FR**		**MR**	**MR**	**PR**	**MR**	**MR**	**PR**	**MR**
	ISO/IEC 38501:2015															
Establecer y sostener un entorno apto		**MR**		**FR**	**MR**	**FR**	**FR**	**PR**	**FR**	**FR**		**MR**	**MR**			**FR**
Gobernar TI		**FR**	**FR**	**PR**	**FR**	**MR**	**MR**	**MR**	**FR**	**FR**	**MR**	**FR**	**PR**	**PR**	**PR**	**PR**
Revisión Continua			**MR**	**MR**	**MR**	**FR**	**FR**	**FR**								

Para objeto del análisis se tomó en consideración solo aquellos resultados que están fuerte y moderadamente relacionados. La norma ISO 27014:2013 con la norma ISO 38500:2015 están fuerte y moderadamente relacionados lo que permite establecer que el Gobierno de Seguridad de la Información no está separado del Gobierno de TI, con una fuerte relación entre los dos en el ámbito de sus actividades de dirección, evaluación y monitorización como se observa en la Tabla 65.

Tabla 65. ISO 27014:2013 relacionado con ISO 38500:2015

		ISO/IEC 27014:2013															
		Modelo	**Objetivos**				**Actividades**					**Principios**					
	ISO/IEC 38500:2015	Sistema de dos niveles (Ejecutivo gestión y gobierno corporativo)	Proporcionar alineación entre la información objetivos de seguridad y estrategias y negocios objetivos y estrategias	Agregar valor al tablero. de directores y partes interesadas	Asegurar que la información los riesgos están siendo adecuadamente tratado	*Evaluar*	*Dirigir*	*Monitorear*	*Comunicar*	*Asegurar*	Establecer la seguridad de la Información en toda la	Adoptar un enfoque basado en riesgos	Establecer la dirección de las decisiones de inversión	Asegurar la conformidad con los requisitos internos y externos	Fomentar un entorno de seguridad positiva	Desempeño de la opinión en relación a los resultados de
Modelo	Sistema de dos niveles (organismo de gestión y **gobierno corporativo**)	**FR**		**MR**	**MR**	**FR**	**FR**	**FR**	**FR**	**FR**	**FR**		**MR**	**MR**		**FR**
Objetivos	Equilibrar los riesgos y fomentar las oportunidades derivadas del uso de TI.	**FR**								**MR**			**MR**	**MR**		**FR**
	Mitigar el riesgo de los directores no cumpliendo con sus obligaciones		**MR**			**FR**	**FR**	**FR**	**MR**	**MR**	**MR**	**FR**	**MR**			
	Asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI.	**FR**	**MR**	**FR**							**MR**					
	Asegurar que el uso de TI contribuya positivamente al desempeño de la organización		**FR**	**MR**					**MR**	**MR**	**FR**	**MR**	**FR**	**MR**	**MR**	**FR**
Actividades	*Evaluar*	**FR**				**FR**										**FR**
	Dirigir	**FR**	**MR**	**MR**		**MR**	**FR**			**MR**	**FR**		**MR**	**MR**		
	Monitorear	**MR**	**MR**	**FR**	**FR**	**MR**	**MR**	**FR**				**FR**	**MR**			
Principios	**Responsabilidad**		**FR**	**MR**		**FR**	**FR**	**FR**			**MR**	**MR**	**MR**	**MR**	**MR**	**MR**
	Estrategia		**MR**	**FR**	**MR**	**FR**	**FR**	**FR**	**MR**			**MR**	**MR**	**MR**	**MR**	
	Adquisición			**MR**	**MR**	**FR**	**FR**	**FR**				**MR**		**MR**	**MR**	
	Desempeño		**MR**		**FR**	**FR**	**FR**	**FR**			**MR**		**MR**	**FR**	**MR**	**MR**
	Conformidad		**FR**	**FR**	**MR**	**FR**	**FR**	**FR**	**MR**	**MR**	**MR**	**MR**			**MR**	**MR**
	Comportamiento Humano		**FR**	**FR**	**FR**	**FR**	**FR**	**FR**		**MR**	**MR**		**MR**	**MR**		**MR**
	ISO/IEC 38501:2015															
Establecer y sostener un entorno apto		**MR**		**FR**	**MR**	**FR**	**FR**		**FR**	**FR**		**MR**	**MR**			**FR**
Gobernar TI		**FR**	**FR**		**FR**	**MR**	**MR**	**MR**	**FR**	**FR**	**MR**	**FR**				
Revisión Continua			**MR**	**MR**	**MR**	**FR**	**FR**	**FR**								

6.8.1 Resultados de la armonización

A. Modelo

La norma ISO 27014:2013 con las de la norma ISO/IEC 38500:2015 muestra una fuerte relación entre los dos modelos desde el punto de vista seccional: gestión y gobierno. Además, comparten una fuerte relación con las actividades y elementos.

También se puede observar que el modelo ISO 27014:2013 está fuertemente relacionado con el equilibrio de los riesgos y en el fomento de las oportunidades derivadas de TI en el cumplimiento de las obligaciones del uso aceptable de las TI y las propiedades de gobierno que corresponden a la norma ISO/IEC 38501:2015.

Por otro lado, el establecimiento de políticas de seguridad de la información permitirá medir correctamente el desempeño en relación a los resultados del negocio.

B. Principios

Al momento de realizar el mapeo de ambas normas, nos encontramos que la norma ISO 27014:2013 tiene una fuerte relación con cinco de los seis principios de la norma ISO 38500:2015: responsabilidad, estrategia, desempeño, conformidad y comportamiento humano que permiten establecer la seguridad de la Información en toda la organización adoptando un enfoque basado en riesgos para medir el desempeño en relación a los resultados de negocio.

Finalmente, los principios de responsabilidad, estrategia, desempeño, comportamiento humano, conformidad, desempeño y análisis de riesgos están fuertemente relacionados en las dos normas. Cada uno de ellos con sus descripciones y conceptualizaciones que permiten describir las actividades relacionadas con la seguridad, integridad y confiabilidad de la información.

C. Actividades

Con respecto las actividades de evaluar, dirigir, monitorear, comunicar y asegurar de la norma ISO/IEC 27014:2013 se encuentra fuertemente relacionadas con el modelo de gobierno de TI (organizamos de gestión y gobierno corporativo), además tres de ellas (evaluar, dirigir, monitorear) está fuertemente relacionado con el objetivo de la norma ISO/IEC 38500:2015 mitigación de riesgo de los directores al no cumplimiento de sus obligaciones.

Por otra parte, se observa una relación entre moderada y fuertemente con los con los seis principios del modelo de gobierno de la norma ISO/IEC 38500:2015, de manera directa con responsabilidad, estrategia, comportamiento humano, conformidad, desempeño.

D. Objetivos

El objetivo agregar valor al tablero de directores y partes interesadas, proporcionar alineación entre la información objetivos de seguridad, estrategias y negocios de la ISO/IEC 27014:2013, está fuertemente relacionado con el objetivo de asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI, asegurar que el uso de TI contribuya positivamente al desempeño de la organización de la norma ISO/IEC 38500:2015.

Además, se establece una relación moderada al proporcionar una alineación entre la información y objetivos de seguridad con la mitigación de los riesgos que tienen los directores al no cumpliendo con sus obligaciones y el asegurar el cumplimiento de las obligaciones relativas al uso aceptable de TI a nivel de integridad, confiabilidad y disponibilidad de la información dentro de la organización.

6.8.2 Modelo de Gobierno de Seguridad de la Información para IES

Como resultado de los análisis realizados en el apartado anterior se establece la estructura del Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior (MoGSIIES) basado en los elementos que aportan las normas relacionadas.

El modelo está dividido en tres niveles: principios, objetivos e indicadores de madurez, de gobernabilidad y cuantitativos; los cuales deberán ser evaluados (Evaluar), dirigidos (Dirigir), monitoreados (Monitorear), comunicados (Comunicar) y Asegurar (Ver Gráfico 18).

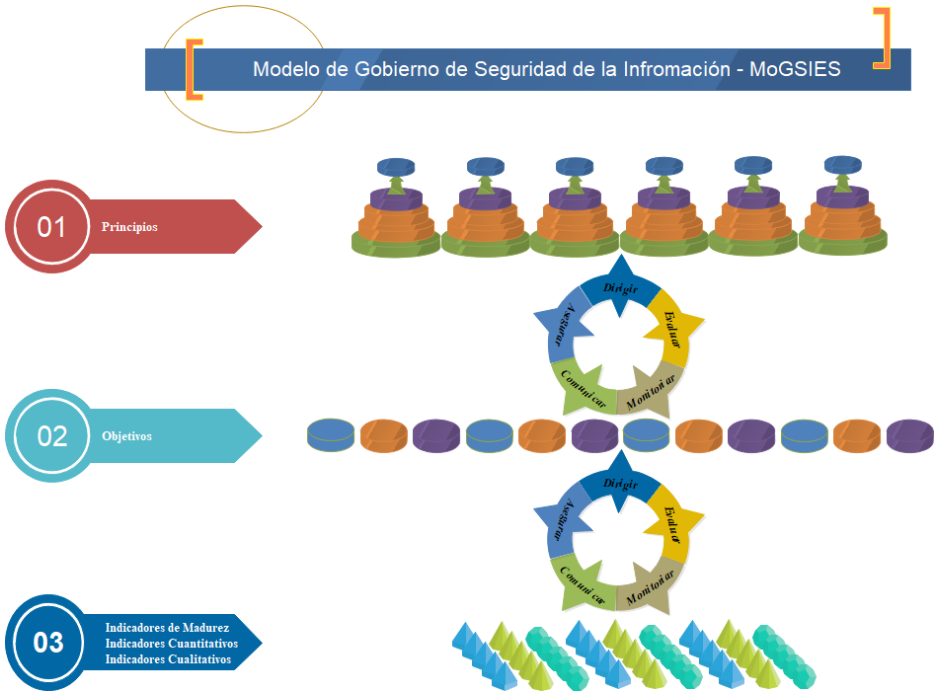

Gráfico 48. Modelo de Gobierno de Seguridad de la Información para IES (MoGSIIES).

El modelo propuesto establece que los responsables de las IES deben gobernar la seguridad de la información en cinco acciones:

Evaluar las estrategias, principios y acciones que las IES deben tomar en cuenta

sobre el gobierno de seguridad de la información, los directivos deberán examinar y tomar las decisiones sobre el estado actual y fututo de la seguridad de la información. La evaluación deberá ser continua y tomar en cuenta las necesidades presentes y futuras para lograr los niveles de seguridad de la información y así mantener la ventaja competitiva y alcanzar los objetivos estratégicos organizacionales y de TI.

Dirigir está enfocado a la preparación y a la implementación de los planes y políticas que permitan garantizar la seguridad de la información de los activos de la IES, así como, a la garantizar la ejecución de las estrategias y acciones planificadas, las acciones tomadas deberán garantizar la integridad, confiabilidad de la información de las operaciones de la IES.

Las políticas deberán garantizar los niveles de seguridad de la información según los planes establecidos considerando el impacto en las estrategias, proceso y procedimientos organizacionales de las IES. También deben promover una cultura del gobierno de seguridad de la información requiriendo de los directores de TI informes periódicos y sobre todo pidiendo respeto a los principios del MoGSIIES.

Monitorear mediante un sistema de medida, las políticas, procedimientos y planes de seguridad de la información se deberá controlar su rendimiento a través de un seguimiento y monitorización de los indicadores de seguridad establecidos.

Comunicar es el proceso de gobierno bidireccional mediante el cual el cuerpo directivo de la IES y las partes interesadas intercambian información sobre seguridad de la información adecuada a sus necesidades específicas. Es importante que se genere una cultura de comunicación en todo momento para de esta forma evitar que se distorsione la ejecución de las políticas, proceso y procedimientos de seguridad de la información por parte de todos los involucrados

Asegurar es el proceso de gobierno mediante el cual se audita, revisa o certifica las actividades de gobierno y operativas con el fin de alcanzar el nivel deseado de seguridad de la información.

El MoGSIIES está estructurado de la manera siguiente:

Principios: ocupan el nivel superior del modelo y son:

- Responsabilidad (R).
- Desempeño (D).
- Comportamiento Humano (CH).
- Análisis de Riesgos (AR).
- Conformidad (C).
- Estrategia (E).

Objetivos: se encuentran en el nivel intermedio del modelo y se han diseñado en función de los resultados obtenidos en el mapeo y análisis realizado en el apartado anterior, y son:

1. La Institución de Educación Superior debe tener clara cuál es su estrategia de Seguridad de la Información para toda la organización.
2. Alinear la estrategia Institucional, TI con la Estrategia de Seguridad de la Información.
3. Disponer de una estructura de dirección y modelo de toma de decisiones alineaos a las estrategias de seguridad de la información.
4. Establecer políticas y procedimientos de alto nivel para gestionar la seguridad de la información considerando las normativas vigentes y los estándares internacionales.
5. Toma de decisiones debidamente argumentadas y efectivas en relación a la seguridad de la información.
6. Definir a arquitectura de seguridad de la información que incluya procesos y la integración con los sistemas.
7. Los niveles de seguridad de la información deben permitir garantizar la información de los servicios basados en TI.
8. Conocer y gestionar los riesgos asociados con la seguridad de la información
9. Disponer del personal adecuado y con la formación respectiva para ocuparse de la gestión eficiente de la seguridad de la información.
10. Integrar los valores organizacionales dentro de estrategias de Seguridad de la

Información.

11. Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.
12. Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos de TI y de Seguridad de la información de la IES.

Relación Principios y Objetivos: Una vez realizado el análisis de la relación que debe tener cada uno de los objetivos con los principios del MoGSIIES se logró establecer que objetivo son los que se trabajará con cada uno de los principios, es decir que cada principio puede ser alcanzado por la consecución de varios objetivos y que un objetivo puede contribuir para alcanzar varios objetivos como puede observarse en la Tabla 66.

