DISEÑO DE UNA METODOLOGÍA PARA AUDITAR LA SEGURIDAD DE LA INFORMACIÓN EN PRODUCTOS DE SOFTWARE ORIENTADOS A SERVICIOS DE GESTIÓN E INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR

ARELIS GÓMEZ NOVA

Universidad Autónoma de Bucaramanga
Facultad de Ingeniería de Sistemas
Maestría en Gestión, Aplicación y Desarrollo de Software
Bucaramanga
2017

DISEÑO DE UNA METODOLOGÍA PARA AUDITAR LA SEGURIDAD DE LA INFORMACIÓN EN PRODUCTOS DE SOFTWARE ORIENTADOS A SERVICIOS DE GESTIÓN E INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR

ARELIS GÓMEZ NOVA

TESIS PARA OPTAR AL TÍTULO:
Magister en Gestión, Aplicación y Desarrollo de Software

DIRIGIDO POR:
Director: Prof. REINALDO NICOLAS MAYOL ARNAO, MSc,PhDc.

Universidad Autónoma de Bucaramanga
Facultad de Ingeniería de Sistemas
Maestría en Gestión, Aplicación y Desarrollo de Software
Bucaramanga
2017

Nota de Aceptación:

Firma Presidente del Jurado.

Firma del Jurado.

Firma del Jurado.

Bucaramanga, Enero 13 de 2017

DEDICATORIA

A Dios, el motor que dirige mi existencia con amor y me enseña a encarar cada vivencia con dignidad y carácter para no desfallecer en el intento.

A mis padres, hermanos y sobrinos por su infinito amor, ejemplo y paciencia. Compañeros de vida, que guían mis pasos con la luz que irradia el verdadero e incondicional amor.

AGRADECIMIENTOS

A Dios, que inspira mi vida y patrocina el emprendimiento de cada proyecto, asegurándose de proporcionar los elementos necesarios para culminarlos con éxito.

A mis padres Emiliana y Esteban, por ser mi orientación y por la constancia en amor infinito, bondad, respeto y generosidad. Los amo y admiro porque han dejado sus sueños y proyectos para que en su lugar se cumplan los míos.

A mis hermanos Robinson, Sandra Milena y Yuli Fernanda, y mis sobrinos Laura Jiseth Camila, Mariam Sofia y Juan Esteban; por su inmenso amor y ejemplo. Son la razón para esforzarme a ser mejor persona cada día.

A mi Director Reinaldo Mayol Arnao, por su valiosa y acertada orientación; por su tiempo, dedicación y paciencia; por sus notables aportes, comentarios, correcciones y sugerencias, que fueron un pilar fundamental para el desarrollo mi tesis.

A la Universidad Pontificia Bolivariana, seccional Bucaramanga, que ha sido mi segundo hogar y centro de crecimiento personal y profesional, mi eterno agradecimiento por acogerme en la gran familia Bolivariana. El apoyo de sus directivos ha sido determinante para alcanzar mí éxito profesional.

A mi equipo de trabajo del CTIC, compañeros permanentes de construcción con aciertos y desaciertos. Han sido guía y aprendizaje durante estos años de trabajo, motivando siempre mi formación y aprendizaje.

A mi amigo Reinaldo Mayol Arnao, por su amistad y acompañamiento permanente, sin su credibilidad y fe en mí, difícilmente hubiese sido posible.

A mi gran lista de amigos, compañeros permanentes de batallas y aventuras; testigos de alegrías y adversidades. Confidentes incondicionales que han justificado mi existir y han brindado felicidad a mi vida.

A todos y cada de las personas que acompañan mi diario vivir, mi eterno agradecimiento por aportar lo mejor de cada uno para qué mis sueños y metas se conviertan en exitosas realidades.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE GRÁFICAS

TABLAS

TABLA DE ANEXOS

SIGLAS

IES	Instituciones de Educación Superior
SI	Sistema de Información
SGSI	Sistema de Gestión de Seguridad de la Información
SIT	Sistemas de Información y Tecnología
TIC	Tecnologías de Información y Comunicación
MINEDUACIÓN	Ministerio de Educación Nacional
ISACA	Information System Audit and Control Association
SNIES	Sistema Nacional de Educación Superior
SACES	Sistema de Información para el Aseguramiento de la Calidad
SPADIES	Sistema de Prevención y Análisis de la Deserción en las Instituciones de Educación Superior
CONPES	Consejo Nacional de Política Económica y Social
ICONTEC	Instituto Colombiano de Normas Técnicas y Certificación
COBIT	Control Objectives for Information and Related Technology
IT GI	IT Governance Institute
CCTA	Centro de Informática y la Agencia Nacional de Telecomunicaciones
OCTAVE	Operationally Critical Threats Assets and Vulnerability Evaluation
ISO	Organization for Standardization
NTC	Norma Técnica Colombia
OEA	Organización de Estados Americanos
ACIS	Asociación Colombiana de Ingenieros de Sistemas
CISO	Chief information security officer
CIO	Chief Information Officer
MINTIC	Ministerio de Tecnologías de la Información y Comunicaciones
colCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CCOC	Comando Conjunto Cibernético
CCP	El Centro Cibernético Policial
CSIRT PONAL	El Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional
NIST	National Institute of Standards and Technology
AENOR	La Asociación Española de Normalización y Certificación
OWL	Ontology Web Language
BCP	Business Continuity Plan
IRTs	Respuesta a Incidentes
ISRM	Information Security Risk Management
IEC	Comisión Electrotécnica Internacional
ACIS	Asociación Colombiana de ingenieros de Sistema

RESUMEN

La información cada vez toma mayor valor para las organizaciones, sin importar su razón de ser, ni su sector de desempeño; siendo situada como un activo intangible que proporciona ventaja competitiva. Para su adecuado tratamiento, se debe acudir a herramientas tecnológicas, que faciliten el procesamiento de datos, la generación de informes y la toma de decisiones. El uso tecnológico ha transformado el desempeño y desarrollo de las empresas; en consecuencia, también se ha convertido en un medio para ampliar el margen de riesgos informáticos; siendo un factor en ascenso por el auge de la era digital e Internet. El planteamiento de la propuesta, fue el resultado de la identificación de la carencia de procesos de auditoria en seguridad, para sistemas orientados a la gestión e información académica en la Universidad Pontificia Bolivariana, Seccional Bucaramanga.

Con base en lo expuesto, esta investigación tuvo como propósito contribuir a la detección de amenazas y vulnerabilidades para mitigar el riesgo informático, mediante el diseño de una metodología para auditar la inclusión y calidad de los criterios de seguridad, en la prestación de servicios académicos a través de sistemas de información. En la estructura de la metodología, se definieron tres dimensiones, consideradas relevantes para desarrollar un programa de auditoria. Para cada dimensión, se estableció un criterio, sujeto de evaluación mediante la verificación de la existencia de controles de seguridad. Los controles estuvieron definidos por un listado de requisitos, con el propósito de validar su implementación.

Para verificar la metodología, se aplicó los instrumentos de medición diseñados, en una institución de educación superior, se realizó análisis de los resultados, se emitió el concepto técnico de los hallazgos detectados, las recomendaciones y se verificó la completitud y validez del diseño de la metodología.

GLOSARIO

A continuación, se describirá los principales términos, que han sido utilizados durante el desarrollo de las tesis; con el propósito que los lectores se familiaricen y adquieran mayor compresión del trabajo. Los términos que se incluyen corresponden a definiciones extraídas del libro COBIT 5, de la norma ISO 27000,

- **COBIT 5:** Conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT); usado actualmente solo como un acrónimo en su quinta revisión. Un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información (TI) que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas de TI relacionadas. COBIT describe cinco principios y siete facilitadores que dan soporte a las empresas en el desarrollo, implementación y mejora continua y supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI.
- **Política**: Declaración de la gerencia de lo que debe hacerse para efectuar el control. Una política sirve como base para la implementación de sus procedimientos.

- **Continuidad del Negocio:** Evitar, mitigar y recuperarse de una interrupción. Se puede usar en este contexto también los términos “planificación de la restauración del negocio”, “planificación para recuperación de desastres” y “planificación de las contingencias”; se enfocan en los aspectos de la recuperación dentro de la continuidad y, por esa razón, el factor “resiliencia” también debería ser considerado.

- **Cultura:** Un patrón de comportamientos, creencias, hipótesis, actitudes y formas de hacer las cosas.

- **Estructura Organizativa:** Algo (tangible o intangible) que ayuda a la realización de un gobierno efectivo.

- **Gestión de Riesgo:** Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa.

- **Gobierno:** El marco, principios y políticas, estructuras, procesos y prácticas, información, habilidades, cultura, ética y comportamiento que establecen la dirección y verifican que cumplimiento y rendimiento de una empresa están alineados con el propósito general y los objetivos definidos. El gobierno define quién tiene la responsabilidad última de que las cosas se hagan, la responsabilidad y la capacidad de decisión (entre otros elementos).

- **Gobierno de la empresa:** Un conjunto de responsabilidades y prácticas ejercidas por el Consejo de Administración y los gestores ejecutivos con el objetivo de dotar de dirección estratégica, asegurando que los objetivos son conseguidos, verificando que el riesgo es gestionado de forma apropiada y verificando que los recursos de la empresa son usados de forma responsable. También podría referirse a una visión de gobierno que ve el conjunto de la empresa; la visión más alta de gobierno con la que todas las demás deben alinearse.

- **Gobierno de TI empresarial:** Un activo que, como cualquier otro activo importante de negocio, es esencial para el negocio de una empresa. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, transmitido por correo o de forma electrónica, mostrado en películas o hablado durante una conversación.

- **Información:** Un activo que, como cualquier otro activo importante de negocio, es esencial para el negocio de una empresa. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, transmitido por correo o de forma electrónica, mostrado en películas o hablado durante una conversación.

- **Marco de gobierno:** Una entidad cuantificable que permite la medida de la consecución de una meta de proceso. Las métricas deben ser específicas, medibles, accionables, relevantes y oportunas. Una guía completa para una métrica define la unidad a usar, la frecuencia de medida, el valor objetivo ideal (si resulta apropiado) y también el procedimiento para la realización de la medida y el procedimiento para la interpretación de la evaluación.

- **Buenas prácticas**: Las buenas practicas requieren que las políticas sean parte de un marco general de gobierno y de gestión, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes.

- **Modelo:** Un modo de describir un conjunto de componentes y de como esos componentes se relacionan entre ellos para describir el funcionamiento principal de un objeto, sistema o concepto.

- **Objetivo:** La traducción de la misión de la empresa desde una expresión de intenciones a unas metas de rendimiento y resultados.

- **Objetivo de proceso:** Una declaración describiendo el resultado deseado de un proceso. Un resultado puede ser un elemento, un cambio significativo de estado o una mejora de capacidad significativa de otro proceso.

- **Objetivo de TI:** Una declaración describiendo el resultado deseado de las TI empresariales como soporte a los objetivos de la empresa. Un resultado puede ser un elemento, un cambio significativo de estado o una mejora de capacidades significativa.

- **Control:** Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida.

- **Control de procesos de negocio:** Las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para generar garantías razonables de que un proceso de negocios conseguirá sus objetivos.

- **Contexto:** El conjunto completo de factores internos y externos que pueden influir o determinar cómo actúa una empresa, entidad, proceso o individuo.
- **Contexto Tecnológico**: Factores tecnológicos que afectan la capacidad de una organización para extraer valor de los datos.

- **Contexto de Datos:** La precisión de los datos, su disponibilidad, grado de actualización y calidad.

- **Habilidades y Conocimiento**: Experiencia general y habilidades analíticas, técnicas y de negocio.

- **Contexto Organizativo y Cultural:** Factores políticos, y si la organización prefiere datos a la intuición.

- **Contexto Estratégico**: Metas corporativas estratégicas.

- **Práctica de Gobierno (gestión):** Para cada proceso COBIT, las prácticas de gobierno y gestión proveen un conjunto completo de requerimientos de alto nivel para el gobierno y la gestión efectiva y práctica de TI de una empresa. Se trata de declaraciones de acción de los cuerpos de gobierno y gestión.

- **Principio:** Un catalizador del gobierno y la gestión. Comprende los valores y las hipótesis fundamentales contenidas en la empresa, las creencias que la guían y que definen sus límites entorno a los procesos de decisión, comunicación interna o externa y la administración de los activos que pertenecen a otros.
- **Servicio TI:** La provisión diaria a clientes de la infraestructura y de las aplicaciones TI y de soporte para su uso. Los ejemplos incluyen el centro de servicios, la provisión de equipamiento y los movimientos, y las autorizaciones de seguridad.

- **Sistema de control interno:** Las políticas, estándares, planes y procedimientos y las estructuras organizativas diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse y de que los eventos no deseados serán evitados o detectados y subsanados.

- **Confidencialidad:** Hace referencia a la protección de la información, cuya divulgación no está autorizada.

- **Integridad:** La información debe ser precisa, coherente y completa durante de su ciclo de vida (desde que se crea hasta que se destruye).

- **Disponible:** La información debe estar disponible en el momento y formato que se requiera en el ahora y el futuro.

- **Confiabilidad**: La información debe ser apropiada y cumplir con los requerimientos necesarios para su emisión.

- **Aceptación de riesgo**: Cantidad de riesgo, a nivel global, que la empresa está dispuesta a aceptar en el cumplimiento de su misión.

- **Activo**: Algo de valor, ya sea tangible o intangible, que se debe proteger, incluyendo personas, sistemas, infraestructura, finanzas y reputación.

- **Agrupación de riesgo**: Proceso de integración de las evaluaciones del riesgo a nivel corporativo para obtener una visión completa sobre el riesgo global de la empresa.

- **Amenaza**: Cualquier incidente no-deseado que es capaz de actuar contra un activo de manera que se pueda presentar un perjuicio.

- **Análisis de impacto en el negocio (BIA)**: Evaluación de la criticidad y sensibilidad de los activos de información.

- **Análisis de riesgo**: Proceso por el cual se estima la frecuencia y magnitud de los escenarios de riesgo de TI. También se puede considerar como los pasos iniciales de la gestión de riesgos (Análisis del valor de los activos, identificación de amenazas, evaluación de vulnerabilidades).

- **Apetito de riesgo**: es el nivel de riesgo en diferentes aspectos que una empresa está dispuesta a aceptar en pos del cumplimiento de su misión (o visión).

- **Capacidad de riesgo**: El nivel objetivo de perdida que una empresa puede tolerar sin arriesgar su viabilidad. Difiere del apetito del riesgo, el cual es una decisión de la gerencia o del directorio, sobre cuanto riesgo es deseable aceptar.

- **Comité de gestión de riesgo corporativo (ERM)**: Es el grupo de ejecutivos corporativos que es responsable de la colaboración y consenso a nivel corporativo requeridos para soportar las actividades y decisiones de ERM. Este comité es considerado para ser la segunda línea de defensa contra las manifestaciones del riesgo. Se puede establecer un Consejo de Riesgos de TI para considerar los riesgos de TI con mayor detalle y asesorar al comité de ERM. Los miembros de este comité son usualmente miembros del consejo directivo y está liderado por el CEO.

- **Compartir el riesgo**: Forma de tratamiento del riesgo que involucre la distribución acordada del riesgo con otras partes. Transferir el riesgo.

- **Conducta humana**: La comprensión de las interacciones entre personas y otros elementos de un sistema con la intención de asegurar el bienestar de las personas y el buen rendimiento del sistema. Incluye la cultura, necesidades y aspiraciones de las personas como individuos y como grupo.

- **Consecuencia**: Resultado de un evento que afecta a los objetivos.

- **Cultura del riesgo**: Conjunto de valores y creencias compartidas que rigen la actitud hacia la asunción de riesgos, la atención y la integridad, y determina cuan abiertamente el riesgo y perdidas se presentan y discuten.

- **Declaración del riesgo**: Descripción de las condiciones actuales que pueden conducir a la perdida, y una descripción de esa pérdida (debe incluir descripción de las condiciones actuales que pueden conducir a una perdida).

- **Escenario de riesgo**: Descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio.

- **Evaluación de riesgos**: Proceso usado para identificar y evaluar los riesgos y sus posibles efectos.

- **Evento**: Algo que sucede en un lugar y/o tiempo específico. Ocurrencia o cambio de un conjunto particular de circunstancias.

- **Evento de amenaza**: Cualquier evento durante el cual un elemento/actor de una amenaza actúa contra un activo de forma que tiene la posibilidad de causar directamente un perjuicio.

- **Evento de partida**: Cualquier evento durante el cual una amenaza ocasiona una perdida.

- **Evento de vulnerabilidad**: Cualquier evento durante el cual se da como resultado un aumento sustancial de la vulnerabilidad, que puede ser el resultado de cambios en las condiciones de control o de los cambios en la capacidad y/o fuerza de la amenaza.

- **Exposición**: Susceptibilidad a la ganancia o pérdida; generalmente se cuantifica en términos de impacto potencial.

- **Factor de riesgo**: Condición que puede influir en la frecuencia y/o magnitud, y en última instancia, en el impacto, en el negocio, y los eventos y/o escenarios relacionados con TI.

- **Frecuencia**: Medida de la ratio de ocurrencia de eventos durante un cierto periodo de tiempo. Numero de ocurrencias de un evento o resultado para un periodo de tiempo definido.

- **Finalidad del negocio**: Traducción de la misión de la empresa en los objetivos de rendimiento y resultados desde una declaración de intenciones.

- **Gestión**: El sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización. Está sujeta a la guía y monitorización establecidas mediante el gobierno corporativo.

- **Gestión del riesgo corporativo (ERM)**: Disciplina por la cual se evalúa, controla, explota, financia, y monitorea el riesgo de todas las fuentes con el fin de incrementar el valor de la empresa a corto y largo plazo para sus inversores.

- **Gobierno corporativo**: El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información.

- **Incidente**: Interrupción no planificada de un servicio de TI o reducción en la calidad de un servicio de TI. También lo es el fallo de un elemento de configuración que aún no ha impactado en el servicio. Evento en el que se produce una pérdida o se podría haber producido, independientemente de la severidad.

- **Indicador de riesgo**: Métrica capaz de demostrar que la empresa está sujeta, o tiene una alta probabilidad de ser sometida, a un riesgo que excede la aceptación de riesgo definida.

- **Impacto en el negocio**: Efecto neto positivo o negativo, sobre la consecución de los objetivos de negocio.

- **Incertidumbre**: Estado total o parcial de la falta de información relacionada a la comprensión o el conocimiento de un evento, su consecuencia o probabilidad de ocurrencia. Incapacidad para saber de antemano la probabilidad o el impacto exactos de eventos futuros.

- **Incidente relacionado con TI**: Evento relacionado con TI que causa un impacto operacional, de desarrollo y/o estratégico en el negocio.

- **Indicador de retraso**: Métrica para la consecución de objetivos, es un indicador relativo a un resultado o al resultado de un facilitador, y solo estará disponible después de que los eventos ocurran.

- **Indicador de riesgo clave**: Subconjunto de los indicadores de riesgo que son altamente relevantes y poseen una alta probabilidad de predecir o señalar un riesgo importante.

- **Indicador principal**: Métrica para la aplicación de buenas prácticas, es un indicador relativo al funcionamiento de un facilitador, es decir, el indicador proporcionara una indicación sobre el posible resultado del facilitador.

- **Interesado (*stakeholder*)**: Individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a ser afectado, por una decisión o una actividad.
- **Magnitud**: Medida posible de la gravedad de la pérdida o la potencial ganancia de eventos y/o escenarios conocidos.

- **Mapa de riesgo**: Herramienta grafica para clasificar y visualizar riesgos mediante rangos definidos para su frecuencia y magnitud.

- **Matriz de riesgo**: Herramienta para clasificar y visualizar el riesgo mediante la definición de categorías de riesgo (por ej., riesgo financiero, de seguridad y contextual, etc.); definiendo rangos para las consecuencias y los niveles de posibilidad de cada categoría.
- **Nivel de riesgo**: Magnitud de un riesgo expresada en términos de la combinación de las consecuencias y su probabilidad.

- **Objetivo del negocio**: Desarrollo a fondo de la finalidad del negocio en objetivos tácticos y resultados deseados.

- **Perfil de riesgo de TI**: Descripción del riesgo de TI general e identificado al que la empresa está expuesta.

- **Problema**: Causa de una o más incidencias. En el momento en el que se crea el registro de problemas no es frecuente reconocer su causa, por lo que es necesario realizar su investigación mediante el proceso de gestión de problemas.

- **Problema de riesgo**: Combinación de condiciones de control, valor y amenaza que impone un nivel notable de riesgo de TI.

- **Procedimiento**: Una acción que implementa una política.

- **Registro de riesgos de TI**: Repositorio de los atributos clave de los problemas de riesgo de TI potenciales y conocidos (Nombre, descripción, propietario, frecuencia esperada/actual, magnitud potencial/actual, impacto potencial/real en el negocio, etc.).

- **Respuesta al riesgo**: Eliminación de riesgos, compartición y/o transferencia de riesgos, mitigación de riesgos, que lleva a una situación en que el futuro riesgo residual cae tanto como sea posible dentro de los límites de aceptación del riesgo.

- **Riesgo**: Situación probable con frecuencia y magnitud inciertas.

- **Riesgo absoluto**: Nivel de riesgo sin tener en cuenta los controles existentes de riesgos.

- **Riesgo de TI**: El riesgo del negocio asociado con el uso, propiedad, operación, participación, influencia y adopción de las TI dentro de una empresa.

- **Riesgo residual**: Riesgo que queda luego de que se han implementado respuestas al riesgo.

- **Seguridad**: Estrategia de protección contra un riesgo.

- **Tipo del evento**: A los efectos de la gestión de riesgos de TI, uno de los tres posibles tipos de eventos (Amenaza, Perdida o Vulnerabilidad).

- **Tolerancia al riesgo**: Nivel de variación aceptable que la Gerencia esta dispuesta a asumir en algún riesgo en particular, en el seguimiento a los objetivos por parte de la empresa. Disposición de la organización para aceptar el riesgo residual después del tratamiento del riesgo con el fin de alcanzar los objetivos de la organización.

- **Uso de TI**: Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de TI por unidades de negocio internas, unidades especializadas de TI, proveedores externos y "*Utility Services*" (como los que se proveen de software como servicio).

- **Valoración del riesgo**: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

- **Vulnerabilidad**: Debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a las adversidades de eventos de amenaza.

INTRODUCCIÓN

Las organizaciones, con mayor frecuencia están inmersas en un entorno cada vez más abierto a la competencia y al cambio. La globalización de la economía, el dinamismo tecnológico, las nuevas tecnologías de la información y muchos otros factores influyen en sus resultados y se convierten en componentes determinantes para la supervivencia en su entorno de desempeño. En el contexto actual, toda empresa por grande, mediana o pequeña que sea, tiene una relación directa con el consumo de tecnología; de otra manera no podrían ser competitivas y enfrentarse a los nuevos retos y enfoques de gestión. Por ello toda organización buscará obtener ventajas sobre las demás, que se puedan mantener en el tiempo, a través de la identificación de debilidades, amenazas, fortalezas y oportunidades. Una ventaja que marca la pauta, es la adecuada gestión y preservación de los activos de información; al reconocer que se depende de ellos para preservar la historia, ejecutar el presente y construir el futuro corporativo.

Uno de los aspectos más relevantes para determinar cuáles son los procesos creadores de valor en las organizaciones, sin lugar a duda, es la información que se genera a partir de su evolución. Para que la información aporte valor, se requiere que sea fiable, confidencial, integra y que esté disponible en el momento indicado. La conservación de estas características, requiere del compromiso y gestión en todas las estructuras organizacionales, mediante la incorporación de estrategias de desempeño para la gestión de la calidad y seguridad de la información; también para la prevención del riesgo informático. Aunque el valor de este activo no se cuantifique y refleje en los estados económico-financieros, su incidencia en la creación de valor de la organización y para el sistema económico en su conjunto es evidente, al señalar su potencial en términos estratégicos, para maximizar la sinergia de recursos en el desarrollo y mejora de la competitividad(Hamidovic, Researcher, and Sec 2015)

Ninguna entidad está libre de los riesgos, que son de diversos tipos y condiciones, y el uso de recursos informáticos no es ajeno a esta realidad. Este contexto presiona a que las soluciones de tecnología, sean evaluadas periódicamente para identificar, prevenir y controlar los riesgos de seguridad. Con base en los argumentos expuestos, se propone la tesis, cuyo objetivo es el diseño de una metodología, que evalúe la inclusión y calidad de los criterios de seguridad en los sistemas orientados a la gestión académica de las instituciones de educación superior. El interés por las universidades, fue el resultado de la identificación de una carencia en procesos de auditoria de seguridad de la información en las universidades; complementado con la literatura formal, al encontrar estudios que demuestran que las universidades se han ido destacando por ser medios propicios y atractivos para la ciberdelincuencia; por su diversidad de usuarios, por el alto consumo de tecnología y a la combinación de ambientes de trabajo que están reunidos en un mismo escenario(Rehman, Masood, and Cheema 2013)(REDCLARA; TICAL 2015).

Algunas investigaciones han posicionado los ataques informáticos en instituciones de educación superior en primer, segundo o tercer lugar, después del sector financiero y la industria farmacéutica(Rehman et al. 2013). Se considera que los sistemas universitarios se caracterizan por tener una tendencia constante al aumento de riesgos relacionados con la seguridad de la información. Por ello, las comunidades académicas se han interesado en la búsqueda de mecanismos de protección para fortalecer la calidad y fiabilidad de la información; también en proponer auditorías estándares basadas en guías y procedimientos que faciliten la evaluación de los sistemas y la implementación de planes de mejora continua(Rehman et al. 2013).