Tabla 66. Relación Principios – Objetivos MoGSIIES

	R	D	CH	AR	C	E
La Institución de Educación Superior debe tener clara cuál es su estrategia de Seguridad de la Información para toda la organización.						X
Alinear la estrategia Institucional, TI con la Estrategia de Seguridad de la Información						X
Disponer de una estructura de dirección y modelo de toma de decisiones alineaos a las estrategias de seguridad de la información.	X					X
Establecer políticas y procedimientos de alto nivel para gestionar la seguridad de la información considerando las normativas vigentes y los estándares internacionales.	X				X	X
Toma de decisiones debidamente Argumentadas y efectivas en relación a la seguridad de la información	X				X	
Definir a arquitectura de seguridad de la información que incluya procesos y la integración con los sistemas		X		X		
Los niveles de seguridad de la información deben permitir garantizar la información de los servicios basados en TI.		X	X			
Conocer y gestionar los riesgos asociados con la seguridad de la información		X		X		
Disponer del personal adecuado y con la formación respectiva para ocuparse de la gestión eficiente de la seguridad de la información.			X			
Integrar los valores organizaciones dentro de las estrategias de Seguridad de la información			X	X	X	
Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.	X		X		X	
Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos, de TI y de Seguridad de la información de la IES		X		X		

Nota: R= Responsabilidad, D= Desempeño, CH = Comportamiento Humano, AR = Análisis de Riesgos, C = Conformidad, E = Estrategia.

Objetivos del Principio Responsabilidad

- Disponer de una estructura de dirección y modelo de toma de decisiones alineaos a las estrategias de seguridad de la información.
- Establecer políticas y procedimientos de alto nivel para gestionar la seguridad de la información considerando las normativas vigentes y los estándares internacionales.
- Toma de decisiones debidamente Argumentadas y efectivas en relación a la seguridad de la información
- Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.

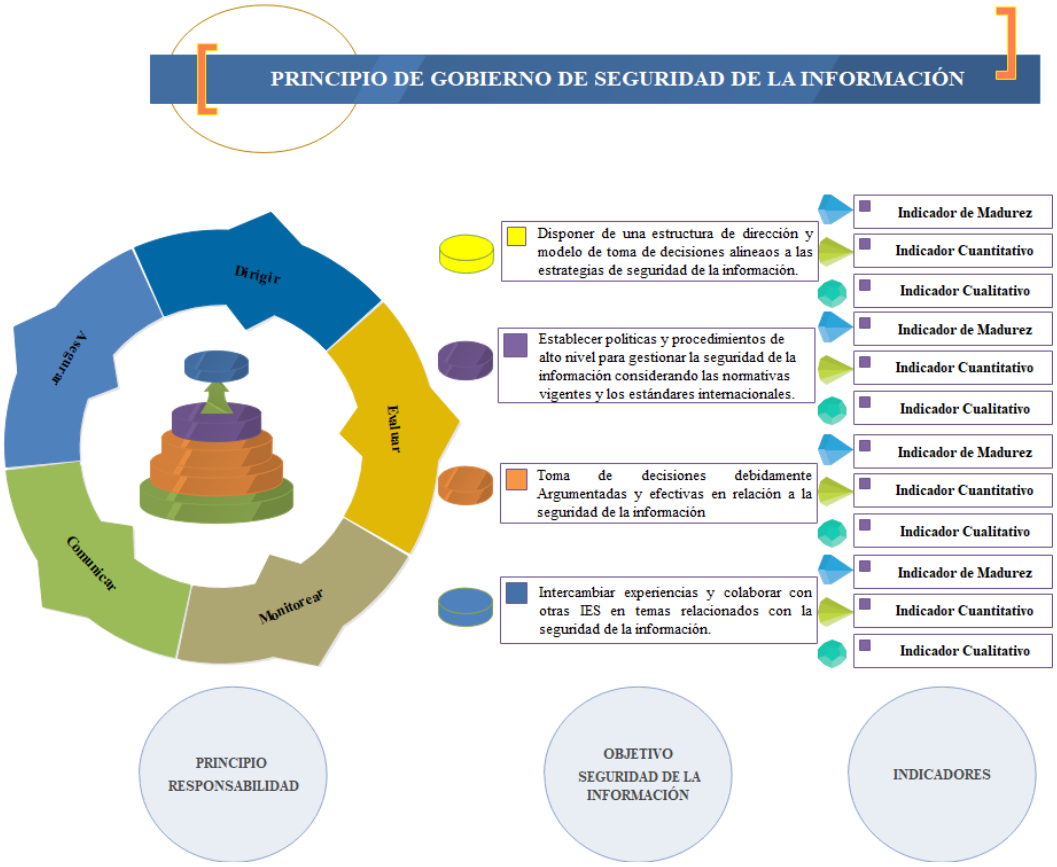

Gráfico 49. MoGSIIES.- Principio Responsabilidad

Objetivos del Principio Desempeño

- Definir a arquitectura de seguridad de la información que incluya procesos y la integración con los sistemas
- Los niveles de seguridad de la información deben permitir garantizar la información de los servicios basados en TI.
- Conocer y gestionar los riesgos asociados con la seguridad de la información
- Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos, de TI y de Seguridad de la información de la IES

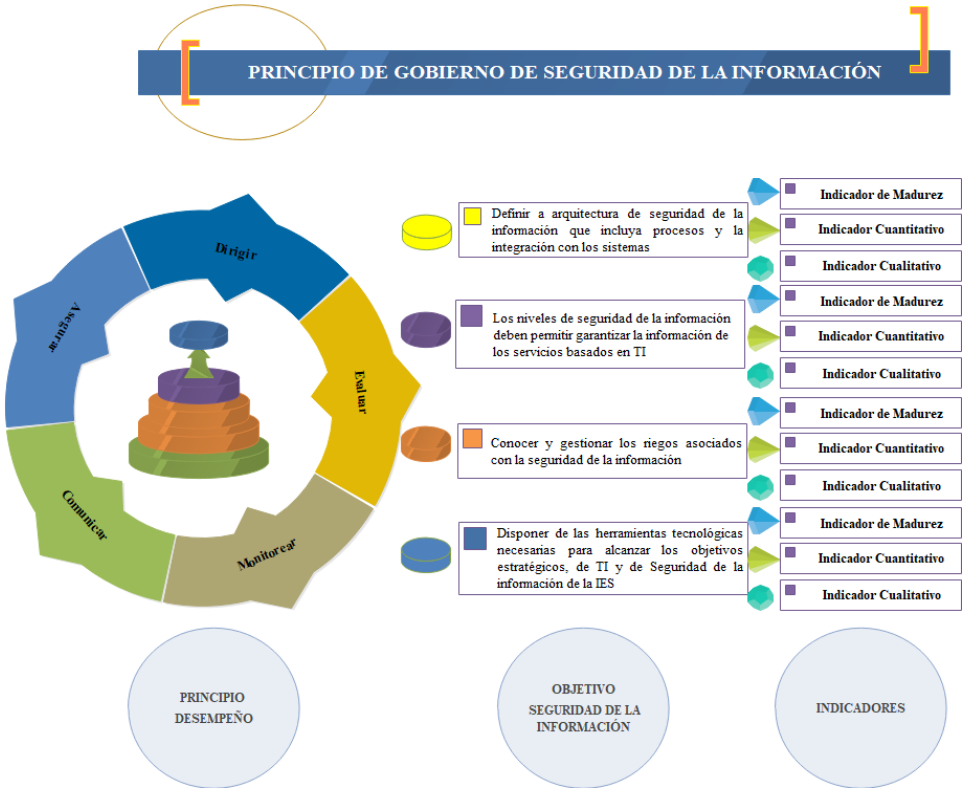

Gráfico 50. MoGSIIES.- Principio Desempeño

Objetivos del Principio Comportamiento Humano

- Los niveles de seguridad de la información deben permitir garantizar la información de los servicios basados en TI.
- Disponer del personal adecuado y con la formación respectiva para ocuparse de la gestión eficiente de la seguridad de la información.
    - Integrar los valores organizaciones dentro de las estrategias de Seguridad de la información
    - Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.

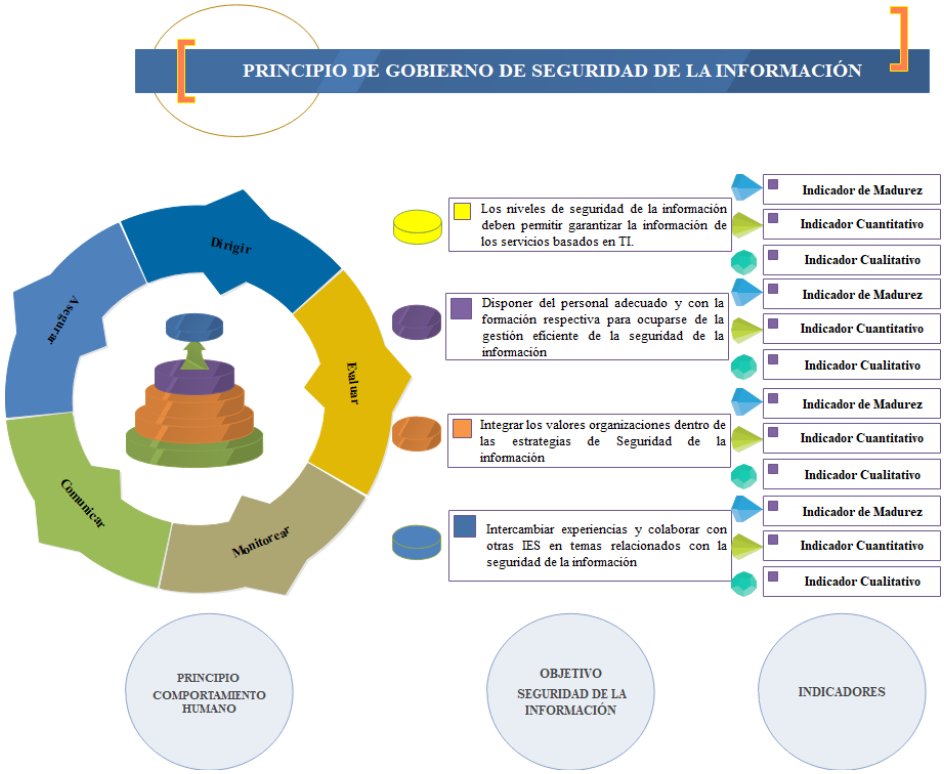

Gráfico 51. MoGSIIES.- Principio Comportamiento Humano

Objetivos del Principio Análisis de Riesgos

- Definir a arquitectura de seguridad de la información que incluya procesos y la integración con los sistemas
- Conocer y gestionar los riesgos asociados con la seguridad de la información
- Integrar los valores organizaciones dentro de las estrategias de Seguridad de la información
- Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos, de TI y de Seguridad de la información de la IES

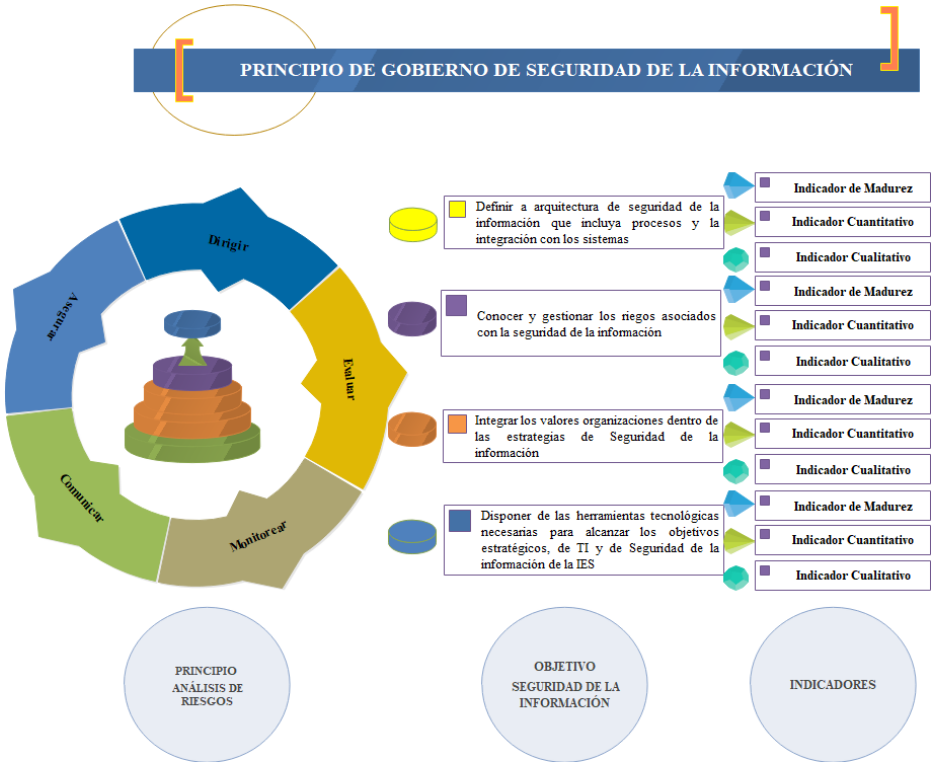

Gráfico 52. MoGSIIES.- Principio Análisis de Riesgos

Objetivos del Principio Conformidad

- Establecer políticas y procedimientos de alto nivel para gestionar la seguridad de la información considerando las normativas vigentes y los estándares internacionales.
- Toma de decisiones debidamente Argumentadas y efectivas en relación a la seguridad de la información.
- Integrar los valores organizaciones dentro de las estrategias de Seguridad de la información.
- Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.