El aporte con el desarrollo de una metodología para auditar la seguridad de la información, está enfocado en brindar una herramienta que basada en las buenas prácticas, proporcione un medio que facilite y motive la incorporación de procesos de autoría, con el propósito de identificar y mitigar riesgos. Algunos autores de metodologías para auditar la seguridad informática, consideran que los recursos son limitados y que esta situación aporta para que los auditores supongan controles; hecho que les ha impulsado a proponer patrones como una opción para que los auditores verifiquen el cumplimiento con base en criterios de auditoria(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008). Con la actual propuesta, se pretende crear un patrón a través de un diseño metodológico aplicable, repetible, adaptativo, flexible, abierto, dinámico e innovador .

El desarrollo de la tesis estuvo representado en siete capítulos. Los dos primeros dedicados a los marcos metodológico y conceptual. Los siguientes al diseño de la metodología compuesta por criterios y controles de seguridad de la información con sus respectivos requisitos de cumplimiento; al diseño de los instrumentos de medición; a la estructura del ciclo de vida del programa de auditoria; al análisis de los resultados obtenidos con la aplicación de los instrumentos; a la evaluación de los criterios de seguridad; al informe ejecutivo compuesto por el concepto técnico de la situación de seguridad de la información en una universidad, para los tres escenarios intervenidos y las recomendaciones para mitigar los riesgos hallados. También se realizó un resumen de todos los componentes propuestos durante el diseño de la metodología, para argumentar la completitud de la propuesta inicial y una descripción de sus características, para demostrar su validez. Finalmente se presentaron las conclusiones del desarrollo de la tesis y las posibles líneas de investigación que se pueden derivar del trabajo realizado.

1. ANTECEDENTES

La gestión de las Tecnologías de Información y Comunicación (TIC) en el contexto universitario ha ido tomando fuerza. A media que las instituciones tienen la necesidad de ser eficientes en la adecuada gestión de sus activos y recursos, requiere incorporar herramientas para responder a los nuevos desafíos que imponen los acelerados cambios a los que se enfrenta la humanidad diariamente. Según *Huma Rehman et al.* (2013), las universidades tienden a funcionar de una manera diferente al resto del sector productivo; debido a la diversidad de usuarios internos y externos que la conforman, a sus procesos que las hacen particulares y a la combinación de modelos de desempeño (educativos, investigativos, sociales y empresariales). Las universidades deben consolidar un esquema propio y diferenciador; que resalté su razón de ser en el entorno para a los desafíos del mercado (REDCLARA; TICAL 2015)(*Rehman et al*. 2013).

Dentro del contexto de gestión de las TIC, la información es uno de los pilares esenciales. Su adecuada gestión se convierte en el componente que mide el desarrollo, la eficiencia, la eficacia y calidad en toda organización. En el contexto universitario, toda institución está obligada a reportar a las entidades de regulación y control información confiable, veraz y medible de acuerdo con las políticas y estrategias establecidas por las entidades de gobierno. Para Colombia es el ministerio de Educación (MINEDUACIÓN), quien ejerce las funciones para generar normas y hacer control a las instituciones de educación, amparada en las políticas y estrategias que establece el sistema de aseguramiento de la calidad de la educación superior (REDCLARA; TICAL 2015)(Anon n.d.).

La política de calidad del Ministerio de Educación, se orienta a que las instituciones reporten permanente al estado y a la sociedad información confiable sobre los servicios educativos que prestan; con el objetivo de generar ambientes de auto evaluación que promuevan la mejora continua. Para ello el ministerio se apoya en cuatro sistemas de información claves: 1) Sistema Nacional de Educación Superior (SNIES), encargado de controlar los datos de las IES y sus programas académicos, 2) Observatorio para la Educación, implementado para hacer seguimiento permanente a los graduados de las IES, 3) Sistema de Información para el Aseguramiento de la Calidad (SACES), almacena la información de los programas académicos para el proceso de Registro Calificado, 4) Sistema de Prevención y Análisis de la Deserción en las Instituciones de Educación Superior (SPADIES) que permite llevar trazabilidad de la deserción académica para calcular el riesgo que se produce y a la vez implementar medidas para prevenirlo (Anon n.d.). Para que las IES puedan dar respuesta eficiente y oportuna al Ministerio de Educación, demás entes de control y la comunidad que las componen, deben apoyarse en sistema de información que les permitan hacer la gestión permitente al interior de las instituciones. Por este motivo los SI deben ser herramientas de gestión adecuadas, diseñadas y desarrolladas con criterios de calidad funcionales y de seguridad de la información para que el tratamiento del dato responda a la veracidad y fiabilidad que

se espera en los diversos reportes y evaluaciones (REDCLARA; TICAL 2015)(Anon n.d.).

Adicional a las exigencias de gestión de la información del Ministerio de Educación, en el año 2016 el Consejo Nacional de Política Económica y Social (CONPES) aprobó la política de seguridad nacional digital, con la cual busca tener mecanismos formales para enfrentar el crecimiento de las amenazas cibernéticas. Esta política aplica sin excepción a todas las entidades que funcionan en Colombia. Su enfoque es cambiar la gestión del riesgo buscando que sea coherente y efectivo contra las nuevas y sofisticadas modalidades del cibercrimen, que encuentran un ambiente adecuado para atacar en la evolución y adopción de las TIC(Glen 2016).

La ley 1581 de 2012 (Ley de Protección de Datos Personales) que rige en Colombia, está ampliamente relacionada con las universidades en Colombia, debido a la diversidad de bases de datos y perfiles de usuario que utilizan y tratan en sus sistemas de información y gestión. La ley 1581 tiene por objeto brindar a las personas mecanismos legales para favorecer el derecho a conocer, actualizar y eliminar sus datos personales en bases de datos físicas o digitales. Las universidades no son ajenas a esta ley y en el tratamiento de los datos requieren SI para gestionar sus procesos con prácticas de calidad y seguridad de la información que garanticen la disponibilidad, fiabilidad y confidencialidad de la información; también su correcto tratamiento, conforme lo establece la norma ISO:27001 (Congreso de Colombia 2012).

En las organizaciones, es común que la ausencia de criterios de selección claros y alienados con los objetivos estratégicos abran la posibilidad de incorporar tecnología sin la suficiente verificación y confirmación que los productos satisfacen a cabalidad los requerimientos de calidad y seguridad de la información. Esta es una situación cotidiana y no ajena a la incorporación de software para apoyar los procesos organizacionales en instituciones de educación superior; haciendo más difícil la vinculación de criterios de seguridad de la información sin tener en cuenta que es un eje trasversal que depende de todas las unidades y principalmente del gobierno universitario, en quien recae la responsabilidad primordial al ser el organismo que define la forma como va a funcionar la seguridad en el conjunto de personas, procesos, subprocesos y actividades para cumplir el reto de garantizar la confidencialidad, integridad y disponibilidad de la información y a la vez alcanzar sus objetivos estratégicos (Rehman et al. 2013)(REDCLARA; TICAL 2015).

La seguridad de la información con frecuencia es comprendida como una gestión a través de elementos de seguridad físicos y de software, desconociendo que es mucho más que esto. Su adecuado tratamiento está directamente relacionado con las personas que hacen parte del sistema, con las políticas y lineamientos estratégicos, con el desempeño de los procesos y la gestión de los activos. Estos elementos deben alinearse perfectamente con las TIC, con la aplicación de buenas prácticas y con el control permanente de la gestión que gira alrededor de la información; siendo la información reconocida como el activo más valioso para cualquier organización. Para el caso de un sistema universitario se produce a partir

de procesos de académicos, investigativos, sociales y administrativos. También en la relación con estudiantes, empleados y proveedores; siendo estos elementos y factores los que hacen de la gestión y el control de la seguridad de la información una tarea compleja en donde con frecuencias se cometen errores en el tratamiento de datos(REDCLARA; TICAL 2015).

En un contexto general la gestión de la seguridad de la información anteriormente estaba estrechamente relacionada con la seguridad informática al igual que los procesos de auditoria de la información, sin embargo la información ha sido reconocida como el activo más valioso en toda entidad. Por ello es necesario incorporar procesos de auditoria propios para evaluar y detectar si existen carencias en la gestión e implementación de planes de seguridad de la información coherentes con el desempeño y los requerimientos identificados; esencialmente en los sistemas de información que soportan de forma trasversal el tratamiento de datos. Esta acción permitirá la detección temprana y el tratamiento del riesgo de forma preventiva; también el hallazgo de vulnerabilidades y amenazas para evitar fugas de información relevante, preservación del buen nombre de las institucionales, cumplimiento de la normatividad y adecuada gestión interna del activo información. También aumentará los argumentos para destinar presupuestos y recursos que den la posibilidad de hacer planes estratégicos robustos y con un cubrimiento total de la organización en donde la seguridad de la información se incluyente y no un componente adicional(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

La comunidad académica ha propuesto diversos modelos para apoyar la gestión y evaluación permanente de la seguridad de la información en sistemas de información, entre ellos se destacan: estudios de casos reales, modelos para evaluar el riesgo informático, metodologías de evaluación en seguridad. También repositorios de redes semánticas, bases de datos de centros especializados en detección y prevención del riesgo informático; modelos para evaluar, las etapas de desarrollo de software y el ciclo productivo de los sistemas de información. Los trabajos de investigación han tenido interés por el análisis de patrones de comportamiento de los gobiernos corporativos y la alta dirección frente a la gestión de la seguridad de la información.

2. MARCO METODOLÓGICO

2.1 Problema a Resolver

Los riesgos de seguridad de la información que se han ido materializando sobre los procesos, por las vulnerabilidades que no han sido identificadas y corregidas en los productos de software al servicio de las instituciones de educación superior.

Las causas para que los productos de software den espacio a la materialización de los riesgos, con frecuencia se relacionan con falencias durante el proceso de desarrollo de los productos(Knowles, Baron, and McGarr 2016). También por desconocimiento de los profesionales de desarrollo sobre seguridad, por la aceleración de los procesos de producción de software, por reducción o no asignación de los presupuesto, sostenibilidad, aseguramiento y calidad. Influye de forma importante cuando las organizaciones no tienen claros sus procesos de negocio, ni los requerimientos funcionales. Desde las dependencias de TI, si los protocolos de mantenimiento y soporte del software son insuficientes, representan un riesgo en su operatividad. También si la actualización de productos no evoluciona con el crecimiento de las organizaciones y el cambio tecnológico del contexto(Baca and Petersen 2013)(Anon n.d.). Estas causas pueden terminar en consecuencias que afecten a las instituciones en perdida de información, ataques cibernéticos, indisponibilidad de los servicios, deficiencias importantes en la calidad de los datos, afectación del prestigio y posicionamiento de las organizaciones en el entorno(Isaca 2013).

La descripción del problema a resolver y las causas que lo sustentan, es la base para proponer el diseño de una metodología; que brinde la posibilidad de auditar la inclusión de los criterios de seguridad de la información en los sistemas de gestión académica, de las instituciones de educación superior. Con el propósito de facilitar la identificación de riesgos y la inclusión de procesos de auditoría, que permitan detectar de forma oportuna amenazas; previniendo que se materialicen y causen daños y pérdidas desestabilicen a las instituciones.

2.2 Justificación

Realizar procesos de auditoría de seguridad, con frecuencia es una tarea compleja, sin embargo, es una medida de diagnóstico para obtener datos de valor, sobre el estado de la protección de la información en una organización(Knowles et al. 2016). El resultado de una auditoría, da la oportunidad de identificar y mitigar los riesgos de seguridad, alinear los sistemas de información con las políticas de gobierno universitario, implementar mecanismos de seguimiento y control, mejorar el mantenimiento y soporte del software e implementar planes de mejora continua. A partir del resultado de una auditoria, se puede prever con mayor precisión presupuestos para realizar inversiones con base en criterios justificados y

sustentados, según el modo de operación de cada institución(Yu et al. 2015)(Anon n.d.).

Diseñar una metodología a la medida, para auditar la seguridad en los sistemas de información de las instituciones de educación superior, se convierte en una ventaja competitiva con impacto estratégico. La información, es la base de toda decisión dentro de una organización y sobre ella se proyecta su evolución, crecimiento e innovación. El valor que tiene la información y la función que ejerce, justifica que se tenga esquemas que mitiguen los riesgos de seguridad y se implemente mecanismos de detección oportuna, para garantizar que la información es un activo confiable, íntegro y que está disponible; reflejando el comportamiento organizacional, alienado al gobierno universitario(Knowles et al. 2016). La gestión de la información también debe estar en sintonía con sus objetivos estratégicos, las regulaciones de ley y tiene la obligación de ser coherente con los servicios universitarios que presta y sus diversos públicos objetivos(Barton 2014)(Anon n.d.)(Herath and Herath 2014).

Dentro de un contexto general, las organizaciones carecen de procesos de auditoría interna en lo referente a la evaluación continua de la seguridad de la información, siendo este un motivo para que aumente el riesgos, las amenazas y las vulnerabilidades de forma recurrente, dada la proliferación continua de la delincuencia digital y el cibercrimen, que cada vez hace mayor presencia en las tecnologías que se incorporan a las organizaciones, elevando el nivel de dificultad para su identificación, seguimiento y tratamiento(REDCLARA; TICAL 2015)(Shameli-Sendi, Aghababaei-Barzegar, and Cheriet 2016)(Glen 2016).

2.3 Pregunta de investigación

¿Cuáles son los criterios más apropiados para diseñar la metodología para auditar la seguridad de la información en productos de software orientados a la gestión académica en instituciones de educación superior?

2.4 Objetivos de la investigación

2.4.1 Objetivo General

Diseñar una metodología para auditar la seguridad de la información en productos de software orientados a servicios de gestión académica en instituciones de educación superior.

2.4.2 Objetivos Específicos

- Definir los criterios de cumplimiento de los requisitos de seguridad en los servicios de información.

- Diseñar los controles para evaluar los criterios de seguridad de la información en los productos de software a intervenir.
- Construir los instrumentos de medición para los criterios identificados en las dimensiones establecidas.
- Verificar la validez y completitud de la metodología diseñada.

2.5 Alcance de la propuesta

Diseño de una metodología que estará enfocada a la auditoria de criterios de seguridad en los sistemas de información, orientados a los servicios de gestión e información en las instituciones de educación superior.

2.6 Resultados esperados

- Definir los criterios para evaluar la calidad e inclusión de los criterios de seguridad de la información.
- Definir los controles de seguridad basados en las prácticas que propone la norma técnica colombiana ISO 27000:2013 e ISACA en su marco de referencia COBIT 5.
- Diseñar los instrumentos de aplicación, que sean coherentes a las dimensiones y criterios de seguridad de la información establecidos.
- Diseñar la estructura del ciclo de vida del programa de auditoría para aplicar la metodología desarrollada.
- Obtener la metodología que sustente el desarrollo de la propuesta de tesis aprobada.
- Recopilar los datos necesarios a partir de la aplicación de los instrumentos diseñados para realizar análisis de seguridad de la información.
- Informe con el resultado obtenido sobre el estado de la institución con relación a la inclusión de los criterios de seguridad en una institucón de educación superior.

3. MARCO CONCEPTUAL

3.1 Estado del arte

Sultan S. Alqahtani, et al en (Alqahtani, Eghan, and Rilling 2016) proponen un enfoque de modelado que consiste en hacer aprovechamiento de las tecnologías de la web semántica[1] para establecer enlaces en entre repositorios de asesoramiento de seguridad de la información y repositorios de desarrollo de software, la novedad del modelado es que le permite a los desarrolladores de software obtener fuentes de información para hacer trazabilidad al desarrollo de software desde bases de datos de vulnerabilidades considerados centros de información confiables.

El enfoque de modelado tiene importancia en el trabajo de tesis propuesto al proveer bases de conocimiento que han sido diseñadas para hacer trazado de vulnerabilidades durante el proceso de desarrollo de software, permitiendo la detección temprana e implementación de controles de seguridad para convertir la seguridad de la información en parte integral de las buenas prácticas adoptadas durante el desarrollo de software, sin embargo existe limitante que no contempla la auditoria de la seguridad de la información una vez el software este en etapa productiva para medir la efectividad de los controles implementados.

Masahito Saito, et al en (Anon n.d.) describen un sistema de gestión basado en casos CBMS, es un sistema de gestión de artefactos integrado a un sistema de gestión del conocimiento (KBMS) para trabajar en casos de desarrollo seguro que combina la gestión del ciclo de desarrollo con la gestión de la seguridad durante la elaboración del software, realizando asociaciones para visualizar conocimiento en seguridad de la información durante las etapas de construcción. En este trabajo se destaca la importancia que tiene la seguridad de la información en el proceso de desarrollo de software, haciendo énfasis que no es suficiente con implementar tecnologías de red, de cifrado o control de acceso; motivo que hace indispensable que el ingeniero de desarrollo de software tenga a su alcance herramientas para trabajar la seguridad de la información durante la elaboración del software.

En el análisis de casos se parte de la base que los ingenieros de desarrollo de software no son expertos en tecnologías de seguridad de la información, que no conocen sobre procesos de desarrollo seguro y que desconocen cómo integrar la seguridad de forma efectiva a los productos que construyen. Se considera que requieren del apoyo de bases del conocimiento que aborden diversos casos en cada etapa de desarrollo de software.

[1] Web semántica: Permite compartir recursos a través de máquinas que interactúan entre sí a través de procesamiento de software, ejemplo: motores de búsqueda y seres humanos.

Para el desarrollo de la tesis aporta en los planes de mejora que debería resultar de una auditoria, buscando concientizar a los profesionales que desarrollan software sobre la necesidad de conocimientos en seguridad de la información y de la importancia que tiene para mitigar el riesgo de amenazas una vez se tengan productos terminados.

Hassan El-Hadary, et al en (Anon n.d.) proponen una metodología para la integración temprana de los requerimientos de seguridad de la información en la etapa inicial del desarrollo de software, basados en los marcos de problemas. El objetivo principal es proveer una metodología que permita hacer ingeniera de los requerimientos de seguridad en la etapa de requerimientos de calidad. Con la aplicación del proceso de modelado y evaluación de requisitos a través de los marcos de problemas se identifica a tiempo los criterios de seguridad.

Los marcos de problemas se definen como las lesiones aprendidas de procesos de desarrollo anteriores y que han sido configurados en un catálogo de requerimientos de seguridad, obtenidos a partir de la ingeniería de requerimientos. Consisten en utilizar abusos de marcos para modelar las amenazas y tramas de problemas de seguridad. El modelado debe repetirse las veces que se considere necesario con el objetivo de identificar nuevas amenazas y problemas que puedan convertirse en vulnerabilidades una vez el software este desarrollado. Esta investigación tiene especial relevancia para nuestro trabajo, debido a que a través del modelado se puede obtener información importante de los criterios de seguridad relacionados directamente con el software que son propensos a ser auditados.

Hemantha SB Herath, et al en (Herath and Herath 2014)proponen un modelo de decisión para evaluación del desempeño en las organizaciones y determinar si vale la pena o no realizar auditorías de seguridad de la información. El modelo se evalúa desde dos perspectivas: costos que origina realizar auditorías periódicas y el riesgo que se esté dispuesto a aceptar. Se basa en determinar si la perdida por fallos de seguridad es desfavorable y si la causa de la desviación es por falta de controles adecuados o por factores incontrolables. La aplicación está enfocado a empresas pequeñas con el objetivo de diseñar modelos de gestión de seguridad, con costos razonables y tomando como referencia dos parámetros: la magnitud de la desviación de pérdida y la probabilidad de las pérdidas por factores aleatorios. Este artículo puede resultar de gran utilidad al presentar un modelo que con base en criterios ya estudiados permita determinar el escenario para realizar una auditoría de seguridad de la información y dimensionar el aporte real que está brindaría a una organización.

William Knowles et al en (Knowles et al. 2016) proponen evaluaciones de seguridad cuando el software se encuentre en producción para identificar deficiencias que no fueron abordadas dentro de las etapas de desarrollo; con el objetivo de hacer una profesionalización continua en la industria. Los resultados fueron obtenidos de aplicar 54 encuestas a usuarios y proveedores de sistemas de información. El

resultado de las evaluaciones de seguridad muestra que se debería evaluar siete áreas dentro del proceso de desarrollo de software, como oportunidad de mejora del ecosistema de seguridad simulada. La investigación finaliza con una propuesta de marco denominado un ecosistema que recopila la información detectada y la normaliza para integrarla de forma controlada a los procesos de desarrollo.

La investigación destaca las directrices de auditoría basadas en la normas ISO /IEC 27001 – 27002 (Ntc-iso-iec 2013) como estándar de control de la seguridad, no obstante se cuestiona que la norma debería ser más específica entre la relación de evaluación y el proceso de desarrollo de software. Dentro del estudio surgen las preguntas ¿qué sentido tiene la norma dentro del proceso de desarrollo?, ¿qué significado tiene la gestión del riesgo? y cuál es la brecha entre la auditoría de seguridad de la información y la normalización terminológica en las etapas de desarrollo?; las soluciones a estas preguntas se propondrán como parte de investigaciones futuras, en donde se pretende revisar experiencias de estudios realizados por entidades como CREST y Tigerscheme. Estos organismos han definido de forma adecuada las competencias que deben tener profesionales que se dedican a evaluaciones de seguridad simuladas cuyos beneficios se han evidenciado principalmente en la industria del software en el Reino Unido.

Firoozeh Rahimian, et al en (Anon n.d.) describen una propuesta de un modelo multidimensional para especificar el nivel de seguridad basado en los datos y estimar el nivel del riesgo de las deficiencias halladas; también los controles de seguridad de la información. En la primera parte de la investigación se hace un análisis de las diferencias conceptuales entre los órganos de auditoria interna y la gestión de las dependencias de IT; quienes normalmente relacionan la seguridad de la información enfocada a la infraestructura tecnológica. Este relacionamiento identifica carencia de conocimiento en técnicas para evaluar riesgos y controles de seguridad de la información.

La propuesta de investigación va enfocada a un modelo y método para ser trabajado en tres dimensiones denominado método OLP. Su objetivo es realizar una estimación cuantitativa de los controles para prevenir la seguridad de los datos y con base en ellos definir una lista de criterios para un proceso de auditoría. Al finalizar la investigación se obtuvo una guía para los órganos de control y auditoria en las organizaciones. Es un modelo que se propone para ser aplicado en entornos empresariales reales, donde exista una necesidad del trabajo colaborativo para reducir costo y tiempo en la gestión de la seguridad de la información, sin embargo su adecuada utilización está sujeta a que la organización disponga de los recursos necesarios para su implementación y monitoreo constante con el fin de identificar los riesgos y falencias en el tratamiento de los datos.

Dejan Baca, et al en (Baca and Petersen 2013), presentan una investigación sobre gráficos para la evaluación del riesgo de seguridad en el software. El enfoque de la investigación ha sido direccionado para que sea compatible con los desarrolladores

en la identificación de amenazas de alto nivel y para que tengan la capacidad de tomar decisiones en las medidas preventivas a adoptar durante los procesos de desarrollo. El enfoque fue diseñado para la reutilización y capacidad de evaluación de las condiciones de seguridad en procesos de desarrollo con metodologías ágiles. La utilización de gráficos de evaluación había sido propuesta en investigaciones en donde se identificaron ataques de seguridad, que fueron clasificados con densidad alta y media. También amenazas de alto y mediado impacto a través de la utilización de los gráficos de contramedidas. Para la aplicación se basaron en modelos de amenazas (Peltier (2001) y Verdon y McGraw (2004)) y en casos de abuso (McDermott y Fox (1999) y McGraw (2006)), métodos utilizados para la identificación y prevención de riesgos. La validez de la investigación se centrará en la capacidad que adquieran los desarrolladores para repetir y reproducir el estudio realizado. Este trabajo tiene importancia, por el aporte que hace en la evaluación de riesgos que se debieron identificar y tratar en los procesos de desarrollo de software, no obstante, no contempla criterios que puedan conducir a un proceso de auditoría de seguridad de la información.

Alireza Shameli-Sendi, et al en (Shameli-Sendi et al. 2016) presentan un enfoque de la taxonomía de la evaluación de riesgos de seguridad recopilado de 125 artículos escritos entre 1995 y 2014. Sus objetivos se enfocan en hacer una selección de métodos estrictamente relacionados con el riesgo y en comparar conceptos de selección de riesgos de propuestas antiguas con respecto a los nuevos conceptos. Responde específicamente al sistema de gestión de seguridad de la información para ayudar a las organizaciones a realizar gestión del riesgo y una evaluación conforme a su entorno y contesto. Esta investigación tiene relevancia para hacer uso de los métodos recopilados en la evaluación del riesgo a los que se enfrenta un sistema de información.

Kresimir Solic, et al en (Solic, Ocevcic, and Golub 2015) presentan un modelo basado en la ontología OWL, publicar y compartir datos usando ontologías en la Web, que sea capaz de cubrir una gama amplia de los diversos problemas de seguridad de la información; integrando a una base de conocimiento directrices de seguridad, mejores prácticas, estándares y soluciones. Su desarrollo se da por algoritmos probatorios basados en cálculos matemáticos y la utilización de agentes inteligentes para soportar las decisiones. En la investigación se detalla la conexión que existe entre los diversos elementos del modelo para obtener la evaluación de la seguridad de la información. Se realizaron pruebas en empresas pequeñas, cuyo resultado arrojó que para lograr el objetivo se requiere adicionar al modelo un desarrollo de software que integre el conocimiento a una base de datos. Los beneficios que resalta el artículo de esta solución son la flexibilidad, aplicabilidad y capacidad de actualización de amenazas de seguridad; según vayan surgiendo. El modelo es versátil en muchos aspectos (seguridad en políticas, lineamientos, software, redes, hardware, personas responsables de la gestión de seguridad).

Nan Feng, et al en (Feng 2014) propone un modelo de análisis de riesgos de seguridad (SRAM), el cual consiste en el análisis de vulnerabilidades y amenazas a los recursos de información. El modelo da la posibilidad de tomar acciones que reduzca el riesgo a un nivel aceptable en los sistemas de información. El propósito es hacer frente a la complejidad y a la incertidumbre en la propagación de vulnerabilidades usando redes bayesianas (BNS) y la colonia de hormigas (ACO). La evaluación del riesgo de seguridad se realiza para calcular la probabilidad de ocurrencia y la severidad de la consecuencia del riesgo. Con la valoración por redes bayesianas es posible calcular la trayectoria de propagación de la vulnerabilidad. De alcanzarse el objetivo se podrá demostrar que el modelo permite mejorar la exactitud y la eficiencia de la gestión de los riesgos de seguridad en los sistemas de información.

Nader Shrabi Safa, et al en (Sohrabi Safa, Von Solms, and Furnell 2016) proponen un método para analizar el comportamiento humano en la seguridad de la información, bajo el argumento que los fallos asociados a la seguridad no obedecen estrictamente a problemas de orden tecnológico. Los datos del estudio revelan que también influyen en una medida importante actuaciones asociadas a la ética, falta de conciencia, resistencia al cambio, responsabilidad y seriedad que se adopte por parte de los empleados de una organización. Según la investigación la política de seguridad de la información es un elemento importante para mitigar riesgos en el comportamiento de los empleados; revelando que tener conocimiento de la misma, hacer aplicación de ella y adoptar buenas prácticas generan colaboración e intercambio de información adecuada y controlada.

Otro aspecto importante de la investigación es la actitud que asumen los empleados frente al cumplimiento de lineamientos de seguridad; demostrando qué, si un empleado no tiene sentido de pertenencia y un enlace social saludable con la organización, difícilmente actúa de forma positiva frente a la aplicación de prácticas de seguridad de la información saludables. El método investigado y aplicado, está basado en estudios de comportamientos sociales asociados a la seguridad de la información. Para realizar la investigación se estudiaron diversos métodos, entre los que se destaca: métodos para cerrar brechas de seguridad (Safa y col 2014), aspectos de seguridad cibernética (Von Solms y Van Niekerk (2013), la seguridad cibernética y la seguridad de la información dentro de la colaboración para establecer entornos seguros (Werlinger et al 2009). El objetivo de la investigación es mejorar el tratamiento de la información en las organizaciones desde la disciplina de la seguridad de la información; para hallar patrones de un adecuado comportamiento de los empleados acorde a la política de seguridad de la información. La investigación se propuso para entornos generalizados frente al comportamiento de las tecnologías en la empresa.

Para el trabajo de tesis que se desarrolla, cobra especial importancia debido a que en una auditoria de seguridad de la información el factor humano tiene una posición importante; las personas determinan la calidad de la información en la organización,

no obstante carece de conceptos asociados directamente a los sistemas de información.

Jeb Webb, et al en (Webb et al. 2014) proponen el modelo para gestión de riesgo utilizando el proceso information security risk management (ISRM). En la primera parte de la investigación se realiza una revisión a la literatura existente con relación a ISRM, determinando que la gestión del riesgo es el mecanismo por el cual las organizaciones preservan la integridad, confidencialidad y disponibilidad de la información; también se identifica que las organizaciones tienen serias deficiencias a la hora de gestionar los riesgos de seguridad de la información y que por tanto las medidas adoptadas frente a los riesgos hallados no son las correctas. El modelo propuesto es una extensión de un modelo anterior. Su aplicación se realizó en la empresa de Seguridad Nacional de Inteligencia de los Estados Unidos. De los aspectos a destacar durante la aplicación del modelo, se reconoce la importancia que tiene la norma ISO 27000(Manuel, Sánchez, and Velthuis 2012), no obstante se señala la importancia de adoptar un modelo único de gestión del riesgo según la estructura de la organización y los controles que requiera para su operación.

EL propósito de utilizar ISRM, en una organización es obtener información que detecte los riesgos de seguridad y apoye la toma de decisión sobre los controles a aplicar; según la gravedad de cada riesgo. La aplicación del modelo evidencia tres deficiencias básicas por las cuales se considera que los riesgos de seguridad de la información no están bien gestionados: 1) Comúnmente se identifica que la información de riesgos de seguridad es superficial, 2) la estimación de los riesgos de seguridad se realiza con baja referencia a la situación real de la empresa, 3) no existe un proceso continuado de la evaluación del riesgo, interrumpiendo la evidencia histórica de los riesgos asociados a determinada organización.

Este artículo tiene bastante relevancia en el desarrollo del trabajo de tesis, debido a que en su contenido se detalla información significativa al momento de plantear una metodología para evaluar la seguridad de la información, sin embargo no hace referencia a la gestión directa en los sistemas de información.

Paul John Steinbart, et al en (Anon n.d.) propone una investigación exploratoria para estudiar la relación que existe entre la auditoria interna y la seguridad de la información; indicando que para el éxito de la gestión de la seguridad de la información debe existir una relación muy estrecha entre las dependencias de seguridad de la información y el área de auditoria. Se indica que los roles de desempeño son diferentes, pero que debe existir sinergia en la comunicación y tener objetivos comunes que permitan velar por la adecuada gestión y la implementación de los controles de seguridad. Por un lado, la investigación señala lo importante que las dependencias de seguridad sigan conductos regulares, políticas y lineamientos acordes a las necesidades de gestión de la seguridad en las organizaciones. También menciona la importancia de las áreas de auditoria interna de hacer seguimiento, control y propuestas de mejora. La investigación indica que

una relación propositiva encaminada a la construcción de un desempeño funcional, evita tomar medidas represivas contra las personas y da la posibilidad de una buena orientación a todos los recursos y personas que interactúan en la seguridad de la información. La investigación se dividió por secciones, en donde la primera sesión está orientado a revisar la literatura relacionada con el tema. En la segunda parte describe las diversas entrevistas realizadas a profesionales de seguridad de la información en cuatro instituciones educativas y a funcionarios de áreas de auditoria interna y externa; haciendo énfasis en las diferencias encontradas entre una auditoria interna y externa en IT, en relación al personal de gestión de seguridad de la información. En la tercera sesión se realiza el análisis de los aspectos comunes importantes hallados y en la última etapa aborda las conclusiones y recomendaciones a través de la propuesta de un modelo que reúne un conjunto de proposiciones interesantes en donde se destaca la importancia de los factores hallados dentro de la investigación. Para esta tesis este artículo tiene una especial importancia, debido a la relación estrecha que debe existir en una organización entre la seguridad de la información y la auditoria, temas directos a desarrollar en el trabajo y por haber sido seleccionadas universidades para su aplicación.

Atif Ahmad, et al en (Ahmad, Maynard, and Shanks 2015) desarrollaron un análisis de estudio de casos de sistemas de información frente a respuestas de incidentes de seguridad de la información. Su objetivo es identificar las deficiencias que existen en las organizaciones en cuanto a las prácticas para tratar la respuesta a incidentes de seguridad de la información. Para el análisis tomaron una empresa australiana del sector financiero con el fin de extraer los hallazgos de incidentes de seguridad y evaluar la forma como las organizaciones incorpora la información a un sistema de lesiones aprendidas en pro de llevar un proceso de mejora continua frente a los casos presentados. Este estudio fue denominado respuesta a incidentes (IRTs). El propósito es analizar el comportamiento de las organizaciones en factores como: fallas de seguridad en los sistemas de información, violaciones de seguridad, incidentes, propagación, técnicas de erradicación, análisis de causas y por último facilitar la recuperación de las organizaciones a través de procesos de mejora continua y lesiones aprendidas.

La importancia de la investigación se centra en que IRTs tiene la capacidad de acumular experiencia en el tratamiento de los diversos fallos de seguridad y en ataques de forma oportuna; conduciendo en todo momento a una evaluación de la forma como se abordan los riesgos de seguridad, los factores de asesoría insuficiente, estrategias ineficaces, desinformación o falta de educación en incidentes y su gestión, políticas que se contradicen entre sí, formalización y sensibilización (SETA) (Shedden, Ahmad, y Ruighaver de 2010). Una vez realizado el análisis se emitieron recomendaciones en torno a desarrollar estrategias en práctica adecuadas orientadas a gestionar incidentes, aprendizaje organizacional, implementación de un modelo de proceso de seguridad – learning, renovaciones en la estrategia, la explotación vs la exploración. La investigación finalizó con conclusiones específicamente para la empresa australiana del sector

financiero. Este trabajo tiene relevancia debido a que expone un análisis real sobre incidentes de seguridad aplicados a sistemas de información, sin embargo está enfocado al aprendizaje en la gestión interna, excluyendo parámetros y fases de auditoria.

Inger Anne Tondel, et al en (Tøndel, Line, and Jaatun 2014) realizaron una recopilación y documentación de forma sistemática de las prácticas de gestión de incidentes de seguridad, con base en la literatura que se ha ido escribiendo en investigaciones anteriores. El trabajo realizado incluye temas de seguridad informática y de la información; también las normas, estándares y marco de referencia. Dentro del método de la investigación se propusieron tres preguntas enfocadas a irlas resolviendo a medida que se identificó literatura pertinente al tema. "¿Cómo es la gestión de incidentes de seguridad de información lleva a cabo en la práctica?, ¿Qué experiencias se reportan en la literatura en la información de gestión de incidentes de seguridad; lo que funciona bien, lo que es difícil?, ¿En qué medida las prácticas actuales se asemejan a las normas y directrices recomendadas?". Como resultado final se visualiza que en general la experiencia está en sintonía con los estándares y que el desarrollo de investigaciones con base en casos reales, pretende mejorar la experiencia frente a los retos de la gestión de incidentes de seguridad de la información.

En la literatura investigada, se incluyó documentos formales, empíricos, informes de casos reales, respuestas a incidentes, conferencias, documentos técnicos de organizaciones como: CERT/CC, SANS y FMI, ISO / IEC 27035, NIST Special Publication 800-61, ITIL, manual CSIRT (West-Brown et al., 2003); a fin de buscar cubrir la gestión de incidentes de seguridad desde diversos frentes y con la revisión de diferentes perfiles a nivel de tecnología general y sistemas de información. Como conclusión de la investigación, se presenta un compendio importante de buenas prácticas, recomendaciones y normas que son necesarias al momento de hacer gestión de incidentes de seguridad de la información, motivando a su implementación. Los autores reconocen que no es una labor sencilla la implementación de un modelo de seguridad de la información, que requiere de grandes esfuerzos, de recursos y de dedicación de personas; por lo que resaltan la importancia de seguir investigando sobre herramientas, técnicas y mecanismos que faciliten y apoyen la labor. Para el trabajo de tesis propuesto se visualiza como un documento resumen importante al abordar la literatura que se requiere para conocer sobre la gestión de seguridad de la información.

María Bartnes, et al proponen en (Anon n.d.) un estudio de las prácticas que se llevan a cabo con relación a la gestión de incidentes de seguridad de la información en organizaciones de control industrial, específicamente de la industria de energía eléctrica en empresas pequeñas y grandes de Noruega, quien tiene aproximadamente 150 gestores de redes de distribución y un aproximado de 10.000 clientes de energía. El estudio fue aplicado específicamente a sistemas distribuidos teniendo en cuenta que el sector esta determino por el alto riesgo de ataques al que

está expuesto, según cifras estadísticas del 2013 presentadas por ICS-CERT; en donde informa que un 59% de los incidentes de seguridad reportados por el Departamento de Seguridad Nacional de Estados Unidos se produjo en el sector de la energía eléctrica.

La investigación se concentra en analizar las prácticas de gestión de seguridad de la información en sistemas distribuidos del sector eléctrico y la influencia que tiene la tecnología en ellos, hallando datos que indican que tanto en empresas pequeñas como grandes se enfoca cada vez más por implementar sistemas de redes inteligentes y enfatizando importancia de la gestión de la seguridad en sistemas, administradores y usuarios. Las entrevistas realizadas para hallar los datos de análisis estuvieron direccionada a directivos de nivel medio de las organizaciones por considerarse que son los perfiles que tienen una visión completa de la organización y sus procesos tanto estratégicos como operativos.

Finalizada la investigación se presenta una serie de hallazgos que comprenden riesgo y amenazas con características similares entre el sector, presentado un documento de recomendaciones basado en los análisis de las entrevistas que se enfocan a mejorar la gestión de los incidentes de seguridad, a proponer cambios estratégicos y mejorar las competencias de los gestores con el objetivo de estar mejor organizados y preparados para las amenazas presentes y futuras; resaltando que se requiere de una mejor comprensión de conceptos de seguridad para entender de forma más adecuada la importancia de la gestión en ámbito de seguridad. Este trabajo aporta a la tesis en desarrollo, en la medida en que amplía la visión de la importancia de gestionar la seguridad de la información en todo producto de software que soporte los procesos organizaciones y estratégicos de toda entidad, también para tomar como ejemplo los instrumentos de evaluación construidos y aplicados a los interesados. No aporta en la gestión y aplicación de auditoria debido a que tienen un enfoque diferente.

Cesario Di sarno, et al en (Anon n.d.) desarrollaron una investigación basada en la seguridad de la información y los sistemas de gestión de eventos (SIEM), siendo utilizados con mayor frecuencia para hace frente a los desafíos de seguridad de la información en infraestructuras críticas (hardware, software, sistemas de información). En este trabajo se propone una versión mejorada de SIEM buscando resolver conflictos entre políticas de seguridad de la información, descubrimientos de accesos no autorizados, reconfiguración de dispositivos de red, integridad, capacidad de no repudio, tolerancia a fallos y aseguramiento de la disponibilidad.

El caso de estudio se desarrolló en sistemas que atienden el desempeño de presas hidroeléctrica por ser identificados como casos críticos y con alta exposición de ataques; considerando un modelo de ataque diseñado para afectar la tecnología de la información, demostrando con éxito que, la información de la seguridad y el sistema de gestión de eventos fue capaz de detectar los incidentes y responder de forma positiva, salvaguardando la seguridad de la información. Los sistemas de

gestión de eventos SIEM, son sistema de monitorización permanente que utiliza tecnología emergente para hacer seguimiento continuo a la seguridad de la información, cuyo propósito es descubrir brechas de seguridad de forma temprana y para almacenar datos recopilados que no ponen en riesgo los sistemas de información.

En sistemas SIEM, anteriores se han detectado limitaciones en la integración entre un sistema de soporte de decisiones y un sistema de almacenamiento de eventos resistentes. Estas limitaciones se han abordado y superado en esta versión de SIEM con el objetivo de hacer más consistente el sistema de gestión de eventos. En posteriores investigaciones se pretende experimentar el sistema SIEM, con el objetivo de analizar su eficacia y gestión de eventos relacionados con falsos positivos para mejorar la detención y respuesta a los ataques ante aplicaciones críticas. Para la tesis, el artículo podría tener incidencia en la revisión del modelo de ataque a fin de conocer la estratégica y funcionamiento del mismo con el ánimo de experimentar la seguridad de la información en los sistemas de información a analizar, también como referente de la gestión de eventos enfocados a la gestión de incidentes.

Nurul Hidayah Ab Rahman, et al en (Makori and Oenga n.d.) proponen un modelo conceptual forense digital conformado por 139 publicaciones dirigidos a mitigar los riesgo en la confidencialidad, integridad, y disponibilidad de los activos en las organizaciones principalmente enfocada a gestionar sus sistemas de tecnología a través de la nube; con el objetivo de mitigar riesgos en pérdidas financieras, jurídicas o de reputación de las organizaciones.

En la primera parte del trabajo se enfoca a recopilar el compendio de literatura formal que se ha generado entre los años 2009 y 2014 sobre conocimiento en manejo de incidentes en el entorno de la nube. Mediante la aplicación de encuesta se determina que la gestión de seguridad de la información es un proceso relativamente maduro, demostrado a través de un número importante de normas, directrices internacionales y una literatura académica robusta, sin embargo se evidencia significativas incoherencias en la gestión de incidencias, gestión de incidentes y respuesta a incidentes en la literatura, por tal motivo el articulo está enfocado a hacer claridad en la terminología utilizada a través de la distinción de términos según corresponda.

Una de las fortalezas que contiene este artículo es la inclusión de los principales estándares internacionales, que son fundamentales en todo modelo de gestión de incidentes. Entre los que se identifican: “cuatro directrices para la gestión de incidentes de seguridad de la información de CERT / CC, que forma parte del Instituto de Ingeniería de Software (SEI), ubicado en la Universidad Carnegie Mellon (CMU)”, “ El Manual de la seguridad informática de Respuesta a Incidentes (CSIRT) (West-Brown et al., 2003)”, “El estado de la práctica de los CSIRT (Killcrece, 2003) está diseñado para ayudar a los equipos nuevos y existentes en la

comprensión de las mejores prácticas y recomendaciones para el manejo de incidentes y servicios relacionados CSIRT". "Los modelos de organización de la publicación CSIRT (Killcrece et al., 2003) se centra en la selección del modelo adecuado para las capacidades de respuesta a incidentes de una organización. Definición de Procesos de Gestión de Incidencias de CSIRT: Una obra en curso (Alberts et al., 2004 proporciona una visión general de los procesos y funciones de apoyo y personas, la tecnología y los procedimientos que están involucrados en la gestión de incidencias)". Sin duda la información contenida en este artículo demanda un nivel de importancia significativo, al ser fuente de consulta durante el desarrollo, por la incidencia y estrecha relación.

Yijun Yu, et al en (Yu et al. 2015) proponen el desarrollo de un meta-modelo unificado en una herramienta automatizada para la evaluación formal e informal de los riesgos de seguridad en los sistema de información para ser abordados a través de catálogos de seguridad públicos en el proceso de desarrollo de software. El meta-modelo se denomina OpenRISA y responde a una nueva versión de un trabajo anterior denominado RISA enfocado al rastreo de riesgos durante el diseño de software. La aplicación de OpenRISA se centra en la evaluación de riesgos de seguridad en sistemas de gestión incluyendo riesgos formales e informales, siendo una herramienta para el ingeniero de seguridad en la construcción de casos de confiabilidad para ser aplicados durante el proceso de desarrollo de software.

OpenRISA se centra en un lenguaje de meta-modelo para la argumentación y evaluación del riesgo con el objetivo de obtener una comprobación formal de los riesgos hallados y valorarlos para determinar si son pertinentes. El modelo fue probado en dispositivos con entradas PIN, que son ampliamente utilizados por consumidores que realizan pagos a través de tarjetas de crédito en puntos de venta, para lo cual se utiliza cristología asimétrica. Posterior a la aplicación se realizó una priorización de los riesgos hallados clasificándolos en altos, medios y bajos según la comprobación realizada en los catálogos de seguridad públicos. Este trabajo se convierte en un ejemplo a consultar sobre las herramientas existentes para la evaluación y gestión del riesgo, siendo un apoyo durante el desarrollo de la tesis, sin embargo no tendría aplicabilidad en la construcción de la metodología para auditoria de seguridad de la información.

Kevin A. Barton, et al en (Barton 2014) realizan un investigación para determinar la influencia que tiene la participación de la alta dirección en la gestión de la seguridad de la información, analizando las motivaciones internas y externas para participar de la gestión. Se muestra que existe más motivación externa que internas debido a las presiones que se ven enfrentados con relación al tema. La investigación se desarrolló a través del modelo de encuestas en línea, en empresas medianas y pequeñas del sur de Estados Unidos con una muestra de 167 encuestados. La primera etapa de la investigación consistió en la revisión de la literatura existente identificando 5 subetapas: apoyo de alta dirección en la seguridad de la información, gestión de la seguridad de la información, cumplimiento de los empleados de la

política de seguridad de la información y controles, cultura de seguridad de la organización, el compromiso de la alta dirección. Posterior se desarrolló el modelo de encuesta a aplicar y el análisis de los datos recopilados; como etapa final el resumen de los resultados obtenidos y las recomendaciones de mejora. También surgieron futuras investigaciones con el fin de ampliar el estudio del tema.

El resultado refleja que con la participación activa de la alta dirección en los sistemas de gestión de seguridad de la información se alcanzaría los objetivos propuestos con altos estándares de calidad, definiendo que no solo influye la asignación de recursos necesarios. Se identificaron datos que concluyen que en las empresas donde la participación de los altos directivos es contante y comprometida, la motivación de los empleados de rangos inferiores por cumplir las políticas, la norma y participar de la gestión es más alta, que incluso no les molesta acatar los controles establecidos, porque tienen un referente superior. Dentro del trabajo de tesis propuesto, tiene importancia este tipo de artículos ya que una de los criterios de auditoria estaría enfocado al compromiso y participación en gobernanza con relación a la seguridad de la información en las organizaciones.

R. Shaw, Charlie C, et al en (Shaw et al. 2009) proponen una investigación basada en un experimento de laboratorio, cuyo objetivo es identificar la conciencia que tienen los empleados en las organizaciones con relación a la seguridad de la información bajo el argumento que una empresa puede incorporar toda la tecnología de punta que desee, sin embargo si sus empleados no desarrollan las prácticas adecuadas y aplican los controles requeridos los riesgos de seguridad están más propensos a ser efectivos. Se identificaron tres problemas asociados a la seguridad de la información: 1) la conciencia de seguridad de la información que se tiene en general, 2) las habilidades informáticas de los empleados, 3) los presupuestos de la organización. La investigación fue conducida sobre tres niveles identificados con relación a la conciencia de seguridad: percepción, compresión y proyección. La aplicación se realizó a 100.000 empleados a través de encuestas en 10 países; en donde se identifica que los empleados que trabajan a distancia tienen mayor conciencia de los riesgos de seguridad con relación a los empleados que trabajan en sitio.

La investigación también apunta a descubrir la eficacia en las alternativas de formación de los empleados con relación a temas de seguridad de la información y sus habilidades en medios informáticos, indicando que se haya mayor éxito en los medios multimedia utilizados con relación a medios de hipertexto; no obstante contrario a una de las hipótesis planteadas por los investigadores donde expresaban que los medios de multimedia podría ser más efectivos en el aprendizaje y toma de conciencia, los resultados arrojan mejores prácticas de seguridad de la información a través del aprendizaje de hipertexto, bajo el argumento que los empleados tienden a adquirir mayor conciencia y aplicar mejor los conceptos asimilados. Durante el análisis de resultados, se identificó que existe una alta fiabilidad del grado de

conciencia de la seguridad de acuerdo con los niveles planteados (percepción, compresión y proyección).

Para el trabajo en desarrollo es importante identificar estudios que indique el grado de conciencia y compromiso de los empleados en una organización con relación a la seguridad de la información, bajo el concepto que la seguridad de la información es un eje trasversal y que cada integrante tiene responsabilidad en su adecuado desarrollo; como lo indica el artículo, no es una cuestión de solo la incorporación de la tecnología y los métodos adecuados, un solo error humano puede causar graves daños y pérdidas a una organización; de ahí la importancia que las empresas trabajen en el aumento de la conciencia y el desarrollo de programas de formación que apunten a mitigar los riesgos en todos los niveles.

Las metodologías en los procesos de auditoría son necesarias para que un equipo de profesionales especializados en el área o áreas a auditar, siga una serie de mecanismos con el objeto de conseguir resultados homogéneos, entendibles y de análisis común; como si hubiese sido ejecutado por un solo profesional. Las auditorías en informática, tuvieron su auge en la época de los 80. Para este momento, normalmente las firmas auditoras tomaron como referencia determinada herramienta de metodología, para seguir el proceso de auditoría; especialmente en el área de seguridad de la información (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

Huma Rehman, et al en (Rehman et al. 2013) proponen un marco general para implementar un Sistema de Gestión de Seguridad de la Información en instituciones de educación y realizan sugerencias con el objetivo que sean adoptadas en redes y sistemas de información con criterios más seguros. El objetivo de este marco es hacer que las instituciones de educación en Pakistán conozcan los riesgos a los que se encuentran expuestas por el volumen de información que se gestionan al interior y exterior de las entidades a través de sus redes informáticas sin importar si el entorno de desempeño es pequeño, mediano o grande.

En la primera parte se hace revisión de la literatura, en segunda estancia, se propone una metodología que considera los principales criterios y controles de seguridad de la información a implementar para asegurar que el entorno académico tiene implementado las prácticas, políticas, procedimientos, tecnologías y medidas adecuadas para proteger los activos de información. Posterior ofrece un compendio de recomendaciones, para el entorno de desempeño educativo y los riesgos a los que se ven expuestas las instituciones, tomando como referencia los que hacen la diferencia con otros contextos de operación y en la última parte del trabajo se analiza los resultados de la implementación realizada. En este artículo, se hallan componentes de interés común; su enfoque está orientado a instituciones de educación superior. Por ello se destaca como un deferente para el diseño de la metodología. En el contenido se encuentra que la investigación fue desarrollada, siguiendo el patrón de buenas prácticas que recomienda la norma técnica ISO

27000 para implementar un sistema de gestión en seguridad de la información; este estándar será utilizado de manera relevante durante el desarrollo de la tesis.

Jenny Abromov, et al en (Anon n.d.) desarrollaron un método denominado método basado en patrones de desarrollo seguro (PBSD) para orientar el proceso de desarrollo y verificar el cumplimiento de patrones de seguridad a través de la construcción de esquemas orientados a hacer las bases de datos seguras. Su enfoque de desarrollo está basado en el lenguaje UML, por eso las técnicas y herramientas utilizadas son las mismas. El contexto de este trabajo es experimental y está enfocado a validar la calidad de las especificaciones de control en el acceso a las bases de datos, basados en las especificaciones de control de acceso en SQL y Oracle VPD, métodos reconocidos por su eficiencia y aplicabilidad.