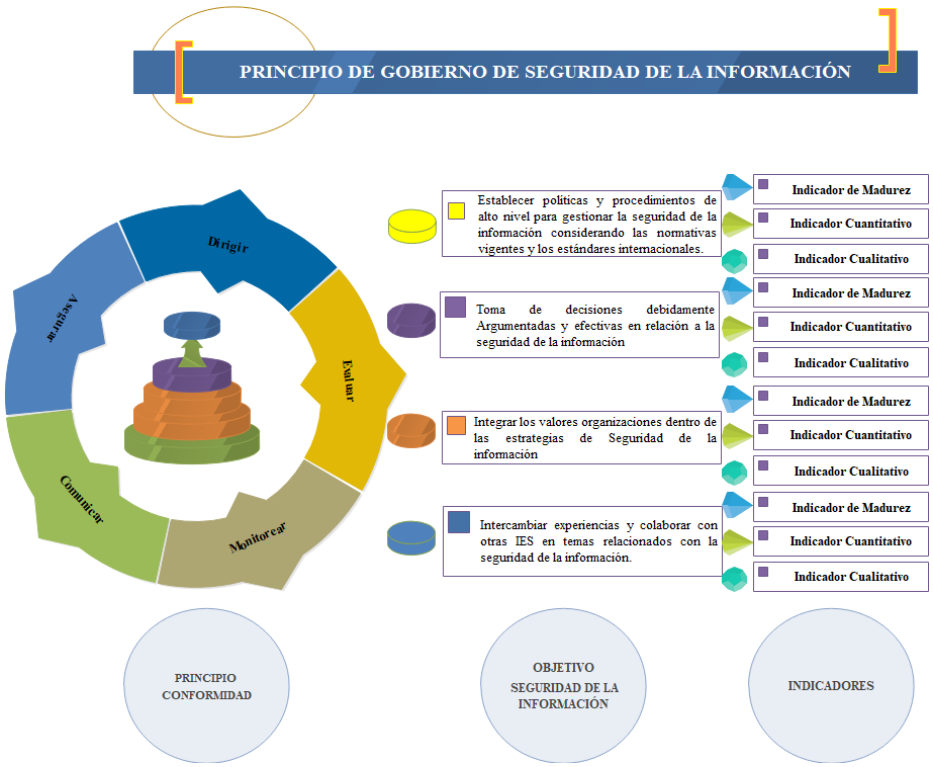

Gráfico 53. MoGSIIES.- Principio Conformidad

Objetivos del Principio de Estrategia

- La Institución de educación Superior debe tener clara cuál es su estrategia de Seguridad de la Información para toda la organización.
- Alinear la estrategia Institucional, TI con la Estrategia de Seguridad de la Información
- Disponer de una estructura de dirección y modelo de toma de decisiones alineaos a las estrategias de seguridad de la información.
- Establecer políticas y procedimientos de alto nivel para gestionar la seguridad de la información considerando las normativas vigentes y los estándares internacionales.

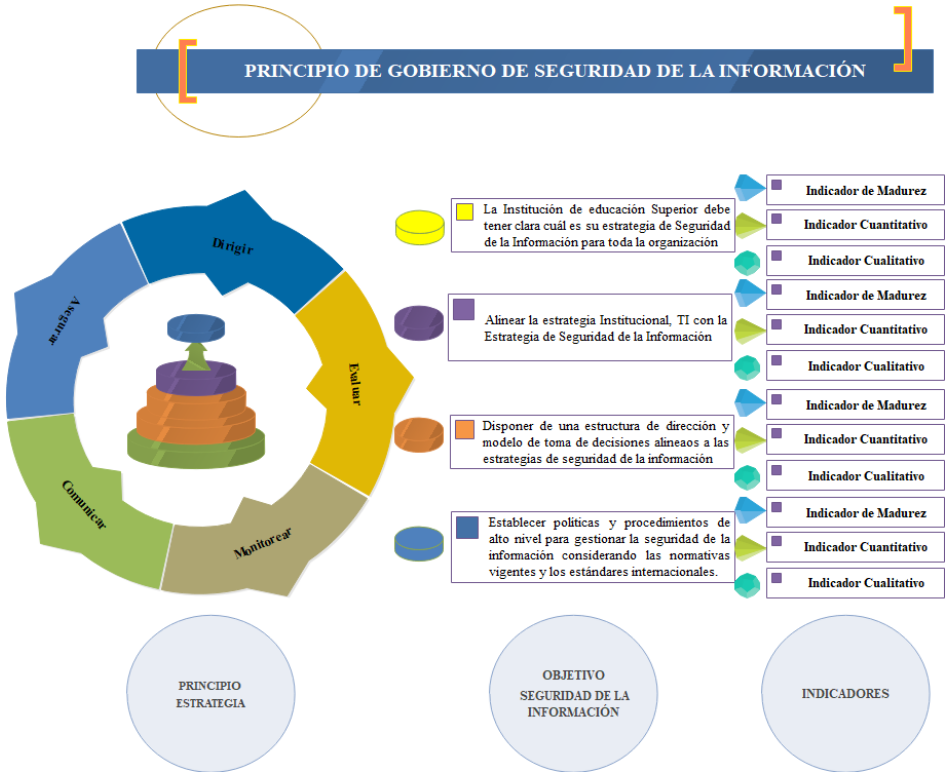

Gráfico 54. MoGSIIES.- Principio Estrategia

6.9 Validación del modelo de Gobierno de Seguridad de la Información.

6.9.1 Validación de expertos del Modelo Propuesto

Para la realizar la validación del modelo de gobierno de seguridad de la información para instituciones de educación superior (véase Anexo 2) se utilizará una evaluación por juicio de expertos, este método consiste básicamente en solicitar a una serie de personas de demanda de un juicio hacia un objeto de estudio, bajo dos elementos importantes que es la validez y la fiabilidad.

La validez según Arribas (2004) se refiere a la medida en la que el objeto de estudio sirve para el propósito para el cual ha sido construido, mientras que la fiabilidad es el grado en el que el objeto de estudio mide el nivel de cohesión de los diferentes elementos que constituyen el objeto de estudio, es decir se refiere al grado de acuerdo entre los expertos

Por los tanto, para el proceso de validación de un juicio de expertos se establece los pasos que de acuerdo con Escobar-Pérez y Cuervo-Martínez (2008) son:

1. Establecer el objetivo del juicio de expertos
2. Selección de los Expertos
3. Especificar los criterios y escalas de valoración.
4. Diseñar la plantilla
5. Calcular la concordancia de los expertos

Objetivo del juicio de expertos

Realizar la validación por juicio de expertos el Modelo de Gobierno de Seguridad de la Información propuesto para las Instituciones de Educación Superior del Ecuador a través de criterios de claridad, coherentes y relevantes.

Selección de los expertos

La selección de los expertos es elemento fundamental para el iniciar el proceso de validez del modelo, para ello se estableció un perfil basado en el grado académico, experticia en seguridad de la información, experiencia en el manejo de seguridad de la información en instituciones de educación superior y temas de conocimiento como lo indica la Tabla 67.

Tabla 67. Perfil para la elección de los expertos

Grado Académico	Doctor en informática o ciencias de la computación/Magister en Telemática, seguridad de la información o en gerencia de sistemas de información o afines
Experiencia	Gobierno de tecnologías de la información Seguridad de la información Dirección de tecnología de la información
Años de experiencia	Superior a tres años en instituciones de educación superior
Temas de conocimiento	Seguridad de la información, implantación de políticas y procesos de seguridad de la información, gestión de seguridad de la información, gobierno de tecnologías de la información.

Para la selección de los profesionales expertos, se revisaron 10 hojas de vida de académicos e investigadores que actualmente se encuentran laborando en instituciones de educación superior y que han tenido experiencia en el área de seguridad de la información. De acuerdo con los criterios mencionados, los expertos que se ha elegido para la validación del modelo son:

Tabla 68. Expertos para validación del modelo

Nombre del Experto	Institución
Robert Enríquez Reyes	Universidad Central del Ecuador
Patricia Viracocha Soria	Instituto Superior Tecnológico Cordillera
Mercedes Torres Bueno	Consultora Empresarial GTS – Seguridad de la Información
Fabián Hurtado V.	Universidad Internacional SEK
Diego Goyes Mosquera	Universidad de la Américas
Claudia Pitty Marcos	Universidad Nacional del Centro de la Provincia de B. Aires
Fabián Astudillos S.	Universidad de Cuenca

Las respuestas de cada uno de los expertos permanecerán anónimas y serán de carácter privado. Además, todos los datos entregados serán absolutamente confidenciales y sólo se usarán para los fines de validación del Modelo de gobierno de seguridad de la información para instituciones de educación superior.

Criterios y escalas de valoración

En este apartado se establecerán los criterios bajos los cuales se realizará la valoración de cada uno de los elementos que conforman el modelo de gobierno de seguridad de la información para instituciones de educación superior.

Los criterios bajo los cuales se establecerá la evaluación se describen en la tabla 69:

Tabla 69. Criterios de validación de expertos

Criterio	Descripción	Indicador
Claridad	Los elementos del modelo de seguridad de la información se comprenden fácilmente, es decir, su sintaxis y semántica son adecuadas	Las conceptualizaciones y descripciones de los elementos del modelo de seguridad de la información no son claros, ni entendibles.
		Los elementos del modelo de seguridad de la información requieren bastantes modificaciones o una modificación profunda respecto al uso de las palabras de acuerdo con su significado o por ordenación de estas.
		Los elementos del modelo de seguridad de la información requieren de una modificación muy específica en la terminología utilizada.
		Las conceptualizaciones y descripciones de los elementos del modelo de seguridad de la información son claros, su semántica y sintaxis son adecuadas.
Coherencia	Los elementos del modelo de seguridad de la información tienen relación lógica entre sí y están articulados a las funciones de docencia, investigación y vinculación.	Los elementos del modelo de seguridad de la información no tienen relación lógica con los procesos de gobernanza.
		Los elementos del modelo de seguridad de la información tienen una relación tangencial con los procesos de gobernanza.
		Los elementos del modelo de seguridad de la información tienen una relación moderada con los procesos de gobernanza.
		Los elementos del modelo de seguridad de la información se encuentran completamente relacionados con los procesos de gobernanza.
Relevancia	Los elementos del modelo de seguridad de la información son esenciales o importantes.	Los elementos del modelo de seguridad de la información pueden ser eliminados sin que se vea afectada la medición de los procesos de gobernanza.
		Algunos de los elementos del modelo de seguridad de la información tienen alguna relevancia.
		Todos los elementos del modelo de gobierno de seguridad de la información son relativamente importantes.
		Todos los elementos del modelo de gobierno de seguridad de la información son muy relevantes.

Además de los criterios se establecieron cuatro dimensiones para el modelo bajo los cuales los expertos deben consignar su valoración. Las dimensiones

establecidas son: principios, objetivos, procesos y modelo, mismas que hacen referencia a cada uno de los elementos que conforman el modelo de gobierno de seguridad de la información para instituciones de educación superior.

Para cada dimensión se propone valoración en claridad, coherencia y relevancia bajo los indicadores de cada uno de los criterios.

La escala de valoración con la cual deberán trabajar los expertos está determinada en un rango de 1 a 4 que representan cuantitativamente a no cumple, cumple parcialmente, cumple moderadamente, cumple toralmente como lo muestra la Tabla 70.

Tabla 70. Escala de validación

Descripción	Escala cuantitativa
No cumple	1
Cumple parcialmente	2
Cumple Moderadamente	3
Cumple totalmente	4

Diseño de la Plantilla de evaluación

Para la realización de la valoración de los expertos se diseñó un instrumento dividido en cuatro dimensiones principios, objetivos, proceso y modelo (véase Anexo 2) cada uno de ellos en los medidos en claridad, coherencia y relevancia.

Para la dimensión principios contiene una matriz en donde en las filas contiene los tres criterios y en las columnas los seis principios del modelo de gobierno de seguridad de la información.

En cuanto a la dimensión objetivos se establece que el análisis se establezca por principio, es decir se valorar por parte de los expertos los objetivos de cada uno de los principios (ver Anexo 3).

En cuanto a la presentación de las dimensiones proceso y modelo se analizan en los mismos descritos anteriormente con los elementos de cada uno.

Calcular la concordancia de los expertos

Una vez que se diseñó la plantilla de recolección de la valoración de los expertos, estas fueron enviadas a cada uno con el fin de tabularlos y procesarlos estadísticamente. Las valoraciones que los siete expertos dieron a cada una de las dimensiones fueron organizadas de tal manera que permita un correcto análisis como se puede observar en el Anexo 3

Luego de la valoración de los expertos los datos son procesados para calcular el coeficiente v de Aiken para el análisis y determinar el grado de validez, es el mismo que se define como la razón de la valoración obtenida sobre la suma máxima de la diferencia entre los valores posibles como se indica 1(Aiken, 1980):

$$v_j = \frac{s_j}{(n(c-1))} \quad (1)$$

$$s_j = \sum_{i=1}^{n} r_{ij} \quad (j = 1..m;\ i = 1..n)$$

Donde:
s_j = Suma de las valoraciones consignadas por los expertos.
n = Número de expertos.
m = Número de elementos del modelo
r = Valor asignado por los expertos
c = Número de valores de la escala.

El coeficiente de validez de Aiken solo puede tomar valores entre o y uno, lo que significa que 0 no existe un acuerdo de los expertos y 1 que existe total acuerdo, para el caso de esta investigación se cuenta con siete jueces con un nivel de significancia $p < 0.05$ para que sea considerado como valido. Escurra Mayaute (1988) establece que para cinco jueces el valor de Aiken es de 0.71, para seis expertos es 0.86 y para siete el valor de 1.

Cuando el $v \geq 0.86$ especialmente para seis de los siete expertos, significa que los expertos están de acuerdo en que los elementos son significativos.

La Tabla 71 muestra el cálculo de los coeficientes de Aiken para la dimensión de principios, en cuanto a la validez muestran que en el criterio calidad existen tres valores por debajo del valor permitido, lo que implica que es necesario revisarlos y considerar las recomendaciones realizadas por los expertos, sin embargo, en el valor del coeficiente a nivel de criterio $v = 0{,}87$ lo que estadísticamente muestra que son significativos y el modelo esta validado en cuanto al criterio de claridad.

Para coherencia se necesita observar las recomendaciones que realizan los expertos E4, E5, E6, ya que sus valores son 0,83; 0,72; 0,78 que se encuentran por debajo del valor mínimo aceptado, sin embargo, el coeficiente de Aiken para el criterio en general es 0, 86 lo que implica que estadísticamente significativo y el modelo es validado en cuento a la Coherencia con la que está estructurado.

Los expertos E3, E5 en criterio relevancia establece un coeficiente de 0,72; 0,78 respectivamente lo que es necesario revisar las recomendación y observaciones realizadas. En términos de criterio relevancia muestra un coeficiente de Aiken de 0,86 lo que estadísticamente valida el modelo en base a dicho criterio.