El experimento fue aplicado en trabajos de estudiantes que se enfocaban en diseñar bases de datos y se evaluó el método haciendo la comparación con políticas de seguridad estándares que son contempladas durante los procesos de desarrollo de software, examinando las dimensiones de privilegios del sistema y estancias de granularidad de acceso. El trabajo reveló que existe una mejor gestión de la seguridad a través de PBSD y que los tiempos de diseño son menores y más consistentes con relación a la aplicación de otros modelos de seguridad. Uno de los inconvenientes hallados es que para su aplicación el desarrollador debe tener conocimientos expertos en seguridad de la información a fin que el método PBSD sea bien utilizado, motivo que hace que este trabajo sea una etapa preliminar para posteriores investigaciones que incluyan otras etapas del desarrollo diferentes al diseño de la base de datos.

Para el desarrollo de la tesis en auditoria constituye un referente de revisión para la contextualización en los diferentes modelos de requerimientos no funcionales de seguridad de la información desde las etapas de desarrollo. Sobre todo, el artículo incluye una recopilación importante de literatura alrededor del tema.

3.2 Fundamentos teóricos

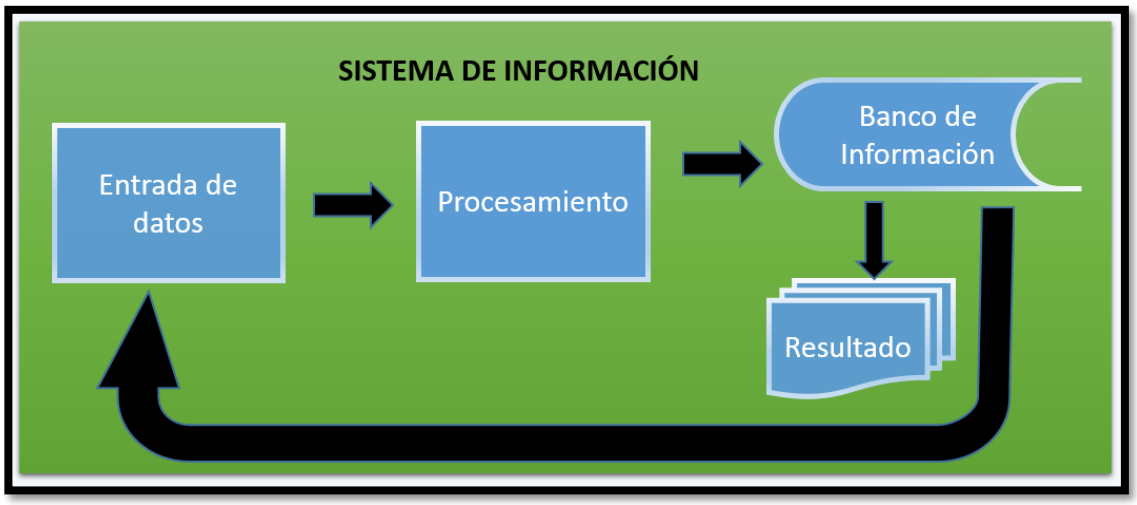
3.2.1 La Información

Es un recurso crítico para personas y organizaciones. Por ello debe ser tratada como un activo de valor superior y estar protegida en todo momento y circunstancia. La información es la base para la toma de decisiones estratégicas que definen el presente y futuro corporativo. Para conservar su carácter de valiosa y razonable, se requiere cumplir con las siguientes características: estar organizada, ser completa, generarse con exactitud, ser identificada como veraz, estar disponible y conservar un estatus de confidencialidad; según los niveles de seguridad y accesos definidos para las personas que hacen uso de ella (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

Los Sistemas de información

Los sistemas de información, cada vez se incorporan a las organizaciones con mayor fuerza y dependencia; su propósito es asumir el rol de eje estratégico que soporta la gestión, transformación y generación de nueva información, a partir de la sistematización de procesos y actividades. Una función principal de las plataformas tecnológicas, es soportar los objetivos de valor y operativos; como apoyo a las diversas dependencias que conforman una organización y a sus empleados. Una característica principal, es ser complemento a las políticas, lineamientos y procedimientos que se emiten desde los estamentos de gobierno corporativo, como contribución al cumplimiento de objetivos y la generación de valor agregado (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)(Hamidovic et al. 2015)(Manuel et al. 2012).

Ilustración 1. Esquema general



Fuente: Elaboración propia

Todo sistema de información, se debe identificar por el cumplir de ciertas características, que son necesarias para garantizar el desempeño de las organizaciones con estándares de calidad, el logro de objetivos estratégicos y para responder a sus compromisos. Dentro del grupo se resaltan las siguientes como las más destacadas: disponibilidad de la Información, suministro de la información de manera “selectiva”, variedad en la forma de presentación de la información, grado de “inteligencia”, tiempo de respuesta, exactitud, generalidad, flexibilidad, seguridad, reserva y amigabilidad [8].

3.2.2 Gobierno en TI

El marco de gobierno, en las organizaciones se ve reflejado por la creación y puesta en práctica de principios, políticas, estructuras y procesos. Un marco de gobierno

debe propender por que el personal vinculado a la organización adopte, entienda y practique una cultura organizacional estándar; que se ha establecido desde la alta dirección, en aras de velar por el cumplimiento de la legislación, los objetivos de valor y el logro de metas organizacionales; en beneficio de la comunidad interna y externa que la conforma. El gobierno define quién tiene la responsabilidad y capacidad de decisión para qué los procedimientos y actividades se cumplan, persiguiendo propósitos y logros colectivos. Una gestión que le compete al equipo de gobierno, es incentivar y motivar a los colaboradores para que la empresa asuma dentro de sus funciones diarias el desempeño responsable, con cero tolerancia a los incumplimientos y faltas a la ética (Hamidovic et al. 2015)(Isaca 2013).

La implementación de gobernabilidad y gestión en Sistemas Tecnológicos de Información (STI), le permite a cualquier organización avanzar hacia la eficiencia en el uso de sus recursos; para la prestación de servicios y alcanzar sus objetivos. Las empresas necesitan prácticas de gestión de STI rentables, fiables, efectivas y seguras. Un mal uso de los SIT puede resultar en un control deficiente de los servicios y procesos de tecnologías. Al tiempo, las faltas de medidas, pueden suponer un obstáculo para la mejora continua. Con alta frecuencia, las empresas experimentan fallos e incidentes en el uso de sus plataformas tecnológicas (Hamidovic et al. 2015).

Dahlberg y Kivijärvi (2006), definen que el gobierno de TI, debe ser integral y contemplar la gestión y control de los SIT desde la estructura estratégica; incorporando toda la cadena de valor tecnológica que la empresa utiliza para desarrolla su razón social. A mediados de los años 70, el concepto de gobierno en TI, se empieza a explorar y aplicar en la industria de la tecnología. A finales de los 90 adquirió el nombre de Gobierno en TI. Para ese momento tomó gran fuerza la incorporación de la tecnología como parte del desempeño de las organizaciones para la gestión, control de procedimientos y ejecución de actividades (Manuel et al. 2012). *Webb et al* (2006), destaca cinco elementos fundamentales en el gobierno de TI en 12 definiciones analizadas: alineamiento estratégico, entrega de valor de negocio a través de las TI, gestión del desempeño, gestión de riesgos, control y responsabilidades.

La necesidad de gestionar los procesos SIT ha llevado al desarrollo de marcos de referencias que recomiendan prácticas probadas y estandarizadas para validar la gestión tecnológica en las organizaciones. Los marcos, han sido considerados factor decisivo en la implementación de modelos de gobierno; una de las características, es el apoyo en ser guía para las actividades de documentación y estandarización con énfasis y especialidad en cada tema tecnológico, según corresponda. Las organizaciones dedicadas a la investigación y propuesta de este tipo de herramientas, parten de la base que el concepto tecnológico cada vez se amplia y que con el auge que ha alcanzado los servicios virtuales, se hace necesario segregar los temas por especialidades, conforme a las necesidades del entorno (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008). Un caso

específico ha sido la seguridad de la información, que ha ido tomando fuerza e importancia no solo en el contexto tecnológico; también a nivel de gobierno y la organización en general, soportada principalmente en la norma SO 27001. Norma emitida por la Organización Internacional de Normalización (ISO) (Isaca 2013). De ella se deriva la norma ISO 27002:2013, como un anexo. Estas normas se han ido incorporando con mayor frecuencia dentro de la gestión tecnológica, por la condición de vulnerabilidad y riesgo en la seguridad de la información dentro del contexto del desempeño de las organizaciones(Saint-Germain 2005).

3.2.3 Gestión del sistema de información en el gobierno de ti

Los sistemas de información, han aportado de forma relevante a la consolidación del modelo de gobierno de TI, porque a partir de ellos se pueden implementar programas que den la posibilidad de:

- Detectar mejoras y aplicar la corrección en el proceso de gestión de la información a través de la reingeniería y simplificación de los procedimientos.
- Alinear los puntos de vista departamentales desde un enfoque de procesos de gestión y gobierno de TI.
- Reducir el riesgo en el uso y la selección del software y el hardware.
- Apoyar que los niveles de seguridad de la información implementados sean los óptimos.
- Alinear la tecnología con los objetivos misionales, así como el uso de las herramientas de software, marco y metodologías de apoyo.
- Asegurar que la tecnología seleccionada este alineada con los objetivos de la organización, previo al diseño e instalación de los sistemas de información adecuados.
- Disminuir costos y riesgos en el uso y compra de tecnología, manteniendo seguridad y control en sus procesos organizacionales y logrando alta eficiencia en el manejo de la información.

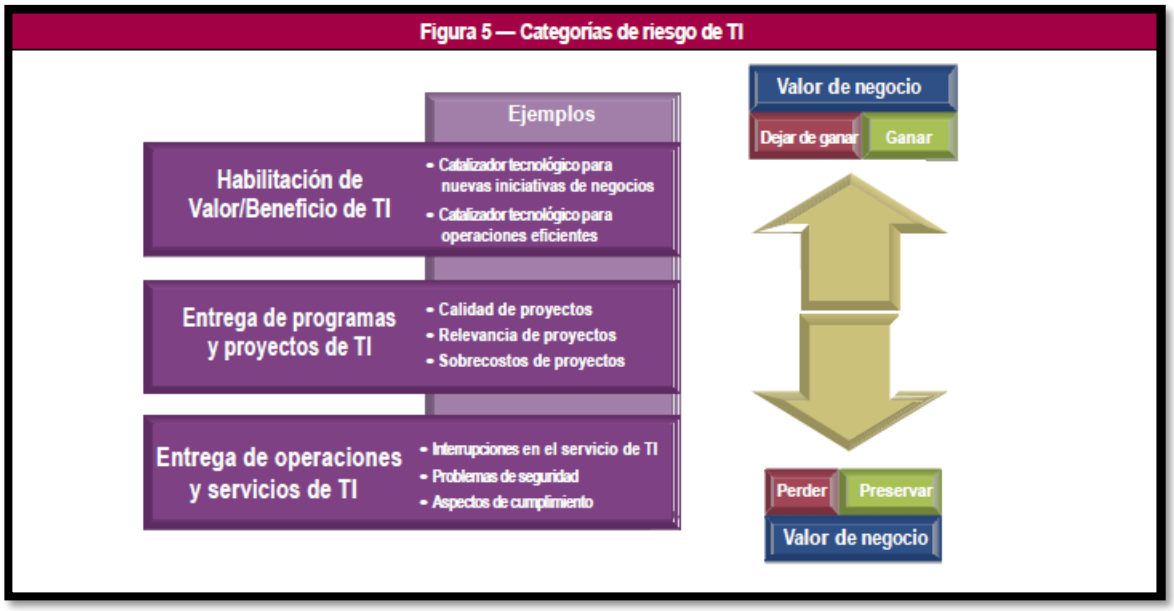
3.2.4 Control interno

El área de control interno está diseñada para apoyar el 100% de los procesos en las organizaciones. Su transversalidad en todos los procesos internos y externos, y en el ámbito técnico-económico, hacen que se convierta en un área relevante para el gobierno corporativo y el resto de la empresa. Su principal función es velar porque se implemente el sistema de control interno; compuesto por políticas, estándares, planes, procedimientos y estructuras organizativas; para proveer una garantía razonable del cumplimiento de los objetivos de valor. Una vez implementado el sistema, corresponde a los responsables, monitorear permanentemente el cumpliendo y aportar para evitar que eventos no deseados ocurran; o que si ocurren sean solventados sin mayores perjuicios para las organizaciones y con tiempos de respuesta aceptables (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.5 Gestión del riesgo

Generalmente el riesgo se define como la combinación de la probabilidad de ocurrencia de un evento y sus consecuencias. COBIT define el riesgo como un riesgo de negocio específicamente. El riesgo de negocio está asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa. Aunque los riesgos no siempre sean identificados ni determinados, siempre existen. En una organización existen riesgos inciertos que nunca han sido advertidos ni detectados, sin embargo actúan de forma inesperada; por ello es necesario prepararse anticipadamente para tratarlos de forma inmediata (Anon n.d.)(Isaca 2013).

Ilustración 2. Categorías de riesgo de ti



Fuente: ISACA, COBIT 5. 2013

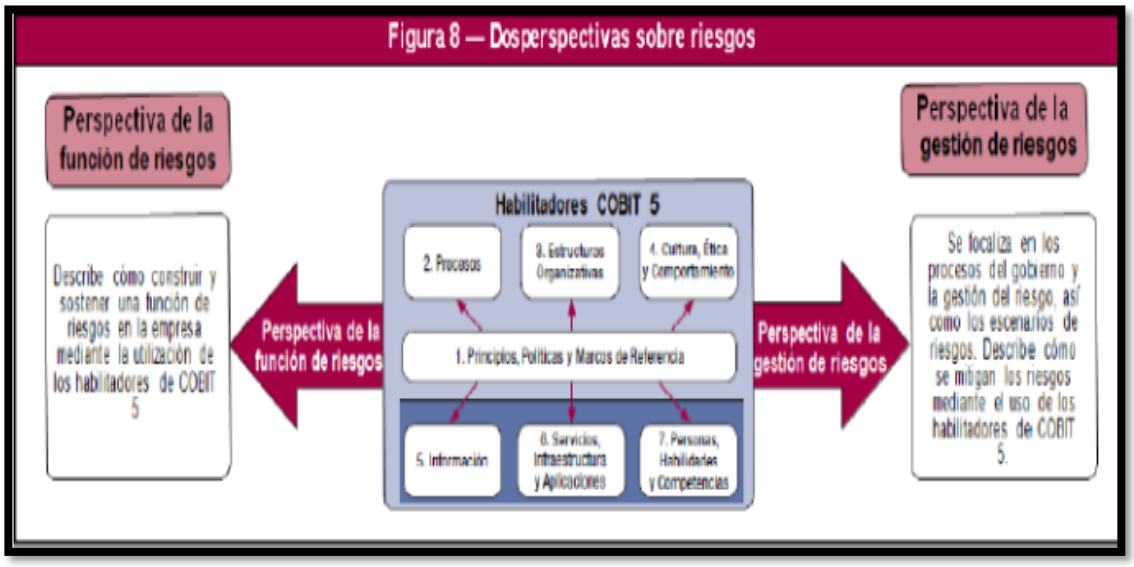
Es importante tener presente que el riesgo puede variar creciente o decrecientemente y se afecta por las decisiones que se tomen relacionadas a él. COBIT, ha definido la siguiente categoría del riesgo asociada a TI(Isaca 2013).

● **Riesgo en la habilitación de valor/beneficio de TI:** Relacionado con las oportunidades o perdidas de utilización de la tecnología implementada, con el fin de mejorar la eficiencia o efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocio (Isaca 2013).
● **Riesgo en la entrega de programas y proyectos de TI**: Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas; generalmente bajo

la forma de programas o proyectos que forman parte de portafolios de inversión(Isaca 2013).

● **Riesgo en la entrega de operaciones y servicios de TI**: Identificado con todos los aspectos del negocio como el desempeño normal de sistemas y servicios de TI, los que pueden destruir o reducir el valor de la Universidad(Isaca 2013).

Ilustración 3. Perspectivas sobre riesgo en COBIT



Fuente: ISACA, COBIT 5. 2013

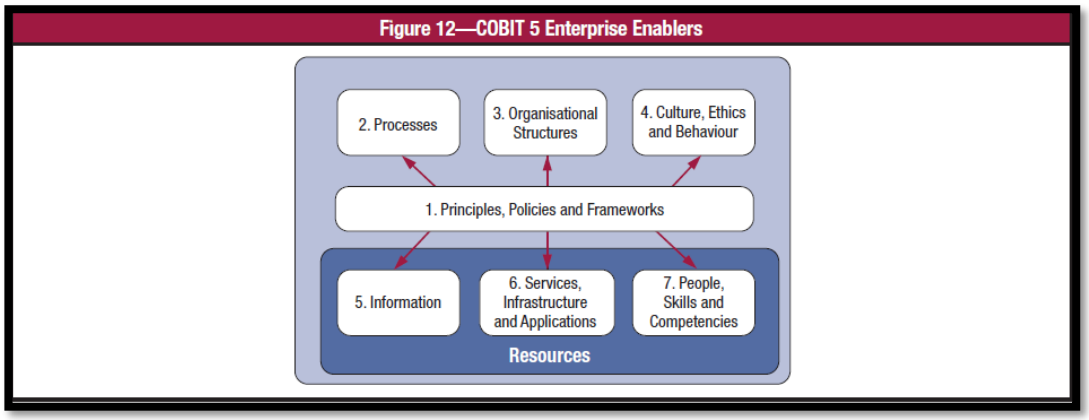
- **Perspectiva de la función de riesgos, 1**

Describe lo necesario para construir y sostener actividades principales de gobierno y gestión del riesgo en forma efectiva y eficiente. Para otros marcos de referencia, se concibe como la optimización del riesgo, en un solo objetivo clave de valor. En COBIT, se considera el gobierno y la gestión del riesgo como parte de una integración y combinación de los dos; teniendo como norte la gestión global de TI en la Organización. Para cada habilitador, la perspectiva de función de riesgos describe cómo contribuye de forma equitativa al gobierno y a la prevención de amenazas(Isaca 2013).

- **Perspectiva de la función de riesgos, 2**

Describe cómo el proceso principal de gestión de riesgos es apoyado por los catalizadores definidos por COBIT, se utilizan para la identificación, análisis, respuesta y reporte sobre los riesgos. Está perspectiva comprende el gobierno y la gestión; es decir, como identificar, analizar y responder al riesgo, y como utilizar el marco COBIT para dicho propósito. Requiere implementar procesos principales del riesgo. El riesgo se representa por los escenarios de riesgo(Isaca 2013).

Ilustración 4. Catalizadores corporativos de COBIT



Fuente: ISACA, COBIT 5. 2013

Todos los catalizadores definidos por COBIT, tienen un conjunto de dimensiones comunes que proporcionan una forma sencilla y estructurada de trabajarlos. Permiten la gestión de las interacciones y facilitan la obtención de resultados exitosos a partir de ellos(Isaca 2013). Las dimensiones según COBIT son:

- Principios, políticas y marcos de referencia.
- Procesos, incluyendo actividades y detalles específicos de la función del riesgo.
- Estructuras organizativas específicas para riesgos.
- Cultura, ética y comportamiento como factores determinantes del gobierno del
- riesgo.
- Información de tipos específicos de riesgos para facilitar el gobierno y la gestión del riesgo.
- Servicios, infraestructura y aplicaciones, capacidades de los mismos y requerimientos de estos para ofrecer su función relacionada al riesgo.
- Personas, habilidades y competencia requeridas por el recurso humano, vistos desde el riesgo.

En otra definición, la Norma Técnica Colombiana, provee la gestión del riesgo como la necesidad de identificar, prevenir y evaluar factores que puedan poner en riesgo a la organización y su entorno. Considera que las principales acciones de un plan de riesgos de seguridad de la información, debe contener las siguientes características (Ntc-iso-iec 2013)(Store 2013).

- Detección de las mejoras en el proceso de gestión de la información.
- Identificación de la situación de riesgo de activos informáticos, junto con su vulnerabilidad y amenazas.
- Probabilidad de ocurrencia de las amenazas e impacto.
- Condición de riesgo en las prácticas diarias.
- Análisis de la situación actual de la organización.
- Medición y comparación del nivel de madurez de los procesos de TI frente a las recomendaciones de un marco de referencia apto.

- Determinación de las acciones que se debe realizar a corto, mediano y largo plazo, integrado al Plan Estratégico de Tecnología.

3.2.6 Continuidad del negocio en gestión de seguridad de la información

Un plan de continuidad del negocio (BCP); es un proceso estructurado para que las organizaciones puedan recuperar y restaurar su operación en el menor tiempo, ante una situación que comprometa su estabilidad; a causa de un evento inesperado y con características de desastre. Es un plan logístico para la práctica de cómo se actúa frente a una emergencia, para reestablecer las funciones críticas, parcialmente o totalmente interrumpidas. Se recomienda que el plan de continuidad establecido para la seguridad de la información, esté integrado a los planes de gestión de toda organización. Según la disposición de la norma ISO 27002, los siguientes aspectos, deben ser contemplados dentro de la planeación y elaboración de continuidad (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)(Store 2013).

- Integrar a los procesos identificados como críticos, los requisitos de gestión de la seguridad; dando prioridad a las disposiciones de ley, recursos financieros, recursos físicos, talento humano, recursos tecnológicos.
- Realizar permanentemente análisis de consecuencias ante desastres, indisponibilidad de servicios, falencias en la seguridad.
- Desarrollar planes de contingencia cumplibles y efectivos con base en la disponibilidad de recursos y situación de las organizaciones.
- Planear mantenimientos de soporte técnico y ejecutarlos conforme a los cronogramas propuestos.
- Realizar permanentemente pruebas de pertinencia de la tecnológica implementada, según nuevas versiones, actualizaciones del mercado y a los nuevos requerimientos del negocio.
- Minimizar a la menor expresión posibles fallas de interrupciones que se asocien a desastres, accidentes, fallas en equipos de operación critica, fallas en sistemas de información.
- Activar a modo de prueba, de forma controlada los planes de recuperación previstos ante incidentes tecnológicos, desastres naturales, perdida de información, fallas en equipamientos técnicos.
- Formar e instruir al personal involucrado y responsable de garantizar la seguridad de la información sobre los diferentes planes implementados, políticas, procedimientos, medidas y controles. De igual forma de los mecanismos de trazabilidad y verificación de cumplimiento.

3.2.7 Metodologías para auditar asociadas a seguridad de la información

La metodología está considerada como una disciplina integrada por técnicas, métodos y estrategias; implementadas de forma sistemática para contribuir a la solución de un problema, adquisición de nuevo conocimiento o habilidades. Se

asocia a características como organizar el tiempo, un lugar de estudio, concentración, comprensión, intereses, guía de buenas prácticas, entre otros hábitos. En otras definiciones, se considera como la secuencia de un proceso riguroso, sujeto a evaluación sobre el estado de una acción con características específicas(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008). El resultado de una metodología aplicada, debe ser, presentar informe de actividades desarrolladas con su diagnóstico, según el análisis realizado. En el área de seguridad de la información, las características que se deben medir a través de una auditoria, se asocian a las amenazas, vulnerabilidad, riesgo e impacto hallado. Después de realizar un programa de auditoría de seguridad de la información, la organización deberá implementar los mecanismos y controles necesarios para que los riesgos se puedan: evitar, transferir, reducir o asumir (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.7.1 Metodologías más comunes enfocadas al análisis de riesgos

Existen diversas metodologías para análisis y gestión del riesgo de seguridad de la información; que han sido desarrolladas por organizaciones internacionales; formadas para estudiar el tema con rigurosidad y diseñar propuestas, que ofrezcan a las organizaciones alternativas de herramientas para detectar, analizar y prevenir el riesgo. El propósito general de una metodología es, identificar la ausencia de controles de seguridad de la información, para que, a partir de hallazgo y análisis, se presente un informe que sustente la situación de riesgo y se proponga planes de mejora (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.7.2 Metodología OCTAVE

Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE), desarrollada en Estados Unidos, por el Instituto de Ingeniería de Software (SEI) de la Universidad *Carnegie Mellon*. Su fin es evaluar los riesgos de la información en los servicios críticos de negocio(Software Engeneering Institute (SIE) at Carnegie Mellon University 2009). La técnica utilizada, se fundamenta en la planificación y consultoría estratégica en seguridad basada en el riesgo, apuntando al cumplimiento de los objetivos. Principalmente, está orientada a identificar riesgos operativos, riesgos en usuario final y prácticas de seguridad(Isaca 2013). Exige llevar la continuidad de la evaluación de la organización y del personal de las áreas de TI; basándose en la confidencialidad, integridad y disponibilidad de los activos de tecnologías e información valorados y considerados de misión crítica (Alberts, Crhistopher; Dorefee, Audrey; Stevens 2003)(Saint-Germain 2005). Octave consta de tres modelos: Octave, Octave – s, Octave Allegro y su aplicación tiene un enfoque práctico, evaluando siempre el nivel de riesgo en los siguientes escenarios(Shamala, Ahmad, and Yusoff 2013):

- Estrategia organizacional
- Estrategia operativa
- Estrategias de protección
- Usuario final
- Consolidación de información a partir de la matriz de seguridad
- Componentes de negocio
- Análisis de riesgo en los recursos y servicios críticos
- Prácticas de Seguridad de la Información
- Tecnología

3.2.7.3 Metodología MAGERIT

Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Estima que la gestión de los riesgos es una piedra angular en las guías del buen gobierno, para la gestión y análisis de riesgos de los sistemas de la información. Se han editado tres libros “Método”, “Catalogo de elementos” y “Guía de técnicas”; que sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos (Shamala et al. 2013)(Soediono 1989).