Tabla 71. Coeficiente V de Aiken dimensión principios

Principios		v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	E1	0,78	0,87	0,86
	E2	0,89		
	E3	0,78		
	E4	0,94		
	E5	0,83		
	E6	0,94		
	E7	0,89		
Coherencia	E1	0,94	0,86	
	E2	0,94		
	E3	0,89		
	E4	0,83		
	E5	0,72		
	E6	0,78		
	E7	0,89		
Relevancia	E1	0,94	0,86	
	E2	0,89		
	E3	0,72		
	E4	0,89		
	E5	0,78		
	E6	0,89		
	E7	0,89		

Luego de haber realizado el cálculo de los valores de Aiken de cada uno de los expertos en función de claridad, coherencia y relevancia en la dimensión de objetivos se puede observar los resultados que se muestran en la Tabla 72.

En el criterio de claridad se debe prestar atención a lo que expresa los expertos E5 y E7 cuyos valores calculados del coeficiente de Aiken es 0,83 y 0.81 respectivamente, de la misma manera para el criterio coherencia se debe prestar atención a las recomendaciones que realizan los expertos E2, E6 y E7 ya que sus valores son 0,85; en cuanto al criterio de relevancia el valor de Aiken más bajo es la del experto E6 cuyo valor es 0,83.

Sin embargo, el valor de Aiken de todos los criterios es mayores a 0,86 valor mínimo aceptado para la validez del modelo, lo que significa que el modelo en cuanto a sus objetivos es claro, coherente y relevantes para el modelo de gobierno de seguridad de la información. Para la dimensión Objetivos el coeficiente es de 0,89 lo que significa que es validado.

Tabla 72. Coeficiente V de Aiken dimensión Objetivos

Objetivos		v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	E1	**0,96**	**0,88**	0,89
	E2	**0,90**		
	E3	**0,88**		
	E4	**0,90**		
	E5	**0,83**		
	E6	**0,88**		
	E7	**0,81**		
Coherencia	E1	**0,90**	**0,89**	
	E2	**0,85**		
	E3	**0,92**		
	E4	**0,94**		
	E5	**0,94**		
	E6	**0,85**		
	E7	**0,85**		
Relevancia	E1	**1,00**	**0,90**	
	E2	**0,88**		
	E3	**0,92**		
	E4	**0,85**		
	E5	**0,96**		
	E6	**0,83**		
	E7	**0,88**		

La Tabla 73 muestra el cálculo de los coeficientes de Aiken para la dimensión del proceso del modelo de gobierno de seguridad de la información, todos los valores calculados están por encima del mínimo (0,86), quiere decir que los expertos validan el proceso en cuanto a claridad, coherencia y relevancia.

De la misma manera para cada criterio los valores son mayores a 0,86 mínimo aceptable, es decir coeficiente de Aiken para claridad es de 0,98, coherencia 0,92 y relevancia 0,90 lo que da un valor de toda la dimensión de 0,94 lo que implica que la dimensión el validada por los expertos.

Tabla 73. Coeficiente V de Aiken dimensión proceso

Proceso		v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	E1	0,87	0,98	0,94
	E2	1,00		
	E3	1,00		
	E4	1,00		
	E5	1,00		
	E6	1,00		
	E7	1,00		
Coherencia	E1	1,00	0,92	
	E2	0,93		
	E3	0,87		
	E4	0,93		
	E5	0,93		
	E6	0,87		
	E7	0,93		
Relevancia	E1	1,00	0,90	
	E2	1,00		
	E3	0,93		
	E4	0,87		
	E5	0,87		
	E6	0,87		
	E7	0,80		

Como resumen general del proceso de validación del modelo por parte de los expertos se puede observar en la Tabla 74 que el modelo es validado en cuanto a claridad, coherencia y relevancia obteniendo un valor de 0,90 por parte de los expertos.

Tabla 74. Coeficiente V de Aiken dimensión modelo

Modelo	Criterios			v de Aiken por dimensión	v de Aiken modelo
	Claridad	Coherencia	Relevancia		
Principios	0,87	0,86	0,86	0,86	0,90
Objetivos	0,88	0,89	0,90	0,89	
Proceso	0,98	0,92	0,90	0,94	

Es evidente que el modelo debe considerar las observaciones realizadas por los expertos en cada una de las dimensiones, para ellos se realiza un análisis cualitativo de cada una de las recomendaciones realizadas entre las que mayor coincidencia tienen los expertos se detallan a continuación:

- Se debe considerar una redacción más clara de los principios de responsabilidad, comportamiento humano orientados a la información o activos de información.

- En los objetivos cuidar la relación y concordancia con los principios.
- Ser muy cauto en la forma de la redacción, para que las instituciones de educación superior puedan entender el modelo de gobernanza y aplicarlo.

En función de estos resultados se redacta la segunda versión del modelo de seguridad de la información (véase Anexo 1).

6.9.2 Conclusiones

- El modelo de gobierno de seguridad de la información para instituciones de educación superior está fuertemente sustentado en las ISO/IEC 38500:2015 e ISO/IEC 27014:2013 de forma integral. La norma ISO/IEC 38500:2015 está presente principalmente en el primer nivel del modelo en lo que respecta a los principios: responsabilidad, desempeño, estrategia y comportamiento humano; con dos elementos sustanciales: análisis de riesgos y conformidad, de la norma ISO 27014:2013 que incluyen las acciones de dirigir, evaluar, monitorear, comunicar y asegurar.

- En este estudio, se ha realizado un proceso de armonización utilizando un mapeo para la comparación de ambos estándares, identificando los elementos relacionados, siguiendo las pautas de Serrano, Gomez, y Juiz (2018) y de Tenorio Chacón (2016), y con la ayuda de la regla de Pareto se ha logrado resumir en la Tabla 18 la correspondencia que existe entre los dos estándares, para de esta forma, definir niveles del MoGSIIES.

- El gobierno de seguridad de la información es parte específica del gobierno de TI. Aunque se lo quiera mirar de forma separada los dos inciden en los procesos estratégicos de las organizaciones. Otro aspecto importante que se ha llevado a cabo es la comprensión de la importancia que tiene el gobierno de seguridad de la información sobre el gobierno de TI, y la responsabilidad en la toma de decisiones que le corresponde al comité estratégico de dirección de la institución.

- Con este estudio se ha contribuido al conocimiento y colaboración de quienes toman decisiones en el comité estratégico de dirección de seguridad de la información en las instituciones, superando la barrera de visibilidad que adolece un gobierno organizacional.

- En este contexto, es crucial establecer elementos de gobernanza de seguridad de la información en cada una de las instituciones de educación superior para garantizar los niveles de seguridad de sus activos de información resultado de sus procesos académicos y administrativos articulados a las funciones sustantivas del sistema de educación superior. Es importante que las instituciones de educación superior aborden el modelo propuesto desde las directrices de cada una, con sus objetivos estratégicos y el direccionamiento de los responsables de la gobernanza de la seguridad de la información, así como, de quienes están frente a las tecnologías de la información.

6.9.3 Recomendaciones

- Es necesario establecer una guía de implementación el modelo de gobierno de seguridad de la información para instituciones de educación superior para dar continuidad al trabajo desarrollado; y realizar un proceso de evaluación de madurez del grado de seguridad de la información para establecer un plan de mejora continua.

- Se recomienda para la implantación del modelo de gobierno de seguridad de la información en las instituciones de educación superior se establezca como prioridad la conformación de un comité de gobierno de seguridad de la información, quien asesorará al gobierno corporativo de la institución de educación superior en las decisiones que se deban tomar en el marco de seguridad de la información.

- Trabajos futuros se enfocarán en el fortalecimiento del modelo mediante análisis factorial de los componentes, con la participación de actores de las instituciones de educación superior del Ecuador, una vez que sea implementado el modelo. De

esta manera se podrá conocer los niveles de confiabilidad de cada uno de los elementos propuestos.

- Es menester lograr que los profesionales del área de Tecnologías de la Información y del gobierno corporativo de la institución de educación superior se empoderen de los términos de gobernanza de seguridad de la información, para que ellos sean entes activos de este elemento estratégico, dentro de la institución.

BIBLIOGRAFÍA

Aiken, L. R. (1980). Content Validity and Reliability of Single Items or Questionnaires. *Educational and Psychological Measurement*, *40*(4), 955–959.

Albán, P., y Saavedra, R. (2009). *Propuesta de un Plan y Sistema de Control Estratégico, Aplicando la Metodología de Cuadro de Mando Integral, en la empresa Kilikos Flowers Cia. Ltda, dedicada a la producción y comercialización de rosas, ubicado en el Cantón Pedro Moncayo*. Escuela Politécnica Nacional.

Aliaga Flores, L. C. (2013). *Diseño de un sistema de gestión de seguridad de información para un instituto educativo* (phd thesis, pontificia universidad católica del perú). recuperado de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5122/cepeda_lorena_estudio_pre-factibilidad_implementacion_cadena_comidas_rapidas_pollo_lima_norte.pdf?sequence=4

Armendáris, N., y López, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica ESPOL*, *30*(Mayo), 51–69.

Arribas, M. (2004). *Diseño y validación de cuestionarios*. *5*, 7.

Asgarkhani, M., Correia, E., y Sarkar, A. (2017). An overview of information security governance. *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017*, *2017-Janua*, 1–4. https://doi.org/10.1109/ICAMMAET.2017.8186666

Baldassarre, M. T., Caivano, D., Pino, F. J., Piattini, M., y Visaggio, G. (2012). Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: From a theoretical comparison to a real case application. *Softw. Qual. J*, *20*(2), 309–335.

Bayona Soto, J. A., Lastra Colobon, R., y Trigos Sanchez, F. (2014). *Guia de gobernabilidad de tecnologias de la informacion y comunicación basada en la norma ntc-iso/iec 38500 para la universidad francisco de paula santander ocaña* (PhD Thesis, Univeridad Francisco de Paula Santander Ocaña). Recuperado de http://200.93.148.28/drupal/files/D1dCBLxWr0Gnvid.pdf

Berrío López, J. P. (2016). *Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001*. Universidad Nacional de Colombia Facultad.

Bowen, P., Chew, E., Hash, J. (2007). *Information Security Guide For Government Executives* (Computer S; C. S. D. I. T. Laboratory, Ed.). Gaithersburg, MD: NISTIR 7359.

Buitrago, C., Bonilla, H., y Murillo, C. (2012). *Diseño De Una Metodologia Para La Implementación Del Sistema De Gestión De Seguridad De La Información—Sgsi, En El Sector De Laboratorios De Analisis Microbiologicos, Basado En Iso 27001*. UNIVERSIDAD EAN.

Cairo, M. M., Puga, O. V., Mallea, I. P., Cobas, R. P., y Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática Methodology for the Implementation of Automated Management of Computer Security Controls. *Revista Cubana De Ciencias Informáticas*, *10*(2), 14–27.

Camacho, R. (2008). *Diseño e implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de los activos informáticos de la Universidad Central de Venezuela* . Universidad Central de Venezuela.

Carcary, M., Renaud, K., McLaughlin, S., y O'Brien, C. (2016). A Framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/MITP.2016.27

Cárdenas-Solano, L.-J., Martínez-Ardila, H., y Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: Revisión bibliográfica/ Information security management: A bibliographic review. *El profesional de la información*, *25*(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Castro Márquez, D. E., Veláquez Pérez, T., y Castro Silva, H. (2018). Integración de Seguridad y gestión de servicios en el Gobierno de las Tecnologías de la Información. *Revista Colombiana de Tecnología Avanzada*, *2*(32), 1–6. https://doi.org/10.24054/16927257.v32.n32.2018.3027

CES. *Reglamento de Régimen Académico.* , (2019).

CGI Group. (2016). IT Security Governance—A holistic approach. *CGI Group INC*, 1–8.

Chaudhuri, A. (2011). Enabling effective IT governance: Leveraging ISO/IEC 38500:2008 and COBIT to Achieve Business-IT Alignment. *Edpacs*, *44*(2), 1–18. https://doi.org/10.1080/07366981.2011.599278

Clark, T. L., y Sitko, T. D. (2008). Information security governance: Standardizing the practice of information Security. *EDUCAUSE Center for Applied Research Research Bulletin*, *2008*(17), 1–11.

Consejo de Educación Superior. (2013). *Reglamento De Régimen Académico (Codificación)*. (211), 1–59.

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador* (R. Oficia, Ed.). Registro Oficial.

Cordero Guzman, D. M. (2015). Mejores Prácticas Para Implantar El Gobierno De Tecnologías De La Información (Ti), En La Universidad Ecuatoriana Best Practices for Implementing the Information Tecnology (It). *Revista científica y tecnología UPSE*, *2*(3), 10.

Da Veiga, A., y Eloff, J. H. P. (2007a). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Da Veiga, A., y Eloff, J. H. P. (2007b). An information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

De Oliveira Alves, G. A., Rust da Costa Carmo, L. F., y Ribeiro Dustra de Almeida, A. C. (2006). Enterprice Security Governance A practical guide to implement and control Information Security Governance (ISG). *IEEE/IFIP Business Driven IT Management*, 71–80. https://doi.org/10.1109/BDIM.2006.1649213

Escobar-Pérez, J., y Cuervo-Martínez, Á. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. *Avances en Medición*, *6*, 27–36.

Escurra Mayaute, L. M. (1988). Cuantificación de la validez de contenido por criterio de jueces. *Revista de Psicología*, *6*(1–2), 103–111.

Fernández, A., Llorens, F., Fernández Martinez, A., y Llorens Largo, F. (2011). Gobierno de las tecnologías de la información en Universidades. *CRUE Conferencia de Rectores de las Universidades Españolas*, pp. 1–10.

Fernandez, A., y Llorenz, F. (2014). Gobierno de TI para Universidades. En Conferencia de Rectores de las Universidades Españolas (Ed.), *Igarss 2014* (CRUE). https://doi.org/10.1007/s13398-014-0173-7.2

Fernández, C., y Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO* (AENORedici; AENORediciones, Ed.). https://doi.org/978-84-8143-764-6

Fernández Mayor, O., y Martínez Fernández, A. (2010). Proyecto de arranque del Gobierno de las TI en una Universidad.

García-Holgado, A., y García-Peñalvo, F. J. (2015). Definition of a Technological Ecosystem for Scientific Knowledge Management in a PhD Programme. *Proceedings of the 3rd International Conference on Technological Ecosystems for Enhancing Multiculturality - TEEM '15*, 695–700. https://doi.org/10.1145/2808580.2808686

Gashgari, G., Walters, R., y Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, 295–301. https://doi.org/10.5220/0006303102950301

Gelbstein, E. (2011a). La integridad de los datos: El aspecto más relegado de la seguridad de la información. *Isaca Journal*, *6*(1), 6.

Gelbstein, E. (2011b). La integridad de los datos: El aspecto más relegado de la seguridad de la información. *Isaca Journal*, *6*(1), 6.

Henderson, J. C., y Venkatraman, N. (1999). Strategic aligment: Leveraging information technology for transforming organizations. *IBM SYSTEMS JOURNAL*, *32*(1), 472–484.

INEN-ISO/IEC. (2019). *Tecnologías de la Información—Gobernanzas de TI para la Organización (ISO/IEC 38500:2015, IDT)* (pp. 1–5). pp. 1–5. Quito: INEN.

INEN-ISO/IEC, N. (2016). *Tecnologías de la Información—Técnicas de Seguridad—Gobierno de Seguridad de la Infromación (ISO/IEC 27014:2013, IDT)* (pp. 1–5). pp. 1–5. Quito: INEN.

ISO. (2013). *Sistema de Gestión de la Seguridad de la Información*.

Llorens, F., Bayona, J. J., Gómez, J., y Sanguino, F. (2010). The University of Alicante's institutional strategy to promote the open dissemination of knowledge. *Online Information Review*, *34*(4), 565–582. https://doi.org/10.1108/14684521011072981

Luqman Ayodele, P. (2018). *Information Security Governance: An action plan for a non-profit organization based in the Nordics* (Thesis, Laurea University of Applied Sciences). Recuperado de https://www.theseus.fi/bitstream/handle/10024/147149/Information_Security.pdf?sequence=1

Martelo, R., Maderay, J., y Betín, A. (2015). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Informacion Tecnologica*, *26*(2), 129–134. https://doi.org/10.4067/S0718-07642015000200015

Martínez, A. F. (2009a). Análisis, Planificación Y Gobierno De Las Tecnologías De La Información En Las Universidades (Universidad de Almería; Vol. 7). https://doi.org/10.1017/CBO9781107415324.004

Martínez, A. F. (2009b). *Análisis, Planificación Y Gobierno De Las Tecnologías De La Información En Las Universidades* (PhD Thesis, Universidad de Almería). https://doi.org/10.1017/CBO9781107415324.004

Marulanda Echeverry, C. E., y López Trujillo, M. (1995). MODELOS DE DESARROLLO PARA GOBIERNO TI. *Scientia et Technica Año XV*, *1*(41), 185–190. https://doi.org/10.1126/science.166.3906.695

McDermid, D., Mahncke, R. J., y Williams, P. A. H. (2010). An Information Security Governance Encounter for Australian Primary Care Health Providers. *Australian Information Security Management Conference*, (November), 637–643. https://doi.org/10.4225/75/57b6734334780

Melorose, J., Perroy, R., y Careas, S. (2015). Gobierno de TI: Estado Actual del gobierno de TI en Empresas Privadas de Seguridad. *Statewide Agricultural Land Use Baseline 2015*, *1*. https://doi.org/10.1017/CBO9781107415324.004

Merchán, V., y Rodríguez, R. (2015). Análisis de los modelos de Gobierno de Tecnologías de la Información y sus relaciones con el Modelo de Excelencia Iberoamericano. En R. de U. con C. en I. (RedUNCI) (Ed.), *XXI Congreso Argentino de Ciencias de la Computación* (Vol. 1, p. 10). Recuperado de http://sedici.unlp.edu.ar/handle/10915/50028

Meyer, C. O. (2014). Normas ISO de Seguridad de la Información. *revista cripto red*, (Gestión y Auditoría de Riesgos y Seguridad de la Información /Normas ISO), 1–13.

Morales Andaluz, J. V. (2015). Modelos de gobierno TI para instituciones de Educación Superior. *Revista Politécnica*, *36*(3), 6.

OCDE. (2004). *Principios de Gobierno Corporativo*. Ministerio de Economía y Hacienda de España.

Ochoa Arévalo, P. A. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL-RTE*, *28*(3), 1–17.

OpenGroup. (2013). TOGAF VERSION 9.1 -Guia de bolsillo. En *Business Management*.

Padilla-Verdugo, R. ;, Cadena-Vela, S. ;, Enríquez-Reyes, R. ;, Córdova-Ochoa, J. ;, y Llorens-Largo, F. (2018a). *"UETIC 2017. Estado de las Tecnologías de la Información en las Universidades Ecuatorianas"* (Primera Ed, Vol. 1; RED CEDIA, Ed.). Recuperado de www.cedia.edu.ec

Padilla-Verdugo, R. ;, Cadena-Vela, S. ;, Enríquez-Reyes, R. ;, Córdova-Ochoa, J. ;, y Llorens-Largo, F. (2018b). *"UETIC 2017. Estado de las Tecnologías de la Información en las Universidades Ecuatorianas"* (Primera Ed, Vol. 1; RED CEDIA, Ed.). Cuenca: RED CEDIA.

Pardo, C., Pino, F. J., Garcia, F., Baldassarre, M. T., y Piattini, M. (2013). From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. *J. Syst. Softw*.

Pérez Lorences, P., y García Ávila, L. F. (2013). The Evaluation and Improvement of IT Governance. *Journal of Information Systems and Technology Management*, *10*(2), 219–234. https://doi.org/10.4301/S1807-17752013000200002

Periñán, I. L. M., y Villegas, G. U. (2011). Gobierno de TI – Estado del arte. *Sistemas & Telemática*, *9*(17), 23–53.

Pillo-Guanoluisa, D., y Enriquez-Reyes, R. (2017). *Propuesta de un Modelo de Gobierno de Tecnología de la Información para Hospitales públicos. Caso: Hospital General Docente de Calderón*. Universidad de las Americas - UDLA.

Quintanilla, M. Y. (2016). Modelo de referencia de gobierno de las tecnologías de la información para instituciones universitarias. *Interfases*, *9*(9), 87–116.

Salazar, J. B., y Campos, P. G. (2009). Modelo para seguridad de la información en TIC. *CEUR Workshop Proceedings*, *488*, 234–253. https://doi.org/10.1017/CBO9781107415324.004

Serrano, A., Gomez, B., y Juiz, C. (2018). Why the governance of projects, programs and portfolios (PPP) cannot be separated from the governance of IT standard. *2017 National Information Technology Conference, NITC 2017*, *2017-Septe*, 106–111. https://doi.org/10.1109/NITC.2017.8285661

Tenorio Chacón, O. (2016). Gobierno de seguridad de información, mito o realidad. En ISACA (Ed.), *IX Congreso ISACA Costa Rica* (pp. 1–21). Recuperado de http://m.isaca.org/chapters12/costa-rica/events/Documents/Presentaciones congreso Isaca 2016/13. Gobierno de Seguridad de la información.pdf

Thiagarajan, V. (2006). BS ISO IEC 17799 SANS Checklist. En *SANS Institute*.

Torres Bermúdez, A. A., y Lucumí Sánchez, W. (2015). Modelo de Gestión y Gobierno de Tecnologías de Información en Universidades de Colombia: Caso Instituciones de Educación Superior en el Departamento del Cauca. *RedClara*, *1*(Octubre), 15.

Valencia Duque, F. J., y 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 y Tecnologías de Información*, (22), 73–88. https://doi.org/10.17013/risti.22.73

Vargas-Bermúdez, F. A. (2015). Marcos De Control Y Estándares Para El Gobierno De Tecnologías De Información (Ti). *Revista I3+*, *3*(1), 30–45.

Vecino Pico, H. (2017). Normas ISO y marcos de referencia para gobernanza de las TIC, revisión. *COMTEL 2017*, 8.

Velasco Melo, A. H. (2008). El Derecho Informático y la Gestión de la Seguridad de la Información: Una Perspectiva con base en la Norma ISO 27001. *Revista de Derecho*, *29*(1), 1–36.

Yory, J. (2006). Un acercamiento a las mejores prácticas de seguridad de información internacionalmente reconocidas en el estándar ISO 17799:2005. *MVA*, 30.

Zamora Jiménez, J. (2010). *Análisis y propuesta de herramientas para el diseño de una PYME basándose en ITIL y COBIT*.

ANEXO 1. MODELO DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA IES

MODELO DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

Primera edición 1.0 2019-10

TECNOLOGÍAS DE LA INFORMACIÓN – GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES).

INFORMATION TECHNOLOGY — INFORMATION SECURITY GOVERNANCE FOR HIGHER EDUCATION INSTITUTIONS

Objeto y campo de aplicación

Este modelo proporciona los elementos, conceptos y principios para que los miembros del comité de seguridad de la información de las instituciones de educación superior del Ecuador puedan medir, evaluar, dirigir, monitorear, comunicar y asegurar las actividades de gobierno de seguridad de la información relacionadas con el desarrollo y articulación de las funciones sustantivas docencia, investigación y vinculación.

Referencias normativas

Las Instituciones de Educación Superior se han visto continuamente amenazadas ante la falta de dirección y control desde la óptica de la seguridad de la información en el contexto del gobierno de tecnologías de la información. La norma ISO/IEC 27014:2013 representa una oportunidad para gobernar la seguridad de la información, sin embargo, adolece de clara alineación que permita articular sus actividades con el gobierno de tecnologías de la información y brindar visibilidad al gobierno organizacional. Mediante un proceso de armonización entre los estándares ISO/IEC 27014:2013 e ISO/IEC 38500:2015 se identificaron problemas debido a la sobre posición de elementos, aunque también se identificó otros elementos fuertemente relacionados lo que coadyuva a un modelo consistente de gobierno de seguridad de la información en tres niveles: principios, objetivos e indicadores.

Este trabajo contribuye al conocimiento y toma de decisiones en los comités estratégicos de dirección y control de la seguridad de la información en las instituciones de educación superior del Ecuador.

Términos y definiciones

Para efecto de este modelo se aplicarán la siguientes conceptualizaciones y definiciones dadas por las normas ISO/IEC 38500:2015, Norma ISO/IEC 27014:2013, ISO/IEC 27000:2009 y la Ley Orgánica Reformatoria a la Ley Orgánica de Educación Superior, 2018.

Tecnologías de la información (TI). - Se refiere a la capacidad que tiene la institución de trabajar con hardware y software para el procesamiento, transmisión y almacenamiento de datos que la misma genera en la realización de sus procesos.

Gobierno Corporativo. – Es el que define la estructura de la organización que se encarga de dirigir y administrar la institución de educación superior, así como la contralora adecuadamente las operaciones de esta, esto también implica la toma de decisiones corporativas después de discutirla y ajustarlos a los intereses de la IES (OCDE, 2004).

Gerencia Ejecutiva. – Son las personas o grupo de personas quienes tienen delegada la responsabilidad del directorio para la implementación de las estrategias y políticas para lograr el propósito de la organización (INEN-ISO/IEC, 2016).

Gobierno de TI.- Es aquel que integra e institucionaliza las buenas prácticas para garantizar que las tecnologías de la información en la empresa se alinean con los objetivos del negocio. Además, el gobierno de TI facilita que la institución aproveche al máximo su información, incremente los beneficios, capitalice las oportunidades y gane ventaja competitiva (Palao, 2010).

Gobierno de Seguridad de la Información. - Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

Dirigir. - Es el proceso de gobierno a través del cual el directorio da las directrices acerca de los objetivos de seguridad de la información y las estrategias que necesitan ser implementadas. La directriz puede incluir cambios en los niveles de dotación de recursos, asignación de recursos, el establecimiento de prioridades en las actividades y las aprobaciones de las políticas, la aceptación de riesgos materiales y planes de gestión de riesgos (INEN-ISO/IEC, 2016).

Evaluar. - Es el proceso de gobierno que considera el logro y previsión de los objetivos de seguridad basados en los procesos actuales y los cambios previstos para determinar donde se requieren ajustes para optimizar el logro de los objetivos estratégicos en el futuro (INEN-ISO/IEC, 2016).

Monitorear. - Es el proceso de gobierno que permite al directorio evaluar el logro de los objetivos estratégicos (INEN-ISO/IEC, 2016).

Comunicar. - Es el proceso de gobierno bidireccional mediante el cual el directorio y las partes interesadas intercambian información sobre seguridad de la información de acuerdo a sus necesidades específicas (INEN-ISO/IEC, 2016).

Asegurar. - Es el proceso de gobierno mediante el cual se audita, revisa o certifica las actividades de gobierno y las actividades operativas con el fin de alcanzar el nivel deseado de seguridad de la información.

Responsabilidad .- Se refiere a que los miembros de la organización entienden y aceptan sus responsabilidades con respecto de los procesos que manejan, así como también, están conscientes de la responsabilidad que se requiere en las acciones que ejecutan para la institución (INEN-ISO/IEC, 2019).

Estrategia .- Es la herramienta de gestión que toma en cuenta las capacidades actuales y futuras de tecnología de la información, los planes para el uso de tecnología de la información, la satisfacción de las necesidades actuales, así como

también, las acciones para la mejora continua de los negocios de la institución (INEN-ISO/IEC, 2019).

Desempeño .- Se refiere al proceso para verificar si las tecnología de la información son adecuadas para apoyar a la institución en los servicios que brinda, valorar sus niveles de calidad y cumplir con los requisitos de negocios actuales y futuros de la institución (INEN-ISO/IEC, 2019).

Conformidad. – Establece que el uso de tecnologías de la información cumple con todas las leyes y reglamentos obligatorios. Las políticas y prácticas se encuentran claramente definidas, implementadas y aplicadas (INEN-ISO/IEC, 2019).

Comportamiento humano. – En las políticas, prácticas y decisiones de TI se demuestra respeto por el comportamiento humano, incluidas las necesidades actuales y futuras de todas las personas involucradas en el proceso (INEN-ISO/IEC, 2019).

Análisis de Riesgo de TI. – Establece la capacidad que tiene la institución para identificar los procesos que generan valor para la organización, así como, las amenazas que puedan impedir que se logre alcanzar los objetivos estratégicos, para minimizar su impacto y plantear acciones de mejora.

Confidencialidad. - Se relaciona con la característica de protección, privacidad y acceso a la información y a las directrices y acciones necesarias para garantizarlos.