MAGERIT, realiza el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información; detallando los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, describe las actividades para realizar un proceso controlado en todas las fases de aplicación. Los aspectos prácticos, han sido considerados muy efectivos para la realización de un análisis; las características que identifican a MAGERIT (Soediono 1989).

- Es una metodología de carácter público, que pertenece al Ministerio de la Presidencia de España.
- Su fin de creación se sustenta en el estudio de los riesgos soportados por los Sistemas de Información, para recomendar medidas encaminadas a controlar el impacto del riesgo.
- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de que éstos sean controlados antes de que se materialicen.
- Ofrecer un método sistemático para el análisis de dichos riesgos.
- Ayudar a descubrir y planificar medidas oportunas para mantener los riesgos bajo control.
- Preparar los procesos de evaluación, auditoría, certificación y acreditación.
- Se relaciona directamente con el uso de las tecnologías de la información; proponiendo mejores prácticas y beneficios para el usuario; a través de buenas

prácticas que impacten y minimicen los riesgos; generando a la vez conciencia y confianza.

- Dentro de sus principales objetivos, esta ayudar a valorar y cuantificar el riesgo, de igual forma ofrece alternativas para la protección del activo hallado en riesgo; una vez identificado basado en técnicas y evitando la subjetividad e improvisación.
- Los elementos que considera más relevantes son: activos, amenazas, vulnerabilidades, impactos, riesgos y copias de respaldo.

3.2.7.4 Método PRIMA

Responde a un compendio de mecanismos de origen español para prevención de riesgos informáticos con metodología abierta. Se caracteriza por guiar las necesidades de los profesionales que desarrollan los proyectos asociados a planes de seguridad; por adaptarse a cualquier herramienta de apoyo metodológico. Tiene un compendio de instrumentos para identificar debilidades y falta de controles. En el desarrollo de la metodología incluye guías para ayudar a los profesionales que no tienen la suficiente experiencia para realizar una auditoría de seguridad de la información. Da la posibilidad de la generación de informes de los procesos de auditoria realizados. Se califica de tipo cuantitativo (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)8].

3.2.7.5 Metodología CRAMM

Metodología de análisis y gestión de riesgos, desarrollada por el CCTA, en el Reino Unido. Se define con el conjunto de actividades guiadas y coordinadas para el control del riesgo en una organización. Se define en tres grandes objetivos: Mejorar la seguridad en los sistemas de información, justificar el presupuesto dispuesto para el plan y herramientas de copias de respaldo, dar confianza en la credibilidad de la información (Analysis et al. n.d.)

CRAMM, realiza un análisis de riesgos cualitativos asociados con una herramienta de gestión. Los elementos esenciales de la recolección de datos, análisis y los resultados de salida que deben estar presentes en una herramienta automatizada de análisis de riesgos están cubiertos en las tres etapas de una revisión CRAMM: Identificar y evaluar los bienes, identificar las amenazas y vulnerabilidades calculando sus riesgos, Identificar y priorizar las medidas de defensa o contra medidas [40].

3.2.7.6 Metodología NIST SP 800:30

Desarrollado por el Instituto Nacional de Estándares y Tecnologías. Define los límites y operaciones en la gestión del riesgo para identificar amenazas y vulnerabilidad. Está definida en nueve fases. La gestión del riesgo está distrubida en cinco categorías del riesgo (Analysis et al. n.d.).

- Riesgos débiles: Bajo impacto.
- Riesgo con amenaza fuerte: Podría ser con alto impacto.
- Riesgos con alta posibilidad de ocurrencia: Pudiese ocurrir frecuentemente con presencia débil. Sus costos son aceptables dentro de los presupuestos.
- Riesgos con alta posibilidad de ocurrencia e impacto débil: Se pueden transferir a un tercero.
- Riesgos que se atienden en su orden de detección.

3.2.7.7 Metodología EBIOS

Creada por la Dirección Central de Seguridad de los Sistemas de Información de Francia, para identificar necesidades de seguridad de la información. Su razón de ser es establecer canales de comunicación efectivos entre clientes internos y externos de una organización en procesos de gestión de riesgos de seguridad de la información. Es compatible con las normas ISO, por lo que apoya el establecimiento de procedimientos para mejores mecanismos que den oportunidad de reconocer riesgos de seguridad. A través de esta metodología se puede identificar los riesgos de seguridad en los activos de la organización (Analysis et al. n.d.).

3.2.8 Auditoría

La Norma Internacional ISO 19011, define la auditoría como un proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen con los criterios auditados(Iso 2011). De acuerdo con ISACA, en el marco de referencia algunos de los principios fundamentales que rigen la auditoria son: formalidad, independencia, ética, normas profesionales, idoneidad, planificación, ejecución e información(Iso 2011).

Esquema general del ciclo de vida de auditoria

El ciclo de vida de una auditoria, está relacionado con el proceso que se debe seguir para realizar las actividades necesarias. Inicia con la planeación, que consiste en prever y provisionar los recursos necesarios para desarrollar el proceso. Ejecución: es la puesta en marcha de las actividades que fueron contempladas como parte de la auditoria a través de un plan de auditoria. Es necesario dejar registro y evidencia de cada actividad desarrollada. Revisión: Es la actividad de verificar la forma como fue desarrollada la auditoria para tomar acciones de mejora, una vez finalizado el proceso. Corrección: Implementación de planes de mejorar del programa de auditoria. El ciclo de vida también es conocido como el ciclo PHVA (planear, hacer, verificar y actuar)(Iso 2011).

3.2.8.1 Auditoría informática

Es una medida de control y prevención que se ha hecho necesaria en las organizaciones por el auge importante que ha tenido, en el uso de los sistemas de información. A medida que los SI son incorporados en las empresas, las amenazas y riesgos informáticos también han empezado a incrementarse por ser la información valorada como uno de los activos más importantes para decidir el presente y futuro de todo ente con base en su propia información. Su objetivo es ofrecer a las organizaciones evaluaciones y recomendaciones de controles internos y buenas prácticas, que son necesarios para lograr la protección de sus activos. Para el caso informático, hace referencia a: sistemas de información, bases de datos e infraestructura tecnológica en general(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

Según los autores Mario Piattini Velthuis, Emilio del Peso Navarro, Mar del Peso Ruiz y los 26 coautores que dieron origen al libro Auditoria de Tecnologías de Sistemas de Información, la auditoria informática, se subdivide en 13 áreas principales, denominadas, auditoria en: *outsourcing* de TI, seguridad física, de la dirección, de explotación, de bases de datos, técnicas de sistemas, desarrollo, seguridad de la información, redes, aplicaciones, Internet, video vigilancia, y reglamentaria de los datos de carácter personal. De las 13 áreas propuestas, para la preparación y elaboración del presente documento, tiene relevancia las auditorias en: *outsourcing*, dirección, bases de datos, de aplicaciones y seguridad de la información. Por la estrecha relación con la auditoria en seguridad de la información. Sin restar importancia a las otras, que en algún punto de su ejecución se interconectan con seguridad de la información (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.8.2 Auditoría en *outsourcing* de TI

La auditoría a los contratos de *outsourcing* tiene por objeto evaluar los criterios usados para la constitución de un contrato bajo esta modalidad. El contrato debe estar jurídicamente constituido por los representantes legales de las partes. Los elementos que debe contemplar el contrato son los siguientes (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008):

- Evaluar los criterios usados para la constitución de un contrato de *Outsourcing* jurídicamente constituido.
- Evaluar el cumplimiento de los acuerdos de nivel, las responsabilidades y elementos de relación para gestionar el proceso.
- Evaluar el modelo de gestión que evite controversias y permita la revisión continúa del contenido y del avance
- Evaluar la claridad entre de los productos contratados y como se esperan recibir.

- Evaluar los vínculos de responsable de la empresa con el proveedor, con objetivos concretos y establecer las cláusulas de penalización para el supuesto que no sean alcanzados.
- Evaluar los mecanismos necesarios para asegurar la continuidad del servicio en caso de rescisión[2].
- Evaluar las actividades de supervisión, control y mejora continua que se desarrollan como consecuencia de la valoración de los niveles de servicio.

3.2.8.3 Auditoría de la dirección

El auditor tendrá la responsabilidad de evaluar y validar que haya efectiva correlación entre el plan estratégico de la organización con los proyectos informáticos; encontrando articulación entre los planes de: dirección tecnológica, operativo anual, arquitectura de la información, recuperación ante desastres o en su defecto con los documentos equivalentes que validen la existente de estos. Otro aspecto a evaluar es la posición en la jerarquía de la empresa que ocupa la Dirección de TI, asegurando que tenga la autoridad e independencia suficiente frente a los usuarios de las otras unidades. La participación activa de la Dirección de TI, en los órganos de decisión de la organización depende de qué tan estratégica y efectiva sea la tecnología de la información para la empresa en el cumplimiento de sus objetivos de valor(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.8.4 Auditoría en bases de datos

Las bases de datos son reconocidas como el corazón de la información. Funcionan a través de tecnología independiente de la plataforma de aplicación, no obstante, necesitan interactuar entre sí y sincronizarse para formar los sistemas de información. Las auditorias en bases de datos, son practicadas regularmente para diagnosticar el estado y calidad de la información que se procesa a través de los SI. Unas de las actividades importantes de un auditor de bases de datos, es validar las leyes que las rigen y controlan; contra el proceso de gestión de las bases de datos de la organización. Una base de datos debe brindar confianza robusta sobre los criterios de calidad y seguridad, para detectar la confiabilidad de los datos y determina si son tratados adecuadamente(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).
COBTI, determina una serie de recomendaciones para realizar auditoria de bases de datos. Se destaca la evaluación en: Arquitectura de la información, el modelo corporativo de la arquitectura de información, el diccionario de datos corporativo y reglas de sintaxis de datos, la clasificación de datos, gestión de Integridad, Requisitos de negocio para la gestión de datos, planes de almacenamiento y

2 ***Rescisión***: *Es un verbo que hace referencia a la acción de dejar sin efecto una obligación legal o un contrato. Por lo tanto, se anula o cancela un acto jurídico que se había contraído con anterioridad.*

retención de datos, sistemas de gestión de bibliotecas de médicos, eliminación de datos, copia de datos, eliminación de datos, copia de datos, restauración de datos, seguridad de la información para la gestión de datos [43].

3.2.8.5 Auditoría de aplicaciones

Su finalidad es evaluar la forma como han sido desarrollados los productos de software, verificando cumplimiento de las etapas técnicas con respecto a las etapas de planificación, diseño, arquitectura. Principalmente se centra en evaluar las especificaciones de requerimientos frente al producto final. Para auditar sistemas de información, es importante tener en cuenta aspectos como: modelos de referencia y calidad externa e interna, procesos de evaluación de un producto de software (ISO, 1999), métricas como herramientas básicas de construcción y control de aplicativos, entornos para la evaluación de las aplicaciones, métodos específicos para auditar aplicaciones de software y buenas prácticas recomendadas para la construcción del software (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008).

3.2.8.6 Auditoría seguridad de la información

Al revisar los diversos tipos de auditoría informática, es válido concluir que la seguridad de la información, está inmersa de alguna forma en los tipos de auditoria descritos. La justificación, obedece a la necesidad de implementar controles y prácticas adecuadas para proteger la información. Esta auditoría, ha entrado a formar parte del modelo estratégico de las organizaciones, por la dimensión e importancia que toma la información. Siendo en muchos casos, la justificación para crea un área de seguridad informática. La necesidad de protección que tiene los gobiernos, sectores económicos, académicos y sociedad en general, determinan la importancia de la seguridad de la información (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)[8].

El gobierno y las organizaciones, a diario unen esfuerzos para generar leyes, políticas, mecanismos de tratamiento, protección y buenas prácticas que conlleven a preservar la confianza sobre su uso, operación y replicación de la información (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008). La función principal de una auditoría en seguridad de la información, es evaluar los controles y prácticas adoptadas en las organizaciones para validar los criterios de seguridad en la información. Estos criterios, están relacionados con la calidad, disponibilidad, fiabilidad, autenticidad y disponibilidad de la información [1].

3.2.9 Organizaciones para la gestión de la seguridad de la información

Son entidades que ha generado conocimiento a través de la investigación formal y la innovación permanente sobre mejores prácticas que aportan beneficio a las

organizaciones en la gestión de la seguridad de la información. Su principal objetivo, es proveer herramientas que aporten en la gestión de la seguridad de la información, la normalización de procesos y la prevención del riesgo informática. Este tipo de organizaciones, normalmente nacen a partir de grupos de investigación, asociaciones de gremios industriales o entidades sin ánimo de lucro, para quienes el tema tiene interés y relevancia por intereses colectivos o incidencias en las que detectan oportunidades de soluciones comunes(Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)(Isaca 2013).

Tabla 1. Principales organizaciones de gestión de la seguridad informática

SIGLA	Entidad	Descripción	Referencia
ISACA	Information Systems Audit and Control Association	Promueve estándares que apoyen el trabajo de los auditores de SI.	http://www.isaca.org
ISO	Organization for Standardization	Normas internacionales, que proporciona herramientas para hacer frente los desafíos globales de hoy.	http://www.iso.org
NIST	National Institute of Standards and Technology	Es una agencia federal fundada en 1901 para la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.	gsi.nist.gov

Fuente: Elaboración propia

3.2.10 Normas para certificar la gestión de seguridad de la información

Son documentos formales que detallan normas relacionadas con la seguridad de la información; emitidas por entidades independientes, es decir, sin carácter gubernamental. Su principal labor es promover la utilización de estándares a través de la emisión de recomendaciones bajo criterios de calidad para ser aplicados en todos los sectores corporativos a nivel mundial(Iso 2011)(Ntc-iso-iec 2013)(REDCLARA; TICAL 2015).

Tabla 2. Principales normas de seguridad de la información

Norma	Descripción	Referencia
ISO 27001 ISO / IEC (BS 7799)	Reconocida como el estándar por excelencia en Seguridad de la Información [8].	http://www.iso.org
	Gestión de la seguridad de la información.	
	Desarrollado por el Comité Conjunto IEC JTC ISO Técnica.	
ISO/IEC 27001:2013	Técnicas de seguridad, sistemas de gestión de seguridad de la información.	http://www.iso.org
ISO/IEC 27003:2010	Técnicas de seguridad, código de prácticas para los controles de seguridad de la información.	http://www.iso.org
ISO/IEC 27002:2013	Tecnología de la información, técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.	http://www.iso.org
Standards for IS Auditing [8]	Normas Generales para la Auditoria de los Sistemas de Información. (ISACA).	http://www.isaca.org
	S6. Realización de Labores de Auditoria.	
	S7. Reporte.	
	S8. Actividades de Seguimiento.	
IS Auditing Guidelines (ISAG) [8]	Directrices de Auditoría	http://www.isaca.org
	G3. Uso de CAAT	
	G8. Documentación de la Auditoria	
	G10. Muestreo de Auditoria	
	G35. Actividades de Seguimiento	
NTC – ISO 31000	Gestión del Riesgo Principios y Directrices	http://www.iso.org

Fuente: Elaboración Propia

3.2.10.1 Marco de referencia ITIL

Compuesto por un conjunto de buenas prácticas y recomendaciones para la administración de servicios de TI. Su enfoque se enmarca en la administración de procesos. Fue desarrollada a finales de 1980 por la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL). Se ha convertido en el estándar mundial de utilizado en la Gestión de Servicios Informáticos. En sus inicios fue guía para el gobierno de Ucrania; la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. ITIL, se estructura en publicaciones, que proporciona la guía necesaria

para ser considero un método integrado, siéndose a las especificaciones que hace el estándar de la ISO/IEC 20000: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio, mejora continua del servicio (Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz 2008)(McCallister, Grance, and Kent 2010).

3.2.10.2 Marco de referencia COBIT5

COBIT, es un marco de referencia para cumplir los objetivos de control sobre la información y recursos tecnológicos asociados. La función principal de COBIT es ayudar a las organizaciones a mapear sus procesos de acuerdo a las mejores prácticas recopiladas por ISACA. Fue desarrollado por Information Systems Audit and Control Association (ISACA), organización sin ánimo de lucro enfocada en el Gobierno y control de IT. La sigla COBIT, significa Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (por sus siglas en inglés: Control Objectives for Information Systems and related Technology). Este marco de referencia usualmente es implementado por compañías que realizan auditorías de sistemas de información. Está dirigido a buenas prácticas y controles en el gobierno de TI en lo que respecta a la gestión de la seguridad de la información, sobre la base de los procesos de negocios de la organización (Isaca 2013)(Ntc-iso-iec 2013).

COBIT 5, se orienta a proporcionar directrices que benefician la gestión de la seguridad de la información para la organización; representada en crea valor para todos los interesados a través de definiciones, actividades, procesos y recomendaciones. Da visión del gobierno a través de una guía detallada, que se compone de políticas, procesos y estructuras organizacionales. Se alinea con otros estándares de seguridad de la información. Aporta mecanismos e instrumentos para respaldar el gobierno y la gestión de la seguridad de la información en la empresa, mediante la definición de cinco principios base (Isaca 2013).

- **Satisfacer las necesidades de las partes interesadas**: Provee los elementos que considera son base para responder a los objetivo de valor en las organizaciones; tomando como referencia que cada empresa es un universo diferente, por ello debe crear su propia estructura realizando una adaptación de COBIT 5, según las necesidades de controles y segurimiento de seguridad que se requiera (Isaca 2013).

- **Cubrir la empresa extremo-a-extremo**: Orientado a cubrir todos los procesos y funciones de la empresa, por considerar que TI es un área trasversal a la organización. Determina que desde el gobierno corporativo debe verse reflejada la gestión de seguridad de la información; teniendo en cuenta los agentes externos que son proveedores o consumidores de los productos y servicios que

provee la empresa y que son relevantes en la gestión de TI, como activos de información y entidades de inspección y control(Isaca 2013).

- **Aplicar un marco de referencia único integrado:** Busca integralidad y alineación con otros estándares, en aras de buscar una fusión de buenas prácticas, principios en beneficio de las áreas de TI y las empresas en general(Isaca 2013).

- **Hacer Posible un Enfoque Holístico:** COBIT 5, define una serie de catalizadores (habilitadores), con los cuales persigue el propósito de hacer más eficiente y eficaz el gobierno y gestión de TI dentro de las organizaciones. Los catalizadores están definidos en cinco líneas que considera fundamentales para una gestión de seguridad de la información: Principios, políticas y marcos de trabajo; procesos, estructuras Organizacionales; Culta, Ética y Comportamiento; información, servicios, Infraestructura y aplicaciones, personas, habilidades y competencias(Isaca 2013).

3.2.11 Norma técnica colombia – NTC – ISO – IEC 27001[3]

La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), aprobaron y publicaron como estándar internacional un conjunto de normas que sirven como guía en la implementación de un SGSI, con rangos de numeración reservados que van desde la 27000 hasta la 27017 y desde la 27030 hasta la 27044. El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), adaptó algunas normas de ésta serie de acuerdo a la legislación Colombiano, facilitando a las empresas nacionales adoptar las medidas necesarias y certificar en ISO27001(Ntc-iso-iec 2013).

Esta norma ha sido creada como instrumento de gestión y apoyo para que las organizaciones implementen dentro de sus procesos de negocio, gestión y operación el sistema de seguridad de la información, adoptando prácticas idóneas que estén en sintonía con el desempeño estratégico, según la razón de existir de la empresa. La norma, recomienda que el establecimiento del sistema de seguridad de la información se oriente por los objetivos, la estrategia, la estructura, el tamaño y el nivel de organización de las empresas. Todos sus elementos deberán estar alineados con los requisitos de seguridad y se espera que su actualización sea permanente con base en el cambio y evolución que se va teniendo en cada estructura organizacional. Es fundamental que en todos los procesos estratégicos, organizacionales y de operación, se incluya la gestión de la seguridad de la información desde los procesos, los sistemas de información y controles de seguridad(Ntc-iso-iec 2013).

[3] “Esta norma es una adopción idéntica (IDT) por traducción ISO/IEC 27001:2013”

La norma NTC – ISO – IEC 27001, además de apoyar la implementación del sistema de seguridad de la información; apoya los procesos de auditoria a través de un compendio de requisitos necesarios para la planeación, la implementación, el mantenimiento, el mejoramiento y la valoración bajo los criterios que rigen la seguridad de la información (Ntc-iso-iec 2013)(McCallister et al. 2010). Algunos requisitos principales son:

- Conocimiento de la organización y su contexto.
- Comprensión de las expectativas y de las partes interesadas.
- Determinación del alcance del sistema de gestión de la seguridad de la información.
- Sistema de gestión de la seguridad de la información.
- Liderazgo y compromiso.
- Política.
- Roles, responsabilidades y autoridades en la organización.
- Planeación.
- Acciones para tratar riesgos y oportunidades.
- Valoración de riesgos de la seguridad.
- Tratamiento de riesgos de la seguridad.
- Objetivos de seguridad de la información y planes para lograrlo.
- Soporte.
- Recursos.
- Competencia.
- Toma de conciencia.
- Comunicación.
- Información documentada.
- Operación
- Planificación y control operacional.
- Valoración del riesgo de la seguridad de la información.
- Tratamiento de riesgos de la seguridad de la información.
- Evaluación del desempeño.
- Seguimiento, medición, análisis y evaluación.
- Auditorías internas.
- Revisión por la alta dirección.
- Mejora.
- No conformidades y acciones correctivas.
- Mejora continua.

3.2.12 Encuesta nacional de seguridad informática aplicada en Colombia

La encuesta nacional de seguridad de informática versión Colombia, es realizada por la Asociación Colombiana de Ingenieros de Sistemas - ACIS, a través de Internet. Su realización está avalada y promovida por la OEA , apoyando la difusión

y distribución entre sus países miembros. Es un referente para Latinoamérica y Colombia en el análisis de datos estadísticos en los retos de seguridad de la información, a los que se ve enfrentado los diversos sectores que mueven la economía en los países. La presente edición[4], contó con la participación de 121 encuestados quienes permiten evaluar la realidad del país en materia de seguridad de la información y/o ciberseguridad(ACIS 2016).

Su propósito principal es visualizar la realidad de la seguridad de la información en el contexto colombiano, contemplando el conjunto de roles y responsabilidades del Director de Seguridad de la Información, en ingles conocido como The CISO. Cargo que cobra mayor importancia en las organizaciones debido a los escenarios digitales, dinámicos y volátiles a los que se enfrenta la empresa por el auge y la demanda tecnológica para apoyar el desempeño eficiente de sus procesos de estrategia y operación. Para esta nueva edición, contempla nuevas preguntas que dan la opción de revisar las encuestas de años anteriores con el fin de identificar los ambientes actuales que viven las organizaciones en cuanto a seguridad de la información y permitir la actualización constante de la encuesta con base en los nuevos escenarios de evaluación de la seguridad de la información(ACIS 2016).

La encuesta busca conocer cómo las organizaciones han enfrentado los nuevos retos ante anomalías del momento. Un ejemplo es el Ramsomware[5], que recientemente hace presencia en el mundo digital de forma global. También busca identificar las tendencias de monitoreo inteligente de amenazas, la construcción de una cultura, gobiernos y gestión de seguridad de la información en las empresas. Con respecto a los estándares, la encuesta busca conocer la forma que han utilizado las organizaciones para la adquisición de herramientas que aporten a la cultura, gobierno y gestión de la seguridad de la información. Para finalizar la encuesta busca determinar los retos en preparación de los profesionales responsables de la seguridad informática en las organizaciones, con el fin de hacer eficiente la gestión de la seguridad de la información(ACIS 2016). A continuación se presenta los datos estadísticos de los principales hallazgo del estudio. Se destaca una tendencia de los responsables de la seguridad de la información por aprender más sobre los procesos y lenguajes organizaciones para aportar soluciones que sincronicen funcionalidad con protección dentro del marco de negocio (ACIS 2016).

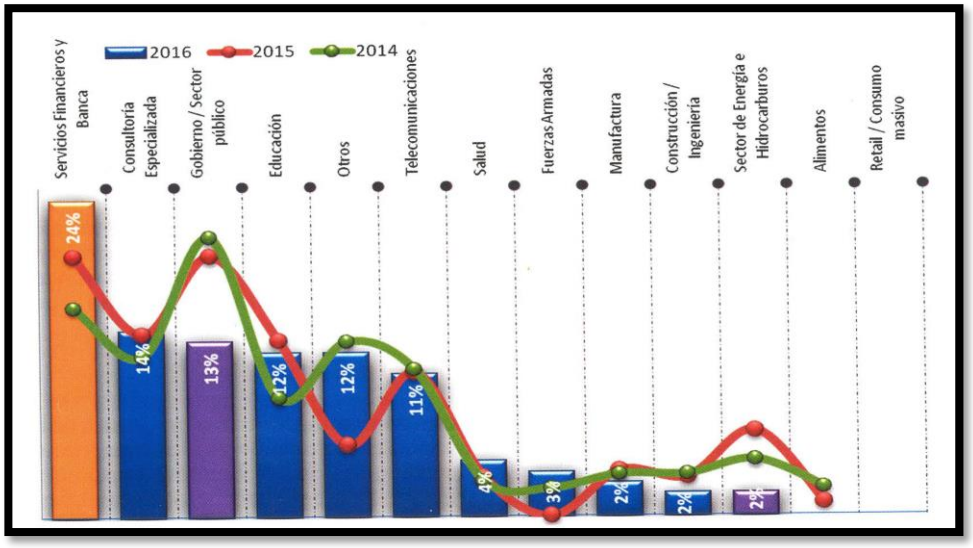
[4] Sistemas, Fraude Informática: viejos trucos, nuevos entornos. No. 139 Abril – Junio 2016 – ISSN0120-5919).

[5] **Ramsomware**: Definido como software malicioso, que al infectar el equipo da la posibilidad de tomar control remoto para encriptar los archivos y que el ciberdelincuente se quede con el control de la información.

3.2.12.1 Resultados de la aplicación de la encuesta

A continuación, se presentarán los resultados que obtuvo la Asociación Colombiana de Ingenieros de Sistemas durante la aplicación de la encuesta. La muestra estuvo representada por empresas de los diversos sectores que conformar el sistema económico e industrial del país.

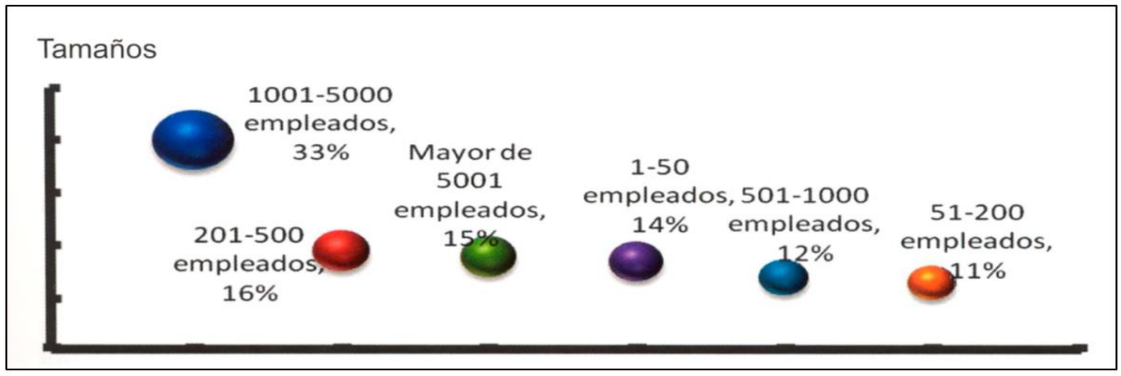
- **Gráfica 1. Sectores de participación**



Fuente: ACIS – Revista “Sistemas, Fraude Informático”

La gráfica 1, muestra el resultado de la comparación entre los años 2016 – 2015 – 2014, se evidenciando que la mayor participación se dio en el sector financiero. Decreció la participación en los sectores gobierno e hidrocarburos. El sector de la educación se mantuvo con promedio medio, ocupando el 4 lugar con un 14% con respecto al sector financiero(ACIS 2016).

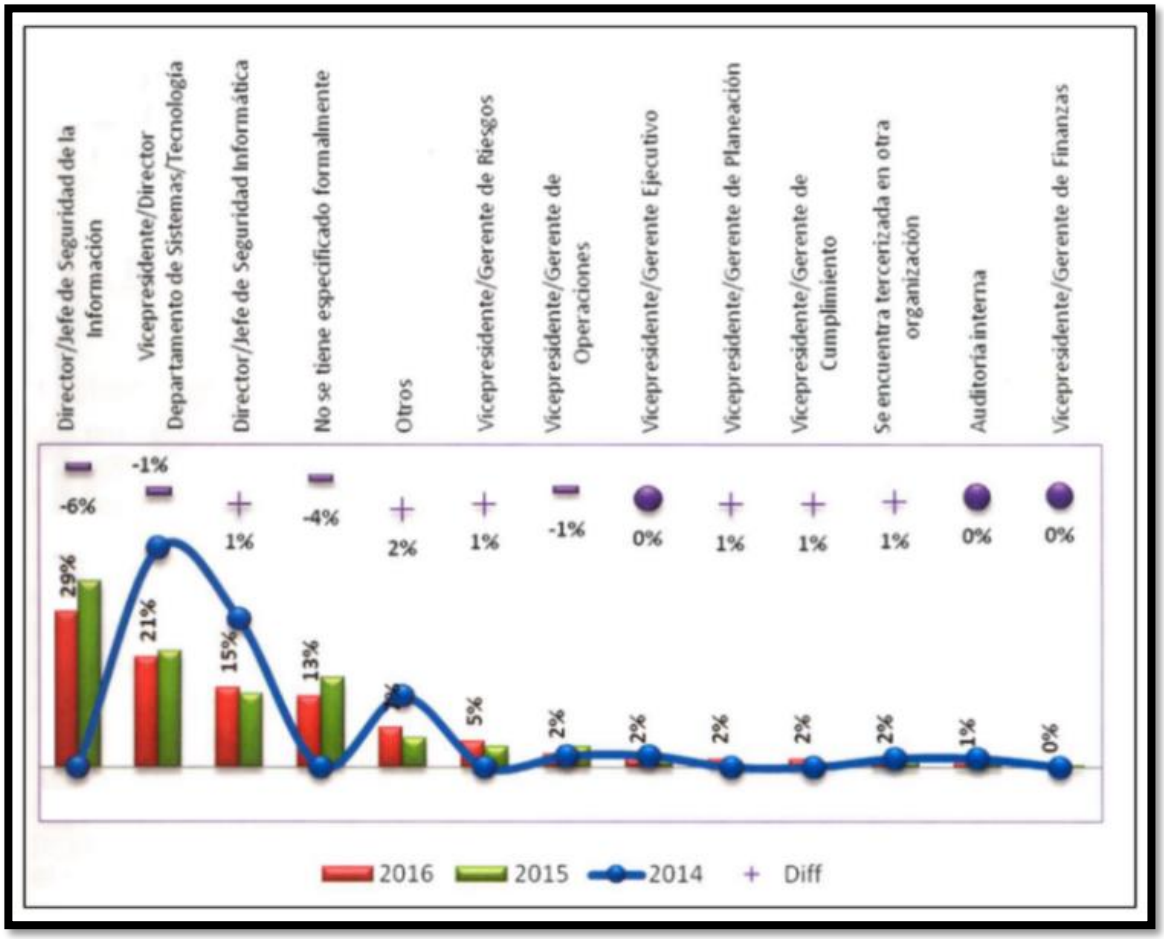
- **Gráfica 2. Medición por tamaños de las empresas**



Fuente: ACIS – Revista “Sistemas, Fraude Informático”

En la gráfica 2, se muestra la participación que tienen las empresas en el año 2016. Según las empresas encuestadas, el rango de empleados oscila entre 1001 – 5000. Está condición depende del tamaño de la empresa y de su actividad económica(ACIS 2016).

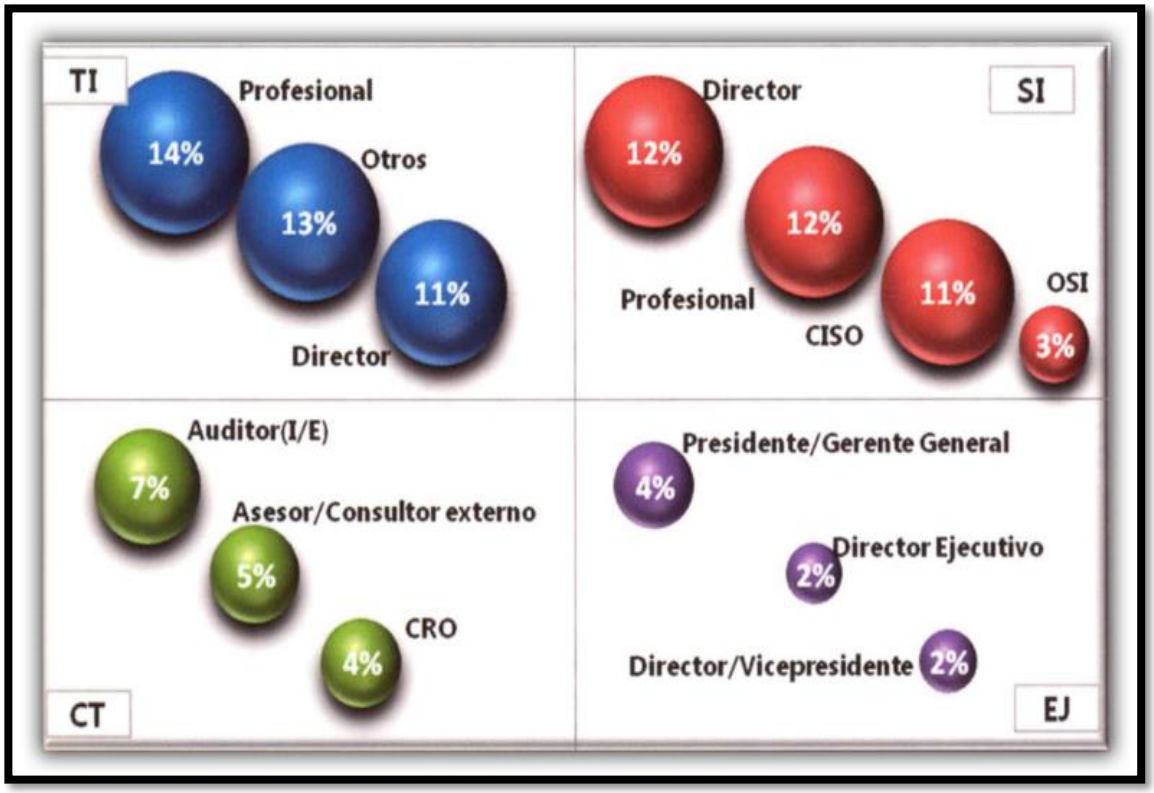
- **Gráfica 3. Dependencias de la seguridad**



Fuente: Asociación Colombiana de Ingenieros de Sistemas

En la gráfica 3, muestra las diversas dependencias que tienen la responsabilidad de la seguridad de la información, notándose que cada vez depende menos de las áreas de tecnología, también se evidencia un decrecimiento de la dependencia de un director de seguridad de la información, a su vez aumentando en un 1% en otros cargos que se responsabilizan de gestionar la seguridad, como gerentes de planeación, servicios, de cumplimiento. Se evidencia una leve tendencia a tercerizar la seguridad de la información, como otra alternativa para su gestión en las organizaciones(ACIS 2016).

- **Gráfica 4. Cargos de los encuestados**



Fuente: ACIS – Revista “Sistemas, Fraude Informático”

En la gráfica 4, se evidencia que las empresas del contexto colombiano han ido tomado conciencia de la gestión de seguridad de la información en sus organizaciones; por tal motivo la encuesta ha sido respondida por diferentes áreas de la organización, obteniendo los siguientes datos: cargos asociados a áreas de seguridad de la información 38%, cargos directamente relacionados con seguridad de la información 38%, áreas de control 16%, y en un 8% los cargos de nivel directivos; esta muestra evidencia que la seguridad de la información en la empresa colombiana ha pasado a ser preocupación y responsabilidad de diversos niveles en las organizaciones.

En el diseño de la metodología tiene relevancia este tipo de estudios, porque motiva a las áreas de control para participar de este estudios y en encuestas y así permitir obtener información estadística formal para la mitigación de los riesgos asociados a la gestión de la seguridad de la información. Mediante el diagnostico oportuno y la implementar de planes de mejora continua permanente(ACIS 2016). También para evidenciar ante las jerarquías estratégicas de la organización la necesidad de asignar talento humano y recursos económicos para una gestión coherente y responsable para la preservación y conservación adecuada de los activos de información.

- **Gráfica 5. Hallazgos más significativos**

Ítem	Descripción	Variación frente al año (2015)
1.	Roles en la organización	
➡	Primer respondiente / gestionador de incidentes de seguridad, este rol creció de manera importante frente al año inmediatamente anterior.	17%
➡	Es el rol de Oficial de Seguridad Informática (ISO), otro de los roles que la organización mas a desarrollado en Colombia y crece frente a años anteriores.	9%
2.	Actividades realizadas por el responsable de seguridad	
➡	Velar por la protección de la información personal	13%
➡	Seguimiento de prácticas en materia de protección de la privacidad de la información personal	12%
➡	Evaluar la eficiencia y efectividad del modelo de seguridad de la información	8%
3.	Activos de Información	
➡	Las organizaciones cuentan con declaraciones formales relacionadas con los activos de información	11%
4.	Información de fallas de seguridad	
➡	Notificación de proveedores	9%
➡	Notificación de colegas	8%
5.	Mecanismos utilizados	
➡	SIEM (Security Information Event Management)	8%
➡	Las herramientas Anti-DDOS	7%
6.	Conciencia de la alta dirección	
➡	La alta dirección entiende y atiende recomendaciones en materia de seguridad de la información.	7%
7.	Notificación de los incidentes de seguridad	
➡	Autoridades locales/regionales.	7%

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

Esta sección está dedicada a mostrar las variaciones que ha tenido la encuesta de 2016 con relación al año 2015, tanto en variaciones positivas como en decrecimientos. En la tabla1, se evidencia que el cargo de Oficial de Seguridad ha tomado especial relevancia; según la encuesta en las empresas colombianas en un 48% tiene un CISO y en un 27% un Oficial de Seguridad, siendo coherente con tendencias mundiales a tener en sus organizaciones responsables de seguridad de la información de acuerdo con la encuesta realizada por la empresa PwC(ACIS 2016).

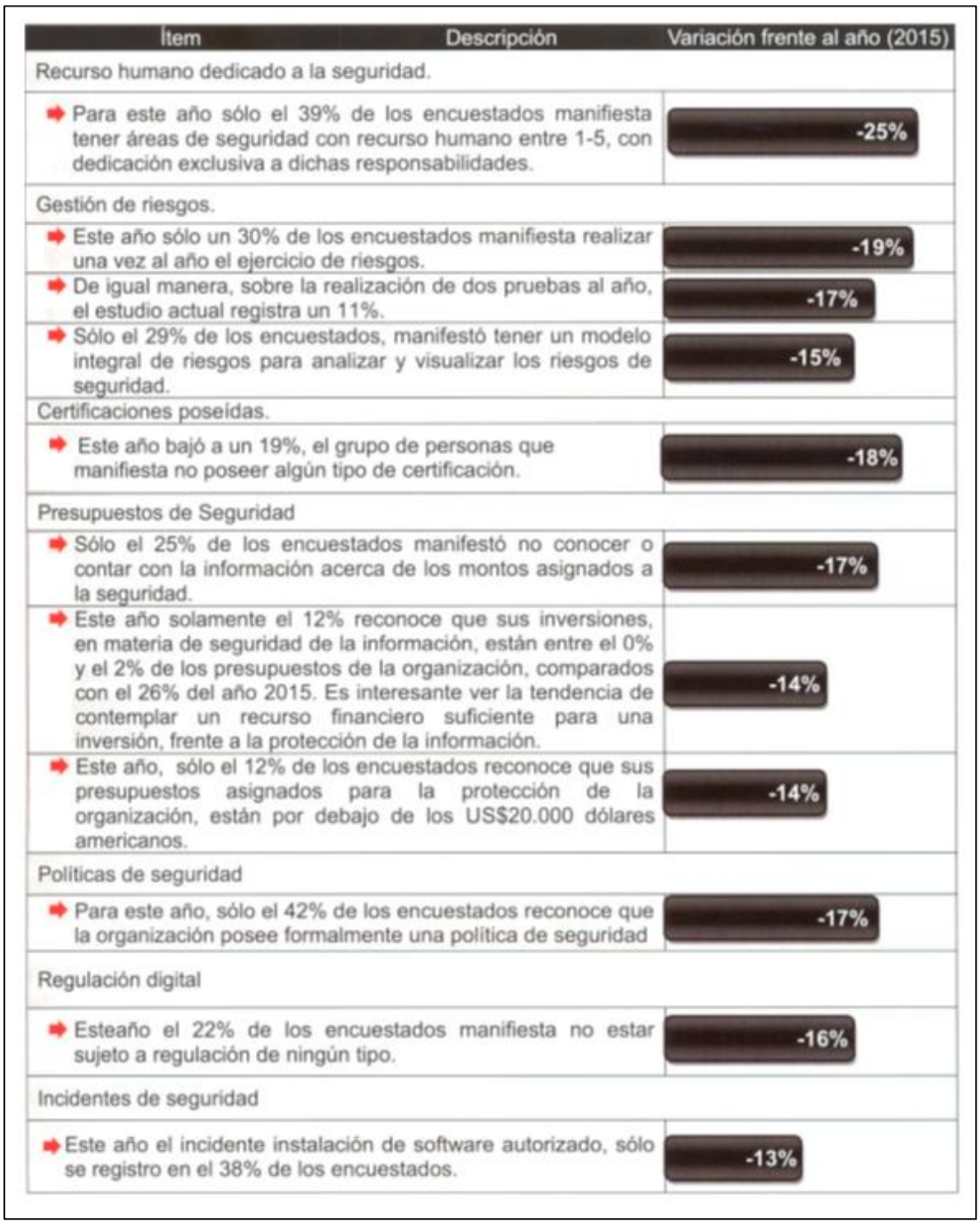
De las nuevas responsabilidades que se identifica para el gestor de seguridad de la información en Colombia, la gestión de protección de datos personales; respondiendo a las exigencias de la ley 1581 de 2012 que reglamenta velar por la adecuada gestión y control de los datos personales las personas que intervienen en el desempeño de una empresa y sus procesos. Para el año 2016 un 71% de los encuestados identifica la necesidad de tener directrices establecidas para gestionar la seguridad de la información con mayor capacidad y competencia, basados en una gobernabilidad de los datos(ACIS 2016).

La conciencia en gestionar la seguridad de la información es otro dato importante que se identificó en la encuesta para el año 2016 en Colombia. La muestra representa un 26% en donde los encuestados manifiestan que los directivos comprenden de forma positiva que es necesario atender los temas relacionados con la seguridad de la información y acata recomendaciones al respecto. Esta tendencia se refleja en el informe de ciberseguridad que realizó ISACA y RSA, en donde se evidencia que el 36% de los directivos en las empresas se preocupan por gestionar la seguridad de la información en sus organizaciones (ISACA 2015)(ACIS 2016).
En la encuesta de la firma Pwc, se identifica que el 45% considera que los cargos directivos en las empresas participan de actividades relacionadas con la gestión de la seguridad de la información en sus empresas(ACIS 2016).

La normatividad colombiana que rige la gestión de la seguridad de la información el 22% manifiesta no estar sujeto a una regulación, frente a un 38% que reporta el mismo dato en el año 2015; su interpretación se da en que cada vez más las organizaciones, la alta dirección y los responsables directos de seguridad de la información reconocen que cada vez más se conoce la regulación legislativa y entiende su importante de incorporarla a la organización (ACIS 2016).

Dentro de la legislación que aplica para Colombia se destaca la ley 1581 que hace referencia a la protección de datos personales, ley 1712 o ley de transparencia y el nuevo CONPES de Ciberseguridad. Estas regulaciones dejan clara evidencia de la importancia que cobra la seguridad de la información entre los entes de gobierno y el compromiso de las organizaciones por su aplicación (ACIS 2016). En cuanto a la política seguridad de la información escrita, aprobada por la alta dirección e informada el 42% manifiesta tener conocimiento en el 2016.

- **Gráfica 6. Variaciones negativas**



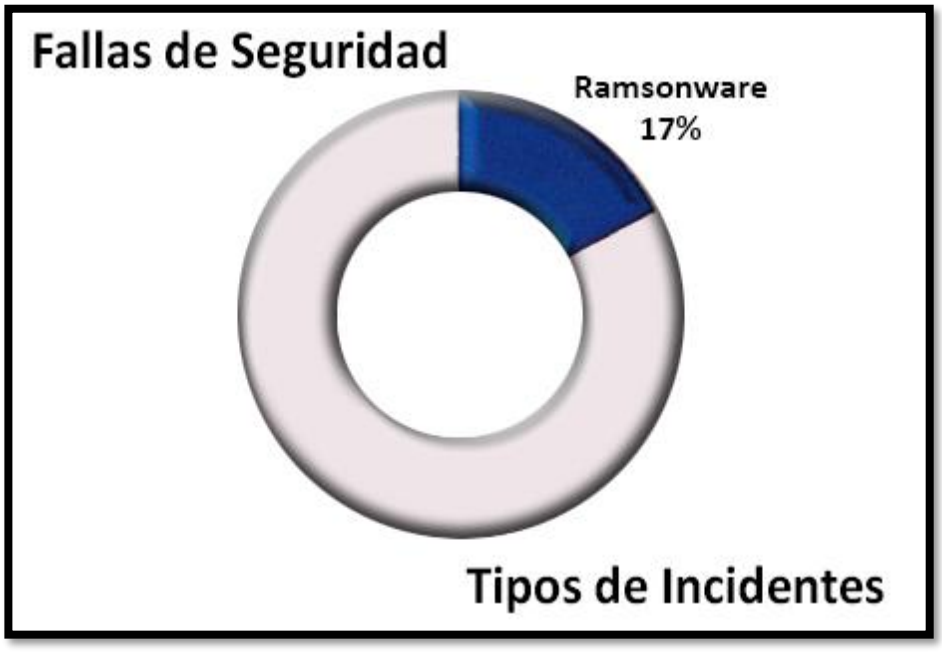
Ítem	Descripción	Variación frente al año (2015)
Recurso humano dedicado a la seguridad.		
➡ Para este año sólo el 39% de los encuestados manifiesta tener áreas de seguridad con recurso humano entre 1-5, con dedicación exclusiva a dichas responsabilidades.		-25%
Gestión de riesgos.		
➡ Este año sólo un 30% de los encuestados manifiesta realizar una vez al año el ejercicio de riesgos.		-19%
➡ De igual manera, sobre la realización de dos pruebas al año, el estudio actual registra un 11%.		-17%
➡ Sólo el 29% de los encuestados, manifestó tener un modelo integral de riesgos para analizar y visualizar los riesgos de seguridad.		-15%
Certificaciones poseídas.		
➡ Este año bajó a un 19%, el grupo de personas que manifiesta no poseer algún tipo de certificación.		-18%
Presupuestos de Seguridad		
➡ Sólo el 25% de los encuestados manifestó no conocer o contar con la información acerca de los montos asignados a la seguridad.		-17%
➡ Este año solamente el 12% reconoce que sus inversiones, en materia de seguridad de la información, están entre el 0% y el 2% de los presupuestos de la organización, comparados con el 26% del año 2015. Es interesante ver la tendencia de contemplar un recurso financiero suficiente para una inversión, frente a la protección de la información.		-14%
➡ Este año, sólo el 12% de los encuestados reconoce que sus presupuestos asignados para la protección de la organización, están por debajo de los US$20.000 dólares americanos.		-14%
Políticas de seguridad		
➡ Para este año, sólo el 42% de los encuestados reconoce que la organización posee formalmente una política de seguridad		-17%
Regulación digital		
➡ Esteaño el 22% de los encuestados manifiesta no estar sujeto a regulación de ningún tipo.		-16%
Incidentes de seguridad		
➡ Este año el incidente instalación de software autorizado, sólo se registro en el 38% de los encuestados.		-13%

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

Son criterios que se identifican en la encuesta, como menos relevantes con relación a encuestas de años anteriores. De los datos a destacar se identifica que el 39% de las personas encuestadas manifiestan que para el 2016 las áreas de seguridad de la información cuentan con los recursos establecidos, marcando una diferencia decreciente con relación al año 2015 en donde un 64% manifestó que las áreas de seguridad de la información poseían recursos específicos. Tendencia que es contraria a los datos de encuestas globales. Sin embargo, se muestra un dato positivo al evidenciarse que únicamente un 3% no posee recursos para gestionar la seguridad de la información. Otro dato analizado es la baja preocupación por gestionar el riesgo, solo el 30% manifestó que realiza evaluación del riesgo en Colombia, datos para el año 2016. Para el año 2015 el dato obtenido fue del 49%, evidenciándose un decrecimiento en la evaluación de la gestión del riesgo del 19%. De igual forma el 11% manifiesta realizar evaluación 2 veces al año, frente a un 27% que manifestó el mismo el dato el año pasado(ACIS 2016).

Con relación a presupuestos destinados para gestionar la seguridad de la información el 25% manifiesta no tener conocimiento de los rubros asignados, al comprar con el 2015 un 42% manifestaba la misma información; por lo que se puede concluir que a las organizaciones cada vez más les interesa destinar presupuestos para gestionar la seguridad de la información.

- **Gráfica 7. Fallas de seguridad**



Fuente: ACIS – Revista “Sistemas, Fraude Informático”

Entre las fallas de seguridad para el año 2016, se muestra un importante crecimiento del malware tipo Ransomware con 17%, lo que obliga a considerarlo como una

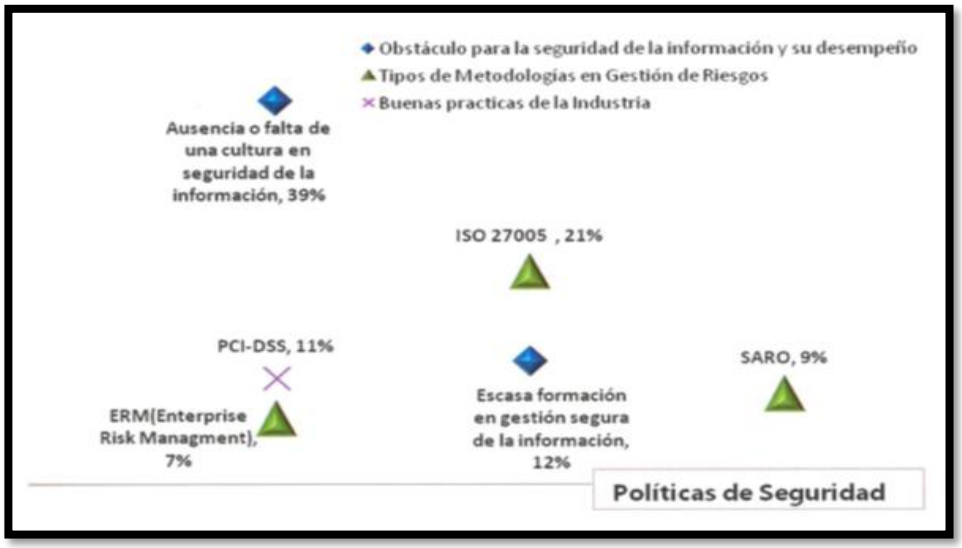
anomalía presente a la que se exponen cada vez con mayor fuerza los activos de información en las organizaciones (ACIS 2016).