Integridad. - Se refiere a la integridad de los datos que son tratados al generar información. Estos deben ser precisos, válidos y coherentes, y contar con mecanismos que impidan su modificación y eliminación no autorizada (Gelbstein, 2011b).

Disponibilidad. - Se refiere a que la información debe estar disponible en el momento que sea requerida por cualquier unidad de negocio, así como también, para los servicios de TI que los requerimientos del negocio necesiten.

Alineamiento Estratégico. - Son las estrategias de gobernanza de TI y las de seguridad de la información que apoyan a la estrategia empresarial.

Docencia. - Se define como la construcción de conocimientos y desarrollo de capacidades y habilidades, resultante de la interacción entre profesores y estudiantes en experiencias de enseñanza- aprendizaje, en ambientes que promueven la relación de la teoría con la práctica y garanticen la libertad de pensamiento, la reflexión crítica y el compromiso ético (CES, 2019).

Investigación. - La investigación es una labor creativa, sistemática y sistémica fundamentada en debates epistemológicos y necesidades del entorno, que potencia los conocimientos y saberes científicos, ancestrales e interculturales. Se planifica de acuerdo con el modelo educativo, políticas, normativas, líneas de investigación y recursos de las IES y se implementa mediante programas y/o proyectos desarrollados bajo principios éticos y prácticas colaborativas (CES, 2019).

Vinculación. - La vinculación con la sociedad, como función sustantiva, genera capacidades e intercambio de conocimientos acorde a los dominios académicos de las IES para garantizar la construcción de respuestas efectivas a las necesidades y desafíos de su entorno. Contribuye con la pertinencia del quehacer educativo, mejorando la calidad de vida, el medio ambiente, el desarrollo productivo y la preservación, difusión y enriquecimiento de las culturas y saberes (CES, 2019).

Relación

Tomando como referencia la importancia que tiene la información que se genera en las funciones sustantivas de docencia, investigación y vinculación y el

resultado del análisis de la armonización de las normas ISO/IEC 27014: 2013 y las ISO/IEC38500:2015 se ha estructurado el diseño del Modelo de gobierno de seguridad de la información para las instituciones de educación superior. Este modelo considera los aspectos de información, talento humano, infraestructura y estrategia por el parte de las IES, y como resultado de la armonización de dichos modelos se considera los principios y objetivos.

Para el nivel directivo de las IES es de mucha importancia desarrollar una visión holística en donde se integre el gobierno de seguridad de la información, las estrategias y los objetivos de la institución, para garantizar que la información que se genera del desarrollo de los procesos de las funciones sustantivas demuestre confiabilidad, integridad y disponibilidad. De esta manera se espera lograr una alineación estratégica y conseguir los objetivos planteados corto, largo y mediano plazo. Como se ilustra en la figura 1.

Figura 1. Relación de las funciones sustantivas con los elementos del gobierno de seguridad de la información

Principios y proceso

Principios del MoGSIIES

En este apartado se describe cada uno de los principios del modelo de gobierno de seguridad de la información, alineados a los procesos que se generan en la docencia, investigación y vinculación. Los principios que se exponen definen las reglas para las acciones emprendidas desde el gobierno y servirán como una guía en la que se describen las tareas que armonizan los elementos de gobierno de TI, el gobierno de seguridad de la información y las funciones sustantivas.

Los principios constituyen la base del modelo de gobierno de seguridad de la información para las instituciones de educación superior. La conceptualización de cada uno de los principios determina lo que debería suceder en términos de gobernanza. El comité de seguridad de la información de la institución de educación superior deberá exigir que se implementen y apliquen los principios y se rinda cuenta de ellos.

Principio 1: Estrategia

Las estrategias que se plantea la IES deben estar en base a los objetivos estratégicos alcanzados y considerar las capacidades que tiene, tanto en infraestructura, como en la inversión en TI, así como también, en los mecanismos de seguridad de la información.

Las estrategias de gobierno de información y de gobierno de TI deben satisfacer las necesidades actuales de los procesos de negocio, asegurando confidencialidad, integridad y disponibilidad de la información cuando esta sea requerida por los actores de la institución de educación superior.

En marco de su actuación la IES debe establecer sus estrategias de seguridad de la información en base a las prioridades que se definan de acuerdo con sus necesidades de seguridad, su vulnerabilidad y riesgo en sus activos de información. Las estrategias deben contemplar un enfoque basado en riesgos y deben ser adoptadas por el gobierno corporativo.

Principio 2: Análisis de Riesgos

El gobierno de seguridad de la información para IES adoptará un nivel de decisión basado en un análisis de riesgos para determinar cuánto es el nivel de seguridad aceptable. De la misma manera este enfoque debe ser consistente e integrado, y definido en base a la disminución de las ventajas competitivas, daños en la reputación institucional, o pérdida y robo de los activos de información de los procesos académicos y administrativos vinculados a las funciones sustantivas.

El gobierno corporativo de la IES debe asignar los recursos para la implementación de una gestión de riesgos vinculados con la seguridad de la información. Esta gestión debe permitir determinar cuáles son sus vulnerabilidades y qué amenazas podrían presentarse y poner en riesgo la información.

En la medida que la IES tenga claro los riesgos a los cuales está expuesta debe implementar acciones preventivas y correctivas que garanticen mayores niveles de seguridad en sus activos de información de gestión y en las funciones sustantivas.

Principio 3: Conformidad

El gobierno de seguridad de la información cumple las políticas y prácticas de seguridad de la información definidas por la IES, las cuales están a su vez articuladas a las políticas y normativas institucionales, así como también, a las leyes, reglamentos y demás disposiciones emitidas por lo entes rectores de la educación superior y gubernamentales. Para ello, el gobierno corporativo de la IES debe gestionar que estas actividades se estén cumpliendo de manera satisfactoria en los procesos internos relacionados con los activos de información.

La conformidad establece el grado de cumplimiento de las políticas y prácticas de seguridad de la información que son llevadas a cabo por docentes, estudiantes, personal administrativo y directivo de la institución de educación superior respecto al manejo de los activos de información de los cuales son custodios. Este proceso implica, además, revisar el desempeño de estos actores en relación con los resultados del negocio.

Principio 4: Desempeño

El gobierno de seguridad de la información para IES debe garantizar que las estrategias y enfoque utilizados para la protección de la información, resultado de los procesos administrativos y académicos vinculados a las funciones sustantivas es apto para el cumplimiento de los objetivos estratégicos institucionales. El desempeño de la seguridad de la información en la IES debe ser mantenido dentro de los niveles establecidos para la satisfacción de las funciones sustantivas y estratégicas de la institución.

El gobierno corporativo de la IES debe evaluar periódicamente el desempeño de las estrategias, políticas y procedimientos de seguridad de la información y medir el impacto que tienen, no solo en términos de eficiencia y eficacia,

sino en cómo estos apoyan a los procesos institucionales y las funciones sustantivas.

Principio 5: Comportamiento Humano

Las estrategias, políticas, procesos, procedimientos y prácticas de seguridad de la información en la IES demuestran respeto por el comportamiento de todos los grupos involucrados (docentes, estudiantes, personal administrativo y directivo) a nivel interno y externo (proveedores) con la finalidad de establecer una cultura de seguridad de la información en la IES. Para ello el gobierno corporativo de la IES debe exigir, promover y apoyar la coordinación de las actividades de cada uno de sus integrantes para lograr un nivel de gobernanza coherente para la seguridad de la información.

El comportamiento humano es uno de los componentes más importantes en el proceso de gobernanza de seguridad de la información, por lo que es indispensable que docentes, estudiantes, personal administrativo y directivo sepan qué activos de información están en su custodio y cuáles son los comportamientos éticos que debe tener antes y durante su permanencia en el IES. Además, debe conocer qué se espera en su actuar durante el proceso de finalización de su contrato o cuando se da un cambio de cargo respecto al traspaso y entrega de información.

Los comportamientos éticos de los docentes, estudiantes, personal administrativo y directivo deben ser establecidos por la IES en concordancia con sus políticas, procesos y procedimientos de gobierno de seguridad de la información, los cuales son definidos a través de sus estrategias. Este proceso incluye la planificación de programas de educación, capacitación y sensibilización sobre seguridad de la información en todos los niveles operativos cuya finalidad es asegurar el cumplimiento del comportamiento ético.

Principio 6: Responsabilidad

El gobierno de seguridad de la información para IES en el principio de responsabilidad establece que se debe garantizar que las actividades que se desarrollan en los procesos de docencia, investigación y vinculación deben ser manejadas con responsabilidad por los profesores, estudiantes, personal administrativo y autoridades; y estos, a su vez, entienden el nivel de responsabilidad de su actuación y sus decisiones.

En el gobierno de seguridad de la información la responsabilidad se refiere a que docentes, estudiantes, personal administrativo y directivo de la institución de educación superior quienes son los custodios de la información y deben asegurar un ambiente en el que se pueda verificar la integridad, la disponibilidad y la confidencialidad de los activos de información. El área responsable de realizar el monitoreo del cumplimiento de las políticas de seguridad definidas es el gobierno de TI.

Objetivos de los principios del MoGSIIES

Objetivos: Estrategia

- Determinar cuál es la estrategia de seguridad de la información para toda la organización con un enfoque basado en riesgos.
- Alinear la estrategia institucional y de TI con la estrategia de seguridad de la información.
- Disponer de una estructura de dirección y modelo de toma de decisiones alineados a las estrategias de seguridad de la información.

- Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas internas vigentes de la institución de educación superior, así como, los estándares internacionales de gestión de seguridad de la información.

Objetivos: Análisis de Riesgos

- Definir la arquitectura de seguridad de la información que incluya procesos y su integración con los sistemas.
- Conocer los riesgos asociados a las vulnerabilidades y amenazas de los activos de información para mitigarlos y minimizar el impacto en la institución de educación superior.
- Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información.
- Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos de TI y de seguridad de la información de la IES.

Objetivos: Conformidad

- Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas vigentes internas de la institución de educación superior, así como, los estándares internacionales de gestión de seguridad de la información.
- Establecer procesos de toma de decisiones en relación con la seguridad de la información.
- Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información.
- Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.

Objetivos: Desempeño

- Definir indicadores de rendimiento de los procesos de integración entre la arquitectura de seguridad de la información y los servicios de TI.
- Garantizar la confiabilidad, integridad y disponibilidad de los activos de información a través de los servicios TI y los procesos de gobierno de seguridad de la información.
- Conocer los riesgos asociados a las vulnerabilidades y amenazas de los activos de información para mitigarlos y minimizar el impacto en la institución de educación superior.
- Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos de TI y de seguridad de la información de la IES.

Objetivos: Comportamiento Humano

- Determinar los comportamientos éticos que deben tener los docentes, estudiantes, personal administrativo y directivo en relación con los activos de información de la cual son custodios, antes, durante y después de su permanencia en la IES o en el caso de cambio de cargo.
- Disponer del personal adecuado y con la formación respectiva para la gestión eficiente de los procesos de gobierno de seguridad de la información en la IES
- Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información.
- Monitorear el comportamiento ético de los docentes, estudiantes, personal administrativo y directivo de la IES respecto a la manipulación de los activos de información de los que son custodios.

Objetivos: Responsabilidad

- Conformar una estructura de dirección y modelo de toma de decisiones alineados a las estrategias de seguridad de la información.
- Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas internas vigentes de la institución de educación superior, así como, los estándares internacionales de gestión de seguridad de la información.
- Establecer procesos de toma de decisiones en relación con la seguridad de la información basados en el análisis de riesgos.
- Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información.

Proceso del MoGSIIES

El gobierno corporativo de la institución de educación superior debe llevar a cabo cada una de las actividades de los procesos para dirigir, evaluar, monitorear, comunicar y asegurar la seguridad de la información que se produce como resultado de las funciones sustantivas y la gestión administrativa.

También, se debe asegurar que la gobernanza de seguridad sea alcanzada en todos los niveles de la institución de educación superior. La figura 2 muestra la relación entre el proceso de seguridad de la información, las funciones sustantivas y los elementos indispensables de la organización.

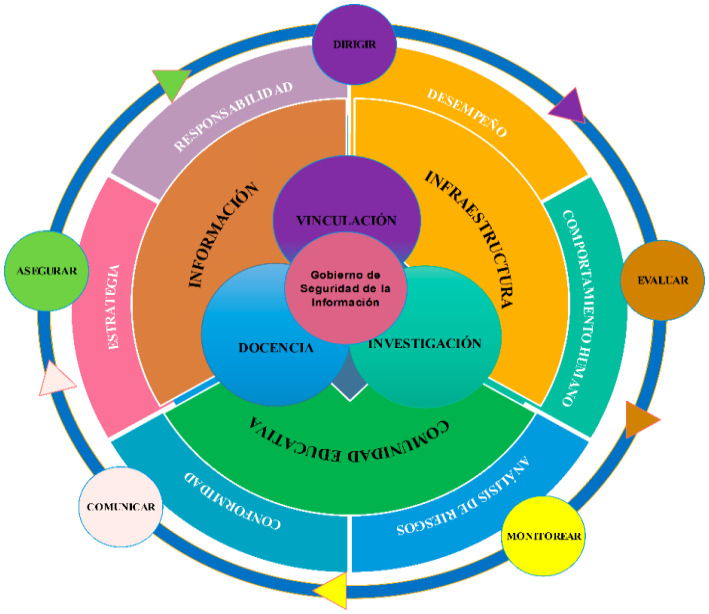

Figura 2. Relación de las funciones sustantivas con el gobierno de seguridad de la información

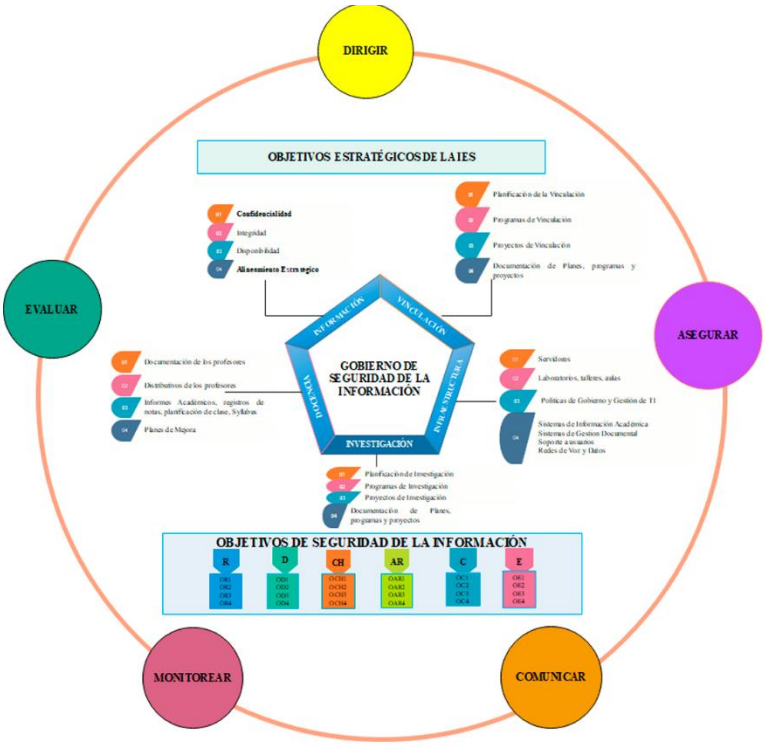

Figura 3. Proceso del gobierno de seguridad de la información

Evaluar las estrategias, principios y acciones que las IES deben tomar en cuenta sobre el gobierno de seguridad de la información. Los directivos deberán examinar y tomar las decisiones sobre el estado actual y futuro de la seguridad de la información. La evaluación deberá ser continua y tomar en cuenta las necesidades presentes y futuras para lograr los niveles de seguridad de la información, para así, mantener las ventajas competitivas y alcanzar los objetivos estratégicos organizacionales y de TI.

El gobierno corporativo y la comisión de seguridad de la información de la institución de educación superior deben:

- Garantizar que los principios y objetivos del gobierno de seguridad de la información se encuentren alineados a los objetivos estratégicos institucionales.
- Medir los desempeños de las políticas y procedimientos de seguridad de la información.
- Presentar y difundir en la comunidad educativa las acciones definidas en el marco del gobierno de seguridad de la información de la institución.

Dirigir está enfocado a la preparación y a la implementación de planes y políticas que permitan garantizar la seguridad de la información de los activos de la IES y la ejecución de las estrategias y acciones planificadas. Las acciones implementadas deberán asegurar la integridad y confiabilidad de la información de las operaciones de la IES.

Las políticas deberán garantizar los niveles de seguridad de la información según los planes establecidos considerando el impacto en las estrategias, procesos y procedimientos organizacionales de las IES. También deben promover una cultura del gobierno de seguridad de la información requiriendo de los directores de TI informes periódicos y sobre todo respetando los

principios del MoGSIIES.

Para llevar a cabo el proceso de ***dirigir*** es necesario que se realicen las siguientes acciones:

- Aprobar la estrategia para la implementación del gobierno de seguridad de la información.
- Conformar un comité de gobierno de seguridad de la información, quien redactará las políticas y procedimientos que respondan a los objetivos estratégicos institucionales.
- Asignar los recursos adecuados para el desarrollo e implementación del gobierno de seguridad de la información.
- Promover una cultura de seguridad de la información en todos los actores de la comunidad educativa para el tratamiento de la información que es resultado de los procesos de la institución educación superior.

Monitorear mediante un sistema de medida, las políticas, procedimientos y planes de seguridad de la información para controlar su rendimiento a través de un seguimiento y monitoreo de los indicadores de seguridad establecidos.

Para permitir que el proceso de monitoreo se cumpla es importante considerar:

- Selección de las métricas para el monitoreo de los niveles de madurez de gobierno seguridad de la información desde la perspectiva de los procesos estratégicos de la institución de educación superior.
- Alertar a la comunidad educativa y al gobierno corporativo de la institución de educación superior sobre las actividades que pueden ser afectadas por la mala aplicación de las políticas, procesos y procedimientos del gobierno de seguridad de la información.
- Proporcionar los resultados de la medición del desempeño de las

actividades relacionadas con el gobierno de seguridad de la información para establecer su impacto en los activos de información de la institución.

- Considerar las estrategias organizacionales, regulaciones y afectaciones sobre la seguridad de la información de toda la institución de educación superior.

Comunicar es el proceso bidireccional mediante el cual el gobierno corporativo de la IES y las partes interesadas intercambian información sobre la seguridad de la información de acuerdo con sus necesidades específicas. Es importante que se genere una cultura de comunicación en todo momento para evitar que se distorsione la ejecución de las políticas, procesos y procedimientos de seguridad de la información por parte de todos los actores involucrados.

La comunicación es uno de los procesos más relevantes del modelo de gobierno de seguridad de la información. Es por ello, que se debe:

- Capacitar a toda la comunidad educativa sobre las medidas tomadas en relación con el gobierno de seguridad de la información para apoyar las directrices y decisiones tomadas por el gobierno corporativos de la institución.
- Asesorar al gobierno corporativo de la institución de educación superior en todos los asuntos concernientes al gobierno de seguridad de la información.
- Informar a toda la comunidad educativa sobre el nivel de seguridad de la información en cada una de las actividades encomendadas de acuerdo con las funciones sustantivas.
- Generar una cultura de comunicación en todo momento para evitar que se distorsione la ejecución de las políticas, procesos y procedimientos de seguridad de la información por parte de todos los integrantes de la comunidad educativa.

Asegurar es el proceso de gobierno mediante el cual se audita, revisa o certifica las actividades de gobierno, con el fin de alcanzar el nivel deseado de seguridad de la información.

Para permitir que el proceso de monitoreo se cumpla es importante considerar:

- Presentar al gobierno corporativo las normas bajo las cuales se debe alcanzar una certificación en los procesos de seguridad de la información y brindar todo el apoyo respectivo para que se lleven a cabo.
- Enunciar recomendaciones objetivas sobre el nivel de cumplimiento de la seguridad de la información y la responsabilidad de los actores que son parte de las funciones sustantivas.

ANEXO 2. INSTRUMENTO DE VALIDACIÓN DE EXPERTOS

ENCUESTA DE OPINIÓN
MODELO DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

Estimado/a experto/a

Me es grato dirigirme a usted, para expresarle un saludo cordial y solicitarle de manera especial su participación en calidad de experto evaluador, dentro del proceso de validación de expertos cuya finalidad es darle el rigor científico a la tesis "**Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior**".

Seguro de contar con su contingente y apelando a su trayectoria y reconocimiento profesional en el área, me despido.

Atentamente

Ingeniero Hugo Heredia Mayorga, Mg

OBJETIVO

Conocer la opinión de expertos con respecto al Modelo de Gobierno de Seguridad de la Información propuesto para las Instituciones de Educación Superior del Ecuador a través de criterios de claridad, coherentes y relevantes.

Su evaluación deberá ser realizada en función de los siguientes indicadores según corresponda.

CATEGORÍA	DESCRIPCIÓN	PONDERACIÓN	INDICADOR
Claridad	Los elementos del modelo de seguridad de la información se comprenden fácilmente, es decir, su sintaxis y semántica son adecuadas	1 no cumple	Las conceptualizaciones y descripciones de los elementos del modelo de seguridad de la información no son claros, ni entendibles.
		2 cumple parcialmente	Los elementos del modelo de seguridad de la información requieren bastantes modificaciones o una modificación profunda respecto al uso de las palabras de acuerdo con su significado o por ordenación de estas.
		3 cumple Moderadamente	Los elementos del modelo de seguridad de la información requieren de una modificación muy específica en la terminología utilizada.
		4 cumple Totalmente	Las conceptualizaciones y descripciones de los elementos del modelo de seguridad de la información son claros, su semántica y sintaxis son adecuadas.
Coherencia	Los elementos del modelo de seguridad de la información tienen relación lógica entre sí y están articulados a las funciones de docencia, investigación y vinculación.	1 no cumple	Los elementos del modelo de seguridad de la información no tienen relación lógica con los procesos de gobernanza.
		2 cumple parcialmente	Los elementos del modelo de seguridad de la información tienen una relación tangencial con los procesos de gobernanza.
		3 cumple Moderadamente	Los elementos del modelo de seguridad de la información tienen una relación moderada con los procesos de gobernanza.
		4 cumple Totalmente	Los elementos del modelo de seguridad de la información se encuentran completamente relacionados con los procesos de gobernanza.
Relevancia	Los elementos del modelo de seguridad de la información son esenciales o importantes.	1 no cumple	Los elementos del modelo de seguridad de la información pueden ser eliminados sin que se vea afectada la medición de los procesos de gobernanza.
		2 cumple parcialmente	Algunos de los elementos del modelo de seguridad de la información tienen alguna relevancia.
		3 cumple Moderadamente	Todos los elementos del modelo de gobierno de seguridad de la información son relativamente importantes.
		4 cumple Totalmente	Todos los elementos del modelo de gobierno de seguridad de la información son muy relevantes.

DIMENSIÓN 1: PRINCIPIOS

PRINCIPIOS	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Responsabilidad				
Desempeño				
Análisis de Riesgos				
Comportamiento Humano				
Conformidad				
Estrategia				

DIMENSIÓN 2: OBJETIVOS

PRINCIPIO ESTRATEGIA	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Determinar cuál es la estrategia de seguridad de la información para toda la organización bajo un enfoque basado en riesgos.				
Alinear la estrategia institucional y de TI con la estrategia de seguridad de la información.				
Disponer de una estructura de dirección y modelo de toma de decisiones alineados a las estrategias de seguridad de la información				
Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas vigentes internas de la institución de educación superior, así como de los estándares internacionales de gestión de seguridad de la información				

PRINCIPIO ANÁLISIS DE RIESGOS	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Definir la arquitectura de seguridad de la información que incluya procesos y la integración con los sistemas				
Conocer los riesgos asociados, las vulnerabilidades y amenazas de los activos de información para mitigarlos y minimizar el impacto en la institución de educación superior.				
Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información				
Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos de TI y de seguridad de la información de la IES.				

PRINCIPIO CONFORMIDAD	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas vigentes internas de la institución de educación superior, así como de los estándares internacionales de gestión de seguridad de la información.				
Establecer procesos de toma de decisiones en relación con la seguridad de la información basado en el análisis de riesgos				
Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información				
Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información				

PRINCIPIO DESEMPEÑO	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Definir indicadores de rendimiento de los procesos de integración entre la arquitectura de seguridad de la información y los servicio de TI.				
Garantizar la confiabilidad, integridad y disponibilidad de los activos de información a través de los servicios TI y los procesos de gobierno de seguridad de la información.				
Conocer los riesgos asociados, las vulnerabilidades y amenazas de los activos de información para mitigarlos y minimizar el impacto en la institución de educación superior.				
Disponer de las herramientas tecnológicas necesarias para alcanzar los objetivos estratégicos de TI y de seguridad de la información de la IES.				

PRINCIPIO COMPORTAMIENTO HUMANO	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Determinar los comportamientos éticos que deben tener los docentes, estudiantes, personal administrativo y directivo antes, durante y después de su permanencia en el IES o cambio de cargo sobre los activos de información del cual son custodios.				
Disponer del personal adecuado y con la formación respectiva para la gestión eficiente de los procesos de gobierno de seguridad de la información en la IES.				
Integrar los valores organizacionales dentro de los comportamientos éticos para alcanzar las estrategias de seguridad de la información.				
Monitorear el comportamiento ético de los docentes, estudiantes, personal administrativo y directivo de la IES en manipulación de los activos de información que son custodios				

PRINCIPIO RESPONSABILIDAD	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Conformar una estructura de dirección y modelo de toma de decisiones alineados a las estrategias de seguridad de la información				
Establecer políticas y procedimientos para gestionar la seguridad de la información considerando los reglamentos y normativas vigentes internas de la institución de educación superior, así como de los estándares internacionales de gestión de seguridad de la información				
Establecer procesos de toma de decisiones en relación con la seguridad de la información basado en el análisis de riesgos.				
Intercambiar experiencias y colaborar con otras IES en temas relacionados con la seguridad de la información				

DIMENSIÓN 3: PROCESO

PROCESO	EVALUACIÓN			
	Claridad	Coherencia	Relevancia	Observación
Dirigir				
Evaluar				
Monitorear				
Comunicar				
Asegurar				

DIMENSIÓN 4: MODELO DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

La estructura del Modelo de Gobierno de Seguridad de la Información para Instituciones de Educación Superior en su conjunto, sus principios, objetivos, procesos y criterios de medición es adecuada para implantar un gobierno de Seguridad de la Información en las Instituciones de Educación superior.	**EVALUACIÓN**			
	1	**2**	**3**	**4**
CLARIDAD				
COHERENCIA				
RELEVANCIA				

Observaciones y recomendaciones

Identificación del experto

Nombres y apellidos	
Grado Académico	
Lugar de trabajo	
e-mail	
Fecha de la validación (día, mes y año)**:**	

Muchas gracias por su valiosa contribución a la validación de este modelo.