- **Gráfica 8. Herramientas y prácticas de seguridad**

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

Entre los mecanismos de protección usados, se destaca servicios de inteligencia de amenazas con 11%, es considerado como una herramienta válida para la detención temprana de incidentes de seguridad, permitiendo ser preventivos y mejorar la gestión de la seguridad de la información (ACIS 2016).

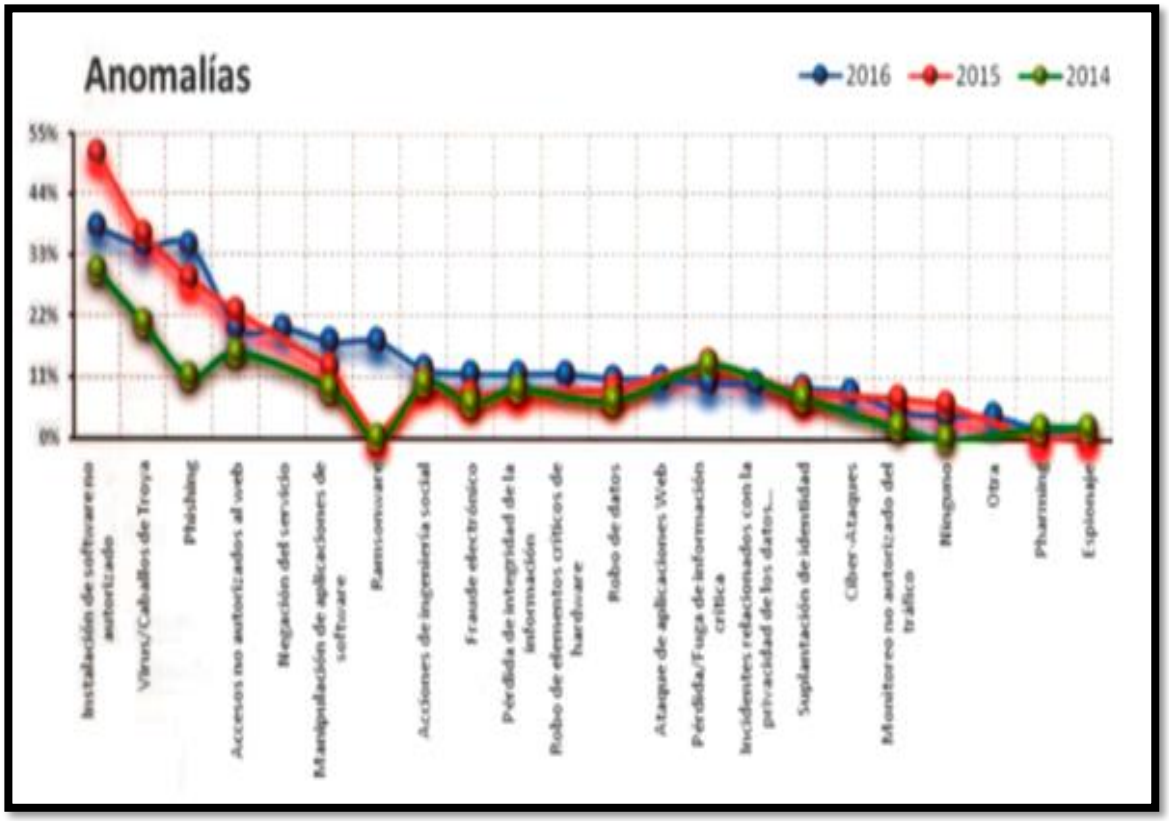
- **Gráfica 9. Políticas de seguridad**



Fuente: ACIS – Revista “Sistemas, Fraude Informático”

En la gráfica 9, se muestra que el 39% de los encuestados manifiestan que en las organizaciones se percibe ausencia de cultura en la seguridad de la información. En cuanto a metodologías para gestionar la seguridad de la información se identifican las siguientes como las más utilizadas en el 2016 para gestionar el riesgo. Para Colombia se muestra entre las más utilizadas: ISO 27005 e ISO 31000 en la identificación de riesgos de seguridad de la información. Con relación a la aplicación de buenas práctica para gestionar la seguridad de la información se incluye PCI-DSS como una buena opción al obtener un resultado de 11% entre los encuestados que dicen hacer uso de ella (ACIS 2016).

- **Gráfica 10. Variaciones en tipos de incidentes**



Fuente: Asociación Colombiana de Ingenieros de Sistemas

En la gráfica 10, se evidencia la presencia que ha tenido el Ransomware como un malware que hace presencia en las anomalías de los activos de información. En cuando a la instalación de software no autorizado, se evidencia que las organizaciones han mejorado sus prácticas y controles. El Phishing al igual que en los años anteriores se muestra como una de las prácticas de ataque más utilizadas, no solo en Colombia, se muestra como una tendencia mundial (ACIS 2016).

- **Gráfica 11. Herramientas de protección**

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

La gráfica 11, muestra que las organizaciones se preocupan cada vez más por incorporar y mejorar sus mecanismos y herramientas de protección. La soluciones de AntiMalware, sistemas de gestión de autenticación, VPNS y Firewall son los mecanismos de control tradiciones, en los que se ha detectado una disminución; dando paso al crecimiento de otros como los sistemas biométricos, SIEM como herramientas eficientes de monitoreo.

Se evidencia una necesidad de incorporar diversas opciones en mecanismos y herramientas que le permita a los responsables de la seguridad de la información hacer mejor gestión y prevención de las amenazas en materia de seguridad; teniendo en cuenta que estas siempre tienen una tendencia al aumento y sobre todo en los nuevos entornos que exige una mayor ciberseguridad (ACIS 2016).

- **Gráfica 12. Diagrama de covey adaptado**

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

La gráfica 12, muestra que la relación entre la gestión de la seguridad de la información y la alta dirección en las organizaciones cada vez es más estrecha; siendo cada vez más frecuente que participen de las decisiones que se toman en cuanto a seguridad de la información. Esta labor principalmente se le atribuye a los CISOS en las organizaciones, quienes cada vez adquieren habilidades gerenciales y lenguaje que le permite interactuar de forma más eficiente con los gerentes y hacerles llegar el mensaje de la necesidad de involucrarse en los temas y decisiones de seguridad. En la encuesta se indaga por la conciencia que tienen los directivos en las organizaciones con la seguridad, su nivel de involucramiento y responsabilidad, haciendo uso de la matriz de los 4 cuadrantes de Covey con una adaptación para hacer una relación entre la variable responsabilidad (eje X) vs compromiso (eje Y). Dentro del cuadrante se ubican los siguientes conceptos: rendimiento y resilencia de la seguridad, identificándose que es alta la responsabilidad y el compromiso. Se evidencia que los directivos en las organizaciones se involucran en la toma de decisiones y asumen los riesgos asociados a la seguridad de la información(ACIS 2016).

En el cuadrante de supervivencia de la seguridad, se evidencia un compromiso bajo y una responsabilidad alta. Se identifica que la alta dirección entiende y acata las recomendaciones de seguridad, aunque no se involucra en la gestión, tiene claro que es importante y necesario entender los riesgos a que se enfrenta la

organización en cuanto a seguridad de la información. En el cuadrante de fatiga de la seguridad, se determina que tanto compromiso como responsabilidad son bajos por parte de la alta dirección en lo referente a seguridad de la información, al igual que los riesgos asociados. Muestra que los directivos no se involucran en los procesos ni toma de decisiones en cuento a seguridad de la información. Cuadrante de receptividad de la seguridad, en esta zona se denota bajo compromiso y alta responsabilidad, en donde se evidencia que la alta dirección delega la responsabilidad en otros funcionarios, esperando estar informado sobre su desempeño(ACIS 2016).

- **Gráfica 13. Conciencia de la dirección**

Fuente: ACIS – Revista “Sistemas, Fraude Informático”

En la gráfica 13, se muestra las variaciones que se ha obtenido en el año 2016 con relación al año 2015. En donde se identifica que la alta dirección está en el camino de entender la gestión de la seguridad de la información como un mecanismo que busca proteger la organización. No es un concepto consensuado entre el 100% de los directivos en las organizaciones, algunos los siguen viendo como una herramienta más de la áreas de tecnologías y no como un mecanismo de tipo estratégico en la organización(ACIS 2016).

- **Conclusiones de la encuesta**

La gestión relacionada con la ciberseguridad y entornos ciberseguros, se entienden como los más complejos de proteger debido auge y proliferación de los ciberdelincuentes, así como el aumento de herramienta de ataque, en los para el

2016 se destaca el Ransomware como un desafío por su volatilidad, incierto y ambiguo; lo cual exige observarlo con especial cuidado y detenimiento para asegurar el adecuado tratamiento(ACIS 2016).

Se observa la imperiosa necesidad que las organizaciones se apoyen en la regulación nacional e internacional con relación a la seguridad de la información para lograr su fortalecimiento y una adecuada gestión que responda a las necesidades de prevención en las organizaciones y su entorno. Se ratifica que en Colombia cree la tendencia a implementar marcos de referencia y estándares de buenas prácticas en seguridad de la información, destacándose la utilización de ISO 27000 y toda su familia, ITIL, COBIT que se consolidad como mecanismos adecuados en la implementación y control de arquitecturas de seguridad de la información; siendo preocupación de los participantes de la encuesta la utilización de un marco de referencia en las organizaciones(ACIS 2016).

3.2.13 Política nacional de seguridad digital[6]

Esta política rige en la República de Colombia, para su elaboración se ha involucrado los Ministerios de Tecnologías de la Información y las Comunicaciones, la Dirección Nacional de Defensa y el Departamento Nacional de Planeación. Colombia, a través de su estructura gubernamental, es consiente del crecimiento y auge que ha tenido el entorno digital en el desarrollo de las actividades sociales y económicas que componen el país. A su vez reconoce que este entorno trae consigo riesgos e incertidumbres inherentes de seguridad digital, los cuales deben ser gestionados y monitoreados permanentemente para mitigar la exposición a amenazas y vulnerabilidades de seguridad, que pueden afectar las actividades socioeconómicas e integridad de los ciudadanos en el país y sus entornos de desempeño. Para la elaboración y aprobación, el gobierno definió los enfoques “Defensa del país” y “Lucha contra el cibercrimen”, considerados de prioridad para contrarrestar las amenazas, vulnerabilidad, riesgos y anomalías que representan afectación para el país y sus sectores productivos (Glen 2016).

Esta política le ha brindado la oportunidad a Colombia que sea reconocida y posicionada en la región como un país que se preocupa y enfrenta los riesgos de seguridad digital; teniendo entre sus principales pilares la gestión del riesgo, que lo ha considerado un aspecto fundamental para minimizar la afectación que puede causar la ciberdelincuencia en el desempeño del estado y sus diversos sectores socioeconómicos. La gestión del riesgo digital requiere de mayores esfuerzos en planeación, prevención y atención (Glen 2016).

Para la puesta en marcha de la actual política, el gobierno ha diseñado un plan de acción para ser ejecutado del año 2016 al 2019 y ha dispuesto una inversión total

[6] *Aprobada por el **CONPES**: Consejo nacional de política económica y social República de Colombia – Departamento Nacional de Planeación*

de 85.070 millones de pesos; delegando la responsabilidad de su ejecución en el MINTIC[7], Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación(Glen 2016). Se espera que con su implementación en el 2020 impacte positivamente la económica de Colombia, que haya generado 307.000 empleo y aportado al crecimiento del PIB[8] en un 0,1% según su variación promedio anual (Glen 2016).

Para el cumplimiento de la política se ha considerado que es de carácter prioritario gestionar el entorno digital, la infraestructura critica de ciberseguridad, componentes de gobernanza, la educación, la regulación, la cooperación nacional e internacional, la investigación, el desarrollo y la innovación. También se ha reconocido como importante que la seguridad digital sea gestionada desde un nivel estratégico combinado con un adecuado desempeño técnico (Glen 2016).

3.2.13.1 Antecedentes de la política

En todos los sectores del país, se ha hecho notoria la importancia de la incorporación en los procesos y actividades digitales, este es un aspecto positivo para la alienación, el desarrollo económico y la integración de Colombia con el mundo socioeconómico global. No obstantes estos aspectos positivos, insertan en el país la necesidad de gestionar las anomalías de seguridad digital, que crecen de acuerdo al uso de las TIC y los entornos digitales. En las gráficas que se muestran a continuación se representa la proyección de crecimiento de la TIC entre el 2015 y 2020 en un entorno global y los grandes casos de ataque cibernéticos en el mundo al 2014 (Glen 2016).

- **Ilustración 5. Proyecciones de indicadores de uso de las tic en el contexto global**

Tabla 1. Proyecciones de algunos indicadores de uso de las TIC a nivel global

Proyecciones	2015	2020	Incremento porcentual
Más usuarios de banda ancha móvil	3 mil millones	4 mil millones	33%
Más terminales conectados	16,3 mil millones	24,4 mil millones	49%
Más datos generados	8,8 zettabytes	44 zettabytes	400%
Más tráfico IP de red (mensual)	72,4 exabytes	168 exabytes	132%
Dispositivos (Internet de las cosas)	15 mil millones	200 mil millones[(a)]	1200%
Tamaño del mercado de la nube pública global	USD 97 mil millones	USD 159 mil millones	63%

Fuente: Adaptado de INTEL SECURITY (2015a).
Nota: [(a)] Proyección a 2018.

Fuente: Política nacional de ciberseguriad digital de Colombia – CONPES 2016

[7] ***MINTIC**: Ministerio de Tecnologías de la Información y la Comunicaciones.*
[8] *PIB: Producto Interno Bruto.*

- **Ilustración 6. Granes casos de ataques cibernéticos en el mundo en el 2014**

Tabla 2. Grandes casos de ataque cibernéticos en el mundo en el 2014

Organización afectada	Sector	Impacto
Snapchat	Red social	4,5 millones de nombres y números móviles comprometidos
Kickstarter	*Crowd funding*	5,6 millones de víctimas
Korean Telecom	Telecomunicaciones	12 millones de suscriptores comprometidos
Heartbleed	*Software*	Primera de tres vulnerabilidades de fuente abierta
Ebay	Compras	Base de datos de 145 millones de compradores comprometida
PF chang´s	Comidas	Más alta violación de información de alto nivel del mes
Energetic bear	Energía	Operación de ciberespionaje a la industria de energía
Cybervor	Tecnología	1,2 billones de credenciales comprometidas
iCloud	Entretenimiento	Cuentas de celebridades comprometidas
Sandworm	Tecnología	Ataque cibernético a la vulnerabilidad de Windows
Sony Pictures	Entretenimiento	Más alta violación de alto nivel del año
Inception Framework	Sector público	Operación de ciberespionaje a sector público

Fuente: Adaptado de Verizon (2015).

Fuente: Política nacional de ciberseguriad digital de Colombia – CONPES 2016

Con base en las proyecciones de crecimiento del uso de las TIC y los antecedentes de ataques tanto nacionales como mundiales, Colombia se ha preocupado por definir sus lineamientos de ciberseguridad y ciberdefensa por lo que ha definido los objetivos sobre los que basará el documento CONPES 3701 que contiene y rige la política nacional de seguridad digital para fortalecer las capacidades del Estado para enfrentar las amenazas que pudieran vulnerar la seguridad nacional (Glen 2016).
Las entidades de gobiernos responsables de elaborar la Política Nacional de Seguridad Nacional, se trazaron los siguientes objetivos estratégicos:

- “Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional”.
- “Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad”.
- “Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática”.

3.2.13.2 Institucionalidad

Con el documento CONPES 3701, se crearon e institucionalizaron los siguientes grupos de respuesta inmediata a temas relacionados con la seguridad digital [6].

- Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia.
- El Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia.
- El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL).
- La Delegatura de protección de datos en la Superintendencia de Industria y Comercio.
- La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones.
- El Comité de ciberdefensa de las Fuerzas Militares.
- Las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.
- COMISIÓN Nacional Digital y de Información Estatal.

3.2.13.3 Capacitación

El enfoque está marcado por la educación, sensibilidad y concientización de los entes de gobiernos y la ciudadanía en general; sobre el uso responsable de los recursos de internet y el contacto digital con otros entornos a nivel de empresa y sociedad. A través del equipo colCERT, se han diseñado campañas de sensibilización y entrenamiento en los principales frentes identificados para contrarrestar la ciberdelincuencia; principalmente enfocado a programas de prevención de jóvenes y niños. El equipo de CCOC, se ha enfocado en el fortalecimiento de las competencias de los equipos dedicados a vigilar y controlar la ciberdefensa y sus unidades estratégicas y de operación; también a establecer los lineamientos necesarios para gestionar la seguridad digital. El equipo CCP, se ha enfocado a las campañas para la ciudadanía en general. Un aspecto a resaltar es el aumento de programas académicos especializados en materia de seguridad de la información. En el 2011 Colombia contaba con 12 programas en todo el país, a la fecha cuenta con más de 50, contemplando desde el nivel técnico hasta estudios en maestría (Glen 2016).

3.2.13.4 Legislación

La Política Nacional de Seguridad Digital, se diseñó para legislar sobre la protección de datos personales. Su fin es tener herramientas jurídicas para atender temas sensibles cómo la explotación, pornografía y turismo sexual. A través de su implementación se crearon medidas especiales con enfoque específico, para proteger los menores de edad. Se destaca la ley 1581 de 2012, que tiene por objeto constitucional defender el derecho que de todas las personas a conocer, actualizar y ratificar la información que se haya recopilado y almacenado en bases de datos públicas y privadas sobre los datos que lo identifican como parte de una sociedad. De igual forma se reconoce el derecho a ser eliminados de las bases de datos en

las que no se desee participar, siempre y cuando estas no interfieran con el reconocimiento como miembro activo dentro del estado y/o grupos de pertenencia específicos (Glen 2016).

3.2.13.5 Cooperación y posicionamiento internacional

En el año 2013, Colombia solicitó de forma oficial a la Unión Europea pertenecer a la Convención Europea sobre Cibercriminalidad[9]. Durante el mismo año también se celebró convenio con Foro Mundial Económico, con el propósito de identificar y abordar los riesgos sistemáticos globales derivados de la conectividad. Se ha fortalecido el trabajo en seguridad digital a través del desarrollo de trabajos de cooperación con organismos como CICTE[10], también se ha logrado establecer proyectos con équidos de incidentes de seguridad de la región. También se han suscrito acuerdos con organizaciones internacionales, una de ella con Antiphishing Working Group para tener la oportunidad de acceder a recursos y programas especializados en ciberseguridad y ciberdefensa y pertenecer a las coaliciones de empresas industriales, autoridades legales y de gobierno que colaboran con los diversos grupos para mejorar la respuesta y los mecanismos de acción frente a la seguridad digital (Glen 2016).

[9] *"**Convenio de Budapest:** Establece los principios de un acuerdo internacional sobre seguridad cibernética y la sanción de delitos cibernéticos".*

[10] **"*Convenio de Budapest:** Comité Interamericano Contra el Terrorismo de la Organización de Estados Americanos (OEA)",*

4. DISEÑO METODOLÓGICO

4.1 Descripción

El diseño de la metodología se basará en establecer un conjunto de parámetros guiados por el cómo se debe auditar la seguridad en los sistemas de información; a partir de las buenas prácticas que propone diversos autores, instituciones y entidades de contexto internacional y del gobierno colombiano; todas reconocidas por tener autoridad, prestigio y responsabilidad para emitir estándares, normas y leyes alusivas a la gestión de la seguridad de la información y prevención del riesgo informático.

La estructura consta de la evaluación de tres dimensiones, a través de tres criterios que permitirán verificar la inclusión y calidad de los criterios de seguridad en los sistemas de información. Cada criterio está compuesto por una lista de controles, que representan las prácticas que propone la norma ISO – 27000 y su familia, ISACA en su marco de referencia COBIT 5, el National Institute of Standards and Technology (NIST), también la comunidad libre y abierta sobre seguridad de la información en aplicaciones: Open Web Application Security Project (OWASP); como guía en la gestión de la información a través de sistemas computarizados.

4.2 Definición de las dimensiones a evaluar

Para el diseño de la auditoria se han determinado tres dimensiones base, que corresponden a los escenarios que se consideran deben ser contemplados durante el programa de auditoria a diseñar, por la incidencia que tiene la seguridad de la información en ellos. A continuación, se describe cada dimensión.

4.2.1 Gobierno universitario

La evaluación de esta dimensión se define a partir de la iteración e incidencia que tiene la información en el ejercicio ejecutivo y en la toma de decisiones de los órganos directivos. El gobierno universitario tiene bajo su responsabilidad velar porque se cumplan las leyes, se generen y apliquen las políticas, los procesos, las estructuras organizacionales y demás requerimientos para administrar, controlar y mitigar los riesgos asociados a la gestión de la información. En la evaluación de la inclusión y calidad de los criterios de seguridad, el gobierno se constituye en un elemento clave al ser quien integra e institucionaliza las buenas prácticas para garantizar el cumplimiento de los objetivos de valor, prever y disponer de recursos suficientes, adecuados y acordes al tamaño y desempeño de la institución. También tiene el compromiso de generar una cultura que concientice y fomente entre la comunidad la adopción y aplicación de prácticas adecuadas en la gestión y protección de la información. Como retribución a la gestión del gobierno universitario, se debe reflejar el máximo aprovechamiento de beneficios,

capitalización de oportunidades y la generación de ventajas competitivas desde la certeza que los activos de información son confiables, confidenciales, auténticos y que están a disposición de los interesados.

4.2.2 Sistemas de Información

La evaluación de las plataformas tecnológicas que soportan la operacionalización de los procesos organizacionales, es una necesidad para medir la calidad técnica y funcional de una entidad en la gestión de su información. La evaluación resulta útil en la medida que los fallos sean detectados y corregidos. Los sistemas de información son elementos claves para determinar la inclusión y calidad de los criterios de seguridad en el tratamiento de los activos de información; a partir de determinar el nivel de confidencialidad, disponibilidad, autenticidad y confiabilidad de los datos que se gestionan. Para aplicar la evaluación se parte de la base que, durante el ciclo de desarrollo del producto, se diseñaron e implementaron controles asociados al manejo de errores, a técnicas de autenticación, implementación de bitácoras (log) que registran las actividades realizadas por los usuarios, técnicas de encriptación, transporte de datos, tratamiento de usuarios y contraseñas. Adicional se parte de la base que para la administración se tiene implementado y documentado los procedimientos necesarios para el manejo de sesiones de trabajo, la gestión de cambios, la actualización de versiones y se dispone de herramientas de protección contra código malicioso.

4.2.3 Mantenimiento y soporte

Evaluar la calidad del mantenimiento y soporte asociado a los sistemas de información, se hace necesario para verificar la existencia de políticas, procedimientos, buenas prácticas y controles para ser aplicados en la gestión de activos, la clasificación de la información, el control operacional, la gestión de copias de respaldo, la intervención de proveedores, la administración y el monitoreo de las actividades relacionadas con la infraestructura de comunicaciones. Es importante que se evalúe la efectividad que cumplen cada uno de los componentes descritos en la gestión de la seguridad de la información y en la prevención del riesgo informático; para determinar la eficiencia, eficacia y coherencia de los lineamientos establecidos y de los recursos asignados para prevenir y mitigar el riesgo tecnológico ante amenazas y/o vulnerabilidades que tengan incidencia en la adecuada operación de los sistemas de información e impacto en la organización.

4.3 Criterios de seguridad para evaluar las dimensiones establecidas

Se definieran tres criterios, para ser la guía de la evaluación que se realizará a las dimensiones establecidas como escenarios de evaluación. El objetivo es tener tres criterios generales, para los que se emitirá un concepto técnico de la situación de seguridad de la información que se hallará durante el programa de auditoria.

4.3.1 Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión universitaria

Para definir la lista de controles, se tomó como referencia la propuesta que hace la Norma Técnica Colombiana ISO 27000 y el marco de referencia COBIT 5 de ISACA, entidades que determinan que, para auditar la apropiación del gobierno corporativo con respecto a la inclusión y calidad de los criterios de seguridad, se debe tener en cuenta los siguientes controles.

- Legislación, principios, políticas y marcos de referencia
- Estructura organizacional
- Disponibilidad de recursos
- Procesos
- Cultura, ética y comportamiento
- Personas, habilidades y competencias
- Perfil de aceptación del riesgo
- Arquitectura de seguridad de la información

4.3.2 Calidad de los criterios de seguridad de la información en ambientes en producción

La lista de controles que se propone a continuación, hace referencia a las buenas prácticas que propone las entidades: ISO, ISACA, NIST y OWASP para la gestión y evaluación de los criterios de seguridad en sistema de información.