ANEXO 3. TABULACIÓN DE VALORACIÓN DE EXPERTOS

Valoración de los expertos dimensión principios

Principios	Claridad							Coherencia							Relevancia						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
Estrategia	4	4	3	4	4	4	4	4	4	4	4	3	3	3	4	4	3	4	3	4	4
Análisis de Riesgos	4	4	4	4	3	4	3	4	3	4	3	3	4	4	4	4	3	3	4	4	4
Conformidad	3	4	3	4	3	4	3	4	4	4	3	4	3	4	4	3	4	3	3	4	4
Desempeño	4	4	3	4	4	4	4	3	4	3	4	3	3	4	4	4	3	4	3	3	3
Comportamiento Humano	3	3	4	3	4	3	4	4	4	3	4	3	4	3	4	4	3	4	4	3	3
Responsabilidad	2	3	3	4	3	4	4	4	4	4	3	3	3	4	3	3	3	4	3	4	4

Valoración de los expertos dimensión objetivos

Objetivos	Claridad							Coherencia							Relevancia						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
Objetivo 1.	4	4	3	4	4	4	3	4	3	4	3	4	3	4	4	3	4	4	4	3	4
Objetivo 2.	4	4	4	4	3	3	3	2	4	3	4	4	3	4	4	3	3	3	4	3	3
Objetivo 3	4	3	4	3	4	4	4	3	4	4	3	4	4	4	4	3	4	4	4	3	4
Objetivo 4	4	4	3	4	3	4	4	4	3	4	4	4	3	3	4	4	4	3	4	4	4
Objetivo 5	4	3	4	4	3	3	4	4	4	4	4	4	4	3	4	3	4	4	3	4	3
Objetivo 6	4	4	3	4	3	4	3	4	4	3	4	4	4	3	4	4	4	4	3	4	4
Objetivo 7	3	4	3	4	4	3	4	4	3	4	4	4	3	4	4	3	4	3	4	4	4
Objetivo 8	4	4	4	3	3	4	3	2	4	4	3	4	3	3	4	4	3	4	4	3	4
Objetivo 9	3	4	4	3	4	4	3	4	4	4	4	4	3	3	4	4	4	4	4	4	3
Objetivo 10	4	4	4	4	3	3	4	4	4	4	4	3	4	4	4	4	3	4	4	3	4
Objetivo 11	4	3	3	4	4	4	3	4	3	4	4	3	4	3	4	4	4	3	4	4	3
Objetivo 12	4	4	4	4	4	3	3	4	3	4	4	4	4	4	4	4	4	4	4	3	3
Objetivo 13	4	4	3	4	3	4	4	4	4	4	4	4	3	4	4	4	4	3	4	4	4
Objetivo 14	4	3	4	4	3	4	3	4	3	3	4	4	4	4	4	3	3	3	4	3	4
Objetivo 15	4	3	4	3	4	4	3	4	4	3	4	3	4	3	4	4	4	4	4	3	4
Objetivo 16	4	4	4	3	4	3	4	4	3	4	4	4	4	4	4	4	4	3	4	4	3

Valoración de los expertos dimensión procesos

Proceso	Claridad							Coherencia							Relevancia						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
Dirigir	4	4	4	4	4	4	4	4	4	3	3	4	4	4	4	4	4	3	3	4	4
Evaluar	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
Monitorear	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
Comunicar	4	4	4	4	4	4	4	4	3	4	4	4	3	3	4	4	3	4	4	4	3
Asegurar	4	4	4	4	4	4	4	4	4	3	4	3	3	4	4	4	4	3	3	3	4

Cálculo de los coeficientes v de Aiken para los principios del MoGSIIES

Principios		P1	P2	P3	P4	P5	P6	v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	**E1**	1,00	1,00	0,67	1,00	0,67	0,33	0,78	0,87	0,86
	E2	1,00	1,00	1,00	1,00	0,67	0,67	0,89		
	E3	0,67	1,00	0,67	0,67	1,00	0,67	0,78		
	E4	1,00	1,00	1,00	1,00	0,67	1,00	0,94		
	E5	1,00	0,67	0,67	1,00	1,00	0,67	0,83		
	E6	1,00	1,00	1,00	1,00	0,67	1,00	0,94		
	E7	1,00	0,67	0,67	1,00	1,00	1,00	0,89		
Coherencia	**E1**	1,00	1,00	1,00	0,67	1,00	1,00	0,94	0,86	
	E2	1,00	0,67	1,00	1,00	1,00	1,00	0,94		
	E3	1,00	1,00	1,00	0,67	0,67	1,00	0,89		
	E4	1,00	0,67	0,67	1,00	1,00	0,67	0,83		
	E5	0,67	0,67	1,00	0,67	0,67	0,67	0,72		
	E6	0,67	1,00	0,67	0,67	1,00	0,67	0,78		
	E7	0,67	1,00	1,00	1,00	0,67	1,00	0,89		
Relevancia	**E1**	1,00	1,00	1,00	1,00	1,00	0,67	0,94	0,86	
	E2	1,00	1,00	0,67	1,00	1,00	0,67	0,89		
	E3	0,67	0,67	1,00	0,67	0,67	0,67	0,72		
	E4	1,00	0,67	0,67	1,00	1,00	1,00	0,89		
	E5	0,67	1,00	0,67	0,67	1,00	0,67	0,78		
	E6	1,00	1,00	1,00	0,67	0,67	1,00	0,89		
	E7	1,00	1,00	1,00	0,67	0,67	1,00	0,89		

Cálculo de los coeficientes v de Aiken para los objetivos del MoGSIIES

Objetivos		Obj.1	Obj.2	Obj.3	Obj.4	Obj.5	Obj.6	Obj.7	Obj.8	Obj.9	Obj.10	Obj.11	Obj.12	Obj.13	Obj.14	Obj.15	Obj.16	v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	E1	1,00	1,00	1,00	1,00	1,00	1,00	0,67	1,00	0,67	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,96		
	E2	1,00	1,00	0,67	1,00	0,67	1,00	1,00	1,00	1,00	1,00	0,67	1,00	1,00	0,67	0,67	1,00	0,90		
	E3	0,67	1,00	1,00	0,67	1,00	0,67	0,67	1,00	1,00	1,00	0,67	1,00	0,67	1,00	1,00	1,00	0,88		
	E4	1,00	1,00	0,67	1,00	1,00	1,00	1,00	0,67	0,67	1,00	1,00	1,00	1,00	1,00	0,67	0,67	0,90		
	E5	1,00	0,67	1,00	0,67	0,67	0,67	1,00	0,67	1,00	0,67	1,00	1,00	0,67	0,67	1,00	1,00	0,83		
	E6	1,00	0,67	1,00	1,00	0,67	1,00	0,67	1,00	1,00	0,67	1,00	0,67	1,00	1,00	1,00	0,67	0,88		
	E7	0,67	0,67	1,00	1,00	1,00	0,67	1,00	0,67	0,67	1,00	0,67	0,67	1,00	0,67	0,67	1,00	0,81	0,88	
Coherencia	E1	1,00	0,33	0,67	1,00	1,00	1,00	1,00	0,33	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,90		
	E2	0,67	1,00	1,00	0,67	1,00	1,00	0,67	1,00	1,00	1,00	0,67	0,67	1,00	0,67	1,00	0,67	0,85		
	E3	1,00	0,67	1,00	1,00	1,00	0,67	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,67	0,67	1,00	0,92		
	E4	0,67	1,00	0,67	1,00	1,00	1,00	1,00	0,67	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,94		
	E5	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,67	0,67	1,00	1,00	1,00	0,67	1,00	0,94		
	E6	0,67	0,67	1,00	0,67	1,00	1,00	0,67	0,67	0,67	1,00	1,00	1,00	0,67	1,00	1,00	1,00	0,85		
	E7	1,00	1,00	1,00	0,67	0,67	0,67	1,00	0,67	0,67	1,00	0,67	1,00	1,00	1,00	0,67	1,00	0,85	0,89	
Relevancia	E1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00		
	E2	0,67	0,67	0,67	1,00	0,67	1,00	0,67	1,00	1,00	1,00	1,00	1,00	1,00	0,67	1,00	1,00	0,88		
	E3	1,00	0,67	1,00	1,00	1,00	1,00	1,00	0,67	1,00	0,67	1,00	1,00	1,00	0,67	1,00	1,00	0,92		
	E4	1,00	0,67	1,00	0,67	1,00	1,00	0,67	1,00	1,00	1,00	0,67	1,00	0,67	0,67	1,00	0,67	0,85		
	E5	1,00	1,00	1,00	1,00	0,67	0,67	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,96		
	E6	0,67	0,67	0,67	1,00	1,00	1,00	1,00	0,67	1,00	0,67	1,00	0,67	1,00	0,67	0,67	1,00	0,83		
	E7	1,00	0,67	1,00	1,00	0,67	1,00	1,00	1,00	0,67	1,00	0,67	0,67	1,00	1,00	1,00	0,67	0,88	0,90	0,89

Cálculo de los coeficientes v de Aiken para el proceso del MoGSIIES

Proceso		Dirigir	Evaluar	Monitorear	Comunicar	Asegurar	v de Aiken por Experto	v de Aiken por Criterio	v de Aiken por Dimensión
Claridad	E1	1,00	1,00	0,33	1,00	1,00	0,87		
	E2	1,00	1,00	1,00	1,00	1,00	1,00		
	E3	1,00	1,00	1,00	1,00	1,00	1,00		
	E4	1,00	1,00	1,00	1,00	1,00	1,00		
	E5	1,00	1,00	1,00	1,00	1,00	1,00		
	E6	1,00	1,00	1,00	1,00	1,00	1,00		
	E7	1,00	1,00	1,00	1,00	1,00	1,00	0,98	
Coherencia	E1	1,00	1,00	1,00	1,00	1,00	1,00		
	E2	1,00	1,00	1,00	0,67	1,00	0,93		
	E3	0,67	1,00	1,00	1,00	0,67	0,87		
	E4	0,67	1,00	1,00	1,00	1,00	0,93		
	E5	1,00	1,00	1,00	1,00	0,67	0,93		
	E6	1,00	1,00	1,00	0,67	0,67	0,87		
	E7	1,00	1,00	1,00	0,67	1,00	0,93	0,92	
Relevancia	E1	1,00	1,00	1,00	1,00	1,00	1,00		
	E2	1,00	1,00	1,00	1,00	1,00	1,00		
	E3	1,00	1,00	1,00	0,67	1,00	0,93		
	E4	0,67	1,00	1,00	1,00	0,67	0,87		
	E5	0,67	1,00	1,00	1,00	0,67	0,87		
	E6	1,00	1,00	0,67	1,00	0,67	0,87		
	E7	1,00	0,67	0,67	0,67	1,00	0,80	0,90	0,94

ANEXO 4. ENCUESTA DE DIAGNÓSTICO

Objetivo: Conocer el estado actual de gobierno de seguridad de la información.

Indicaciones Generales: En cada una de las siguientes preguntas debe marcar con una X según corresponda a su criterio y apreciación, cada pregunta puede ser valorada bajo tres opciones Si: si se considera que la institución si cumple con la interrogante, NO: si no cumple, y No Sé (NS) si no lo sabe. Es importante que las interrogantes planteadas sean contestadas de la manera más honesta con el fin de obtener los resultados esperados.

	PREGUNTAS	SI	NO	(NS)
REM1	¿La institución de educación superior asigna responsabilidades relacionadas con el gobierno de seguridad de la información a su cuerpo directivo?			
REM2	¿La institución de educación superior asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos?			
REM4	¿El cuerpo directivo de la institución de educación superior asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas para hacerlo?			
RDM1	¿El cuerpo directivo encargado del gobierno de seguridad de la información supervisan los diferentes niveles de gestión de seguridad de la información?			
RDM2	¿Los responsables o directores de tecnologías de la información de las instituciones de educación superior toman las decisiones sobre seguridad de la información bajo aprobación del cuerpo directivo?			
RDM4	¿El cuerpo directivo de la institución de educación superior se preocupan de que se planifique de manera adecuada los procesos de seguridad de la información??			
RDM5	¿Comunican los directivos de la institución de educación superior las decisiones que se toma sobre seguridad de la información a docentes, estudiantes y personal administrativo de la institución?			
RDM6	¿Los directivos de las instituciones de educación superior reciben información sobre las estrategias, políticas y procedimiento de seguridad de la información para apoyar su toma de decisiones?			
RMM1	¿Se realiza un seguimiento a los roles y responsabilidades asignadas para garantizar que la ejecución de los procesos relacionadas con la seguridad de la información se realice de manera correcta?			
RMM2	¿Docentes, estudiantes y personal académico comprenden las responsabilidades asignadas por el cuerpo directivo de la institución de educación superior en materia de seguridad de la información?			
EEM1	¿La institución de educación superior dispone de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de Gobierno de seguridad de la Información??			
EEM2	¿El cuerpo directivo de la institución de educación superior supervisa las actividades de seguridad de la información de manera alineada con los objetivos estratégicos de la institución?			
EEM3	¿Analiza el cuerpo directivo los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo institucional?			
EDM1	¿El cuerpo directivo de la institución de educación superior diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información?			
EDM2	¿La institución de educación superior realiza una planificación de la seguridad de la información a pequeño, medio y largo plazo?			

EDM3	¿La institución de educación superior informa a docentes, estudiantes, personal administrativo sobre los elementos estructurales de la planificación de la seguridad de la información?			
EMM1	¿Se lleva a cabo un seguimiento de la ejecución de la planificación de la seguridad de la información?			
EMM3	¿Se comprueba si las políticas de seguridad de la información se están aplicando en todas las unidades administrativas y de gestión de la institución?			
DEM2	¿Los gestores de tecnologías de la información toman las principales decisiones sobre la articulación de la seguridad de la información y los procesos estratégicos de la institución			
DEM3	¿Los directivos de la institución de educación superior comprenden cuales son los riegos que tiene sobre los activos de información y toman de decisiones relacionadas con el desempeño los niveles de seguridad de la información?			
DDM1	¿La institución de educación superior establece indicadores para medir los niveles de seguridad de la información de la institución?			
DMM3	¿Hay políticas y normas internas establecidas para los aspectos más importantes de seguridad de la información para los procesos institucionales?			
CEM1	¿El cuerpo directivo de la institución de educación superior conoce la normativa y el modelo de gobierno de seguridad de la información?			
CEM2	¿El cuerpo directivo de las instituciones de educación superior conocen los principales estándares de gobierno de seguridad de la información?			
CDM1	¿Demuestran docentes, estudiantes y personal administrativo un comportamiento cumpliendo lo establecido en las normas y estándares de gobierno de seguridad de la información?			
CDM2	¿Conocen los estudiantes, docentes y administrativos cuales son las políticas relacionadas con la seguridad de la información de la institución gracias a los procesos de comunicación llevados a cabo?			
CDM3	¿Se han diseñado normas y procedimientos internos, basados en las políticas, cuyo objetivo es alcanzar una adecuada gestión del gobierno de seguridad de la información?			
CMM2	¿La institución de educación superior comprueba bajo indicadores el cumplimiento de las políticas, normas y estándares del gobierno de seguridad de la información?			
HEM4	¿El cuerpo directivo de la institución de educación superior es consciente de los riesgos, amenazas y vulnerabilidad al cual están sujetos los activos de información debido a que no existen procesos de gobernanza de seguridad de la información?			
HDM2	¿La institución de educación superior informa a docentes, estudiantes y personal administrativo de los procesos y procedimientos de gobernanza de seguridad de la información?			

¡¡Gracias por su colaboración!!