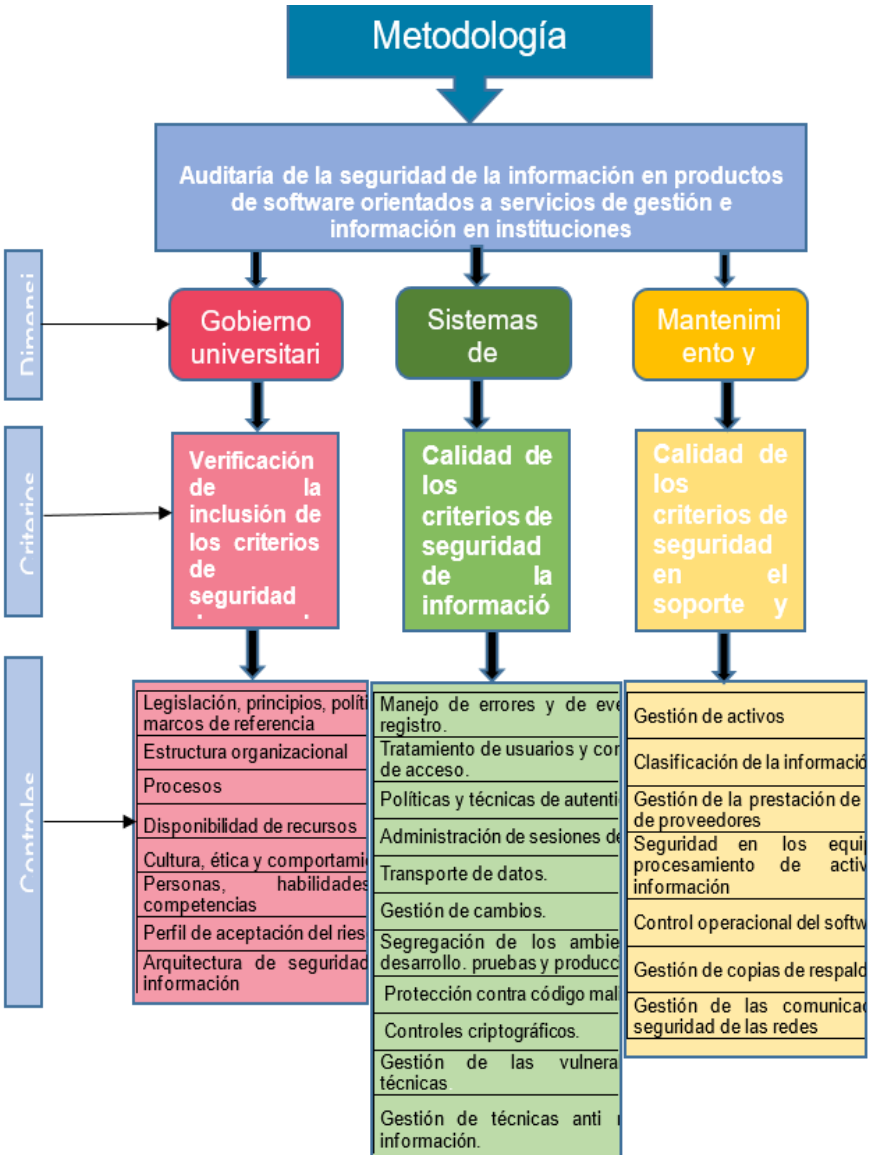
- Manejo de errores y de eventos de registro
- Tratamiento de usuarios y contraseñas de acceso
- Políticas y técnicas de autenticación
- Administración de sesiones de trabajo
- Transporte de datos
- Gestión de cambios
- Gestión de la capacidad
- Segregación de los ambientes de desarrollo. pruebas y producción
- Protección contra código malicioso
- Controles criptográficos
- Gestión de las vulnerabilidades técnicas
- Gestión de técnicas anti robo de información

4.3.3 Calidad de los criterios de seguridad en el soporte y mantenimiento

Los controles descritos a continuación, han sido seleccionados de la norma ISO 27002, cuyo propósito es determinar la inclusión y calidad de los criterios de seguridad en el soporte y mantenimiento de los sistemas de información.

- Gestión de Activos
- Clasificación de la información
- Gestión de la prestación de servicios de proveedores
- Seguridad en los equipos de procesamiento de activos de información
- Control operacional del software
- Gestión de copias de respaldo
- Gestión de las comunicaciones y seguridad de las redes

Ilustración 7. Estructura



Fuente: Elaboración propia

5. DISEÑO DE LOS INSTRUMENTOS

Los instrumentos, estarán conformados por dos elementos (cuestionario y matriz para el análisis de riesgo), con su aplicación se busca obtener un diagnóstico de los criterios de seguridad definidos; para medir la apropiación del gobierno universitario, el desempeño de los sistemas de información, el mantenimiento y soporte.

5.1 Cuestionario

Compuesto por ocho controles que medirán la apropiación del gobierno universitario en la adopción y aplicación de prácticas adecuadas en la gestión de la seguridad de la información. Para cada control se diseñará un listado de preguntas (Anexo A. Instrumento I); todas dirigidas a diagnosticar el grado de conocimiento e involucramiento.

5.1.2 Escala de Evaluación

En la tabla 4, se describe los criterios de escala, valoración e intervalos de porcentaje. Los resultados se obtendrán a través de respuestas emitidas por el entrevistado; las cuales se establecerán en una escala de Liker[11], las opciones se cuantificarán del 1 al 4, según la valoración definida. Al terminar la aplicación del instrumento, se hallarán los resultados por procedimiento aritmético y serán traducidos a intervalos de porcentaje que mostraran el grado de cumplimiento del criterio evaluado.

Tabla 3. Criterios para evaluación del cuestionario

Escala Likert	Nivel de calificación	Descripción	Rango de ubicación según el nivel de calificación alcanzado
1	No alcanzado	No está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro.	0% a 25%
2	Parcialmente Alcanzado	Alcanza su propósito. Está implementado.	> 25% a 50%
3	Ampliamente Alcanzado	Implementado de forma gestionada (planificado, supervisado y ajustado). Los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.	> 50% a 75%
4	Completamente Alcanzado	Implementado usando un proceso definido, que es capaz de alcanzar sus resultados de proceso.	> 75% a 100%

Fuente: Elaboración propia, a partir de COBIT 5

[11] E**scala de *Likert*:** (también denominada método de evaluaciones sumarias), se considera la más utilizada para la aplicación de encuestas. Se denomina así por Rensis Likert.

5.1.3 Determinación de la muestra

Se hará uso de un método no probabilístico, debido a que interesa medir población que esté estrechamente relacionada con la gestión de la seguridad de la información, bien sea como integrante de los órganos directivos, administrador de las plataformas tecnológicas, gestor de la seguridad en recursos informáticos o generador y consumidor de activos de información; con el propósito de obtener información específica, para el análisis estadístico e informe de auditoría.

5.1.4 Determinación de la población objeto de medición

Se limitó a las categorías: Directivo, Director / Jefe y Profesional. Para el análisis se tomará el resultado obtenido del procedimiento aritmético una vez aplicado el cuestionario a dos entrevistados por categoría.

5.1.5 Resultado esperado

Hallar evidencia para una evaluación confiable, coherente y repetible para la verificación de la inclusión de los criterios de seguridad de la información en el ámbito de gobierno y gestión universitaria para garantizar la seguridad de la información.

5.2 Matriz para el análisis de riesgos

El propósito es mostrar las vulnerabilidades y amenazas y su probabilidad de ocurrencia e impacto sobre los procesos de valor. Para la medición se tendrán evaluaran siete sistemas de información, que están clasificados según la criticidad del servicio que prestan. Se evaluará la magnitud del daño, llegado el caso que una probabilidad se convierta en ocurrencia.

5.2.1 Estructura

La matriz estará compuesta por 19 controles que medirán la calidad e inclusión de los criterios de seguridad en ambientes en producción, el soporte y mantenimiento de sistemas de información. Para evaluar cada criterio, se diseñará un elemento de medición (Anexos C y D: instrumento II e Instrumento III).

5.2.2 Escala de valoración

Estará conformada por una matriz de 4 x 4, con una posibilidad máxima de un valor de 16, que representa el mayor nivel de riesgo posible. A medida que

disminuye el número, representa un nivel de riesgo menor, hasta llegar a un valor óptimo de 1. Dependiendo de los valores de la probabilidad de amenaza y la magnitud de daño, la matriz calcula por procedimiento aritmético el producto de dos variables y visualiza el grado de riesgo. Para el método de análisis de riesgo se utilizará la fórmula: Riesgo = (probabilidad de amenaza x magnitud de daño). La probabilidad de amenaza estará representada por la escala:

1= Insignificante
2= Baja
3= Media
4= Alta

La magnitud de daño estará representada por la escala:

1= Bajo
2= Medio
3= Alto
4= Crítico

Tabla 4. Matriz de análisis de riesgo

Instrumento criterio 2 y 3				
Riesgo	**Probabilidad de amenaza**			
Magnitud del daño	**1**	**2**	**3**	**4**
	1	2	3	4
	2	4	6	8
	3	6	9	12
	4	8	12	16

Fuente: Elaboración propia a partir del estándar de matriz de riesgo

Tabla 5. Umbral de riesgo

Umbral del riesgo		
Categoría	**Mínimo**	**Máximo**
Bajo	1	2
Medio	3	6
Alto	8	16

Fuente: Elaboración propia a partir del estándar de matriz de riesgo

El riesgo es el producto de la multiplicación: probabilidad de amenaza por magnitud de daño. Se agrupará por tres rangos, cuya clasificación estará representada por los colores: verde (riesgo bajo), amarillo (riesgo medio) y rojo (riesgo alto). La clasificación será el resultado del mayor de valores en la matriz que se ubiquen dentro de uno de los rangos establecidos.

5.2.3 Selección de la muestra

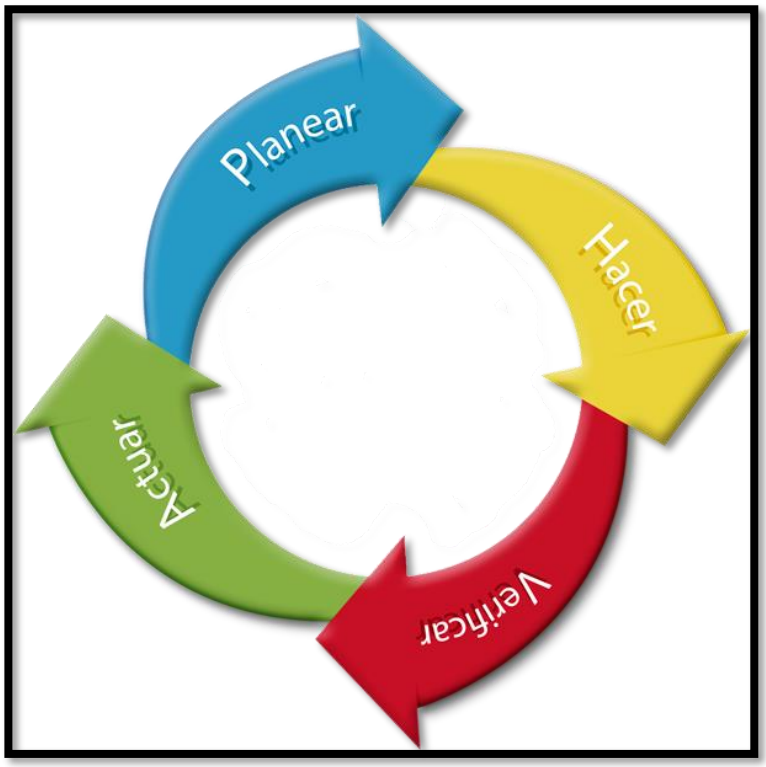
Se hará uso de un método no probabilístico. La matriz está diseñada para que ser aplicada por un experto técnico en seguridad de la información. Los valores de probabilidad de amenaza y magnitud del daño deben ser asignados después de observar el contesto a auditar y la verificación de evidencias.

5.2.4 Resultado esperado

Corresponderá a los datos generados, para emitir concepto sobre el nivel de riesgo al que está expuesto los activos de información, ante la posibilidad de sufrir un daño significativo, causado por una amenaza o vulnerabilidad. También trasmitir recomendaciones, como aporte a la toma de medidas de protección a que haya lugar.

6. ESTRUCTURA CICLO DE VIDA PROGRAMA DE AUDITORÍA

Ilustración 8. Ciclo de vida PHVA



Fuente: Elaboración propia, a partir de la Norma ISO 19011

Para estructurar el ciclo de vida, se tomará como referencia general la Norma Internacional ISO 19011, sobre las directrices para la auditoría de sistemas de gestión, segunda edición 2011 – 11 – 15. Esta norma no establece requisitos, es una guía práctica del cómo realizar un programa de auditoría, siguiendo el ciclo PHVA, planear, hacer, verificar y actuar.

Objetivo: Verificar la inclusión y calidad de los criterios de seguridad de la información en la gestión de los activos de información en instituciones de educación superior.

Propósito: Detectar el estado actual en la gestión de la seguridad y prevención de riesgos informáticos, con relación a los principios (confidencialidad, autenticidad, fiabilidad y disponibilidad) que determinan la calidad y seguridad en el tratamiento de la información, que se genera en instituciones de educación superior.

Alcance: Aplicar los instrumentos de medición diseñados para determinar el nivel de madurez de la organización en la inclusión y calidad de los criterios de seguridad de la información, para obtener un resultado sujeto a análisis y preparar informe de auditoría. El diseño de la metodología propuesta, está contemplado para realizar

un programa de auditoria interna. Es decir, libre de cumplir con responsabilidades para procesos de certificación, resolver conflictos de interés o dar cumplimiento a solicitudes legales.

6.1 Principios y generalidades

La auditoría se caracteriza por depender de varios principios, que deben hacer de ella, una herramienta fiable y eficaz para apoyar las políticas y controles de gestión. Su principio rector, siempre será emitir información veraz, para apoyar la toma de decisiones, con el propósito de mejorar el desempeño. Los principios se convierten en los elementos por los cuales se proporciona conclusiones suficientes y pertinentes sobre el programa de auditoria realizado, de forma objetiva e imparcial.

Evidencia: Información pertinente y verificable que soporta la calificación asignada durante la evaluación. Se basa en la información disponible, que se denomina muestra; generalmente se solicita al evaluado de forma aleatoria, según corresponda al objetivo de la auditoria. Al momento de hacer la evaluación y emitir las conclusiones, el auditor debe apoyarse en las evidencias que captó y verificó durante el desarrollo de la auditoria.

Hallazgos: Son los resultados que indican conformidad o no conformidad según la información detectada durante el programa de auditoria. El auditor está en la obligación de reportar información veraz y exacta, según lo refleje el programa de auditoria desarrollado. Los hallazgos, generalmente conllevan a la identificación de oportunidades de mejorar e implementación de mejores prácticas.

Informe: documento con contexto analítico que expone los hallazgos en forma cuantitativa y cualitativa conforme a los resultados obtenidos. Incluye el concepto del responsable del programa de auditoría, la conclusiones y recomendaciones que estima conveniente.

Grupos de interés: Son todas organizaciones, personas, cargos y recursos a los que se les aplica el programa que se verán afectados directa o indirectamente por el desarrollo de la auditoria. Lo grupos que hacen parte de la auditoria tienen la capacidad de afectar positiva o negativamente los resultados esperados.

Experto técnico: Profesional con experticia, experiencia y amplio conocimiento del tema que origina la auditoría. El programa de auditoria debe asegurar que la persona que desempeñará la responsabilidad está adecuadamente formada para actuar como auditor y que en los resultados se verá reflejado su conocimiento, profesionalismo y ética.

Integridad: Profesionalismo con el que se planea y ejecuta el programa de auditoria. Es un deber del equipo auditor, ejecutar las actividades con responsabilidad, honestidad y diligencia. Un auditor debe mantener un límite de involucramiento y relaciones interpersonales con el grupo auditado y la empresa a auditar; para evitar caer en juicio parciales que no reflejen la realizada de la evaluación realizada.

Confidencialidad: Discreción en el uso y protección de la información a la que se tiene acceso durante el programa de auditoria y después de finalizado el proceso. Bajo ninguna circunstancia se podrá hacer uso de los activos de información de una empresa, para obtener ganancia o beneficios personales ni para el auditado ni para el auditor.

Independencia: El equipo auditor, deberá estar libre de todo sesgo y conflicto de intereses. Los conceptos emitidos deberán ser independiente e imparciales; siempre con actitud objetiva, asegurando que los hallazgos y conclusiones estarán basados solo en las evidencias.

Enfoque basado en la evidencia: El método racional para alcanzar conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático. La evidencia de la auditoria, debe ser sujeta a verificación, en momento que se considere necesario, brindando confianza en el concepto y conclusiones emitidas.

5.1.2 Planeación del programa de auditoria

- Responsabilidades que se asumirán.
- Roles de las personas que participaran.
- Procedimientos a aplicar desde la apertura del programa hasta el cierre.
- Protocolo de las actividades secuenciales a realizar durante la ejecución del programa.
- Recursos asignados para cumplir el programa.
- Riesgos a los que se enfrenta el equipo durante la ejecución del programa.

5.1.3 Implementación del programa

- Reunión de apertura, todos los implicados en el programa.
- Presentación del equipo evaluador.
- Presentación del equipo evaluado.
- Registro de los asistentes.
- Informar los objetivos, el alcance, los procedimientos y actividades a realizar durante todo el programa.
- Informar la metodología del programa de auditoria.

- Informar el cronograma aprobado.
- Informar la norma, los procesos y recursos a auditar.
- Informar la forma como se solicitará y auditará la parte documental, los recursos, las entrevistas y verificaciones a realizar. El equipo auditor no podrá retirar ningún documento proporcionado durante la auditoria, solo tomar evidencias.
- Elaboración de informe.
- Reunión para presentación resultados e informe
- Cierre del programa de auditoria.

5.1.4 Verificar

Después de finalizado el programa de auditoria, se deberá realizar un monitoreo a todas las actividades desarrolladas para detectar acciones de mejora al programa, implementar nuevas funcionalidades o sencillamente concluir que está siendo bien llevado. El monitorio debe ser constante para introducir los cambios que se consideren necesarios de forma oportuna.

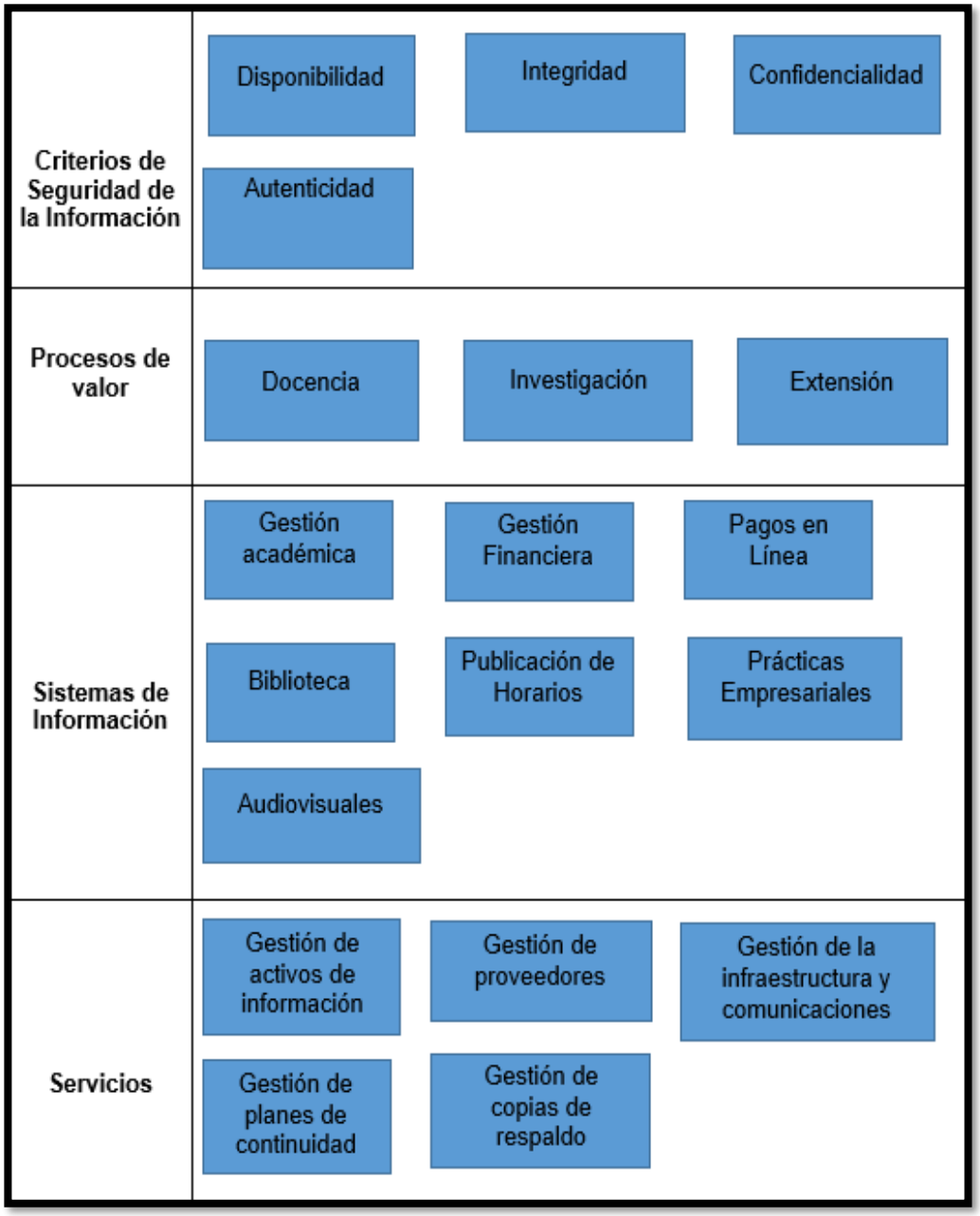
5.1.5 Actuar

El programa de auditoría, en sí mismo debe ser mejorado constantemente para que sea efectivo y no entre en estados de obsolescencia en los procesos y las regulaciones que lo presiden. En cada plan de mejora se deben considerar los recursos necesarios con base en los cambios y/o actualizaciones a realizar.

7. RESULTADOS DE LA APLICACIÓN DE LOS INSTRUMENTOS

A continuación, se describirá los componentes que hicieron parte de la evaluación durante la aplicación de los instrumentos. Cada componente aportó, para determinar la inclusión de los criterios a través de la evaluación de los controles identificados como necesarios en la gestión de seguridad de la información.

Ilustración 9. Componentes del programa de auditoria



Fuente: Elaboración propia

7.1 Instrumento 1 (cuestionario)

El propósito, es recopilar información para evaluar la apropiación del gobierno universitario en la adopción y aplicación de prácticas adecuadas. Su estructura consta de ocho controles, para medir los aspectos relevantes de la gestión del gobierno universitario con respecto a seguridad de la seguridad. El entrevistado, tendrá la opción de seleccionar una respuesta de la escala de Licket: 1= no alcanzado, 2= parcialmente alcanzado, 3= ampliamente alcanzado, 4= completamente alcanzado; según su criterio frente a la pregunta realizada.

- **Tabla 6. Ficha Técnica**

Contiene el resumen de la información requerida para la aplicación del instrumento, con base en la estructura del diseño (ver diseño completo en el anexo 2).

Dimensión	Gobierno Universitario
Criterio	Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión corporativa.
Controles	Estructura organizacional
	Legislación, principios, políticas y marcos de referencia
	Disponibilidad de recursos
	Procesos
	Cultura, ética y comportamiento
	Personas, habilidades y competencias
	Perfil de aceptación del riesgo
	Arquitectura de seguridad de la información
Método de recolección de datos	Cuestionario
Método de aplicación	Entrevista personal y aplicación de cuestionario en línea
Método para selección de la muestra	No probabilístico
Muestra	Funcionarios altamente involucrados en la gestión de los sistemas de información
Población objeto de medición (categorías)	Director / Jefe
	Profesional
	Oficial de seguridad de la información
	Director
	Ingeniero de soporte técnico Sistemas de Información
	Líder Funcional – ERP Institucional
Herramienta para aplicación:	Google docs
Link de acceso al cuestionario	https://docs.google.com/forms/d/1hCv8NqqHvGnwgi3YGSzB-d9Orv6yQgLYFKgFCZLKb5U/
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

Fuente: Elaboración propia

7.1.1 Variables de medición

Las variables se han determinado para que el instrumento se aplique a la población objeto. Los resultados serán sometidos a análisis estadístico cuantitativo y cualitativo en coherencia con los datos obtenidos en la matriz respuestas por escala Likert, que se podrá observar en el análisis descriptivo de cada variable.

Tabla 7. Componentes de medición

Variables	**Control**							
	1	2	3	4	5	6	7	8
Elementos	9	8	3	4	5	4	8	7
Escala Likert	1 al 4							

Fuente: Elaboración propia

Compuesto por los ocho controles de seguridad que se definieron para evaluar la inclusión de los criterios de seguridad de la información en el gobierno universitario. Cada control tiene asociada una lista de preguntas relacionadas con la gestión que se espera, debería ejercer por el gobierno universitario como aporte al adecuado tratamiento de los activos de información. La escala de Likert, está regida por una calificación, que se deberá interpretar de la siguiente forma: 1) no alcanzado, 2) Parcialmente alcanzado, 3) Ampliamente alcanzado), 4) completamente alcanzado; como se especifica en el diseño.

7.1.2 Caracterización de resultados

A continuación, se presentará la medición obtenida después de aplicar el instrumento denominado cuestionario, con el propósito de analizar resultados obtenidos por control. Los criterios de interpretación serán los establecidos en la tabla 4. (criterios de evaluación), que dieron origen la escala de Likert. (Anexo B. Cuestionario Aplicado).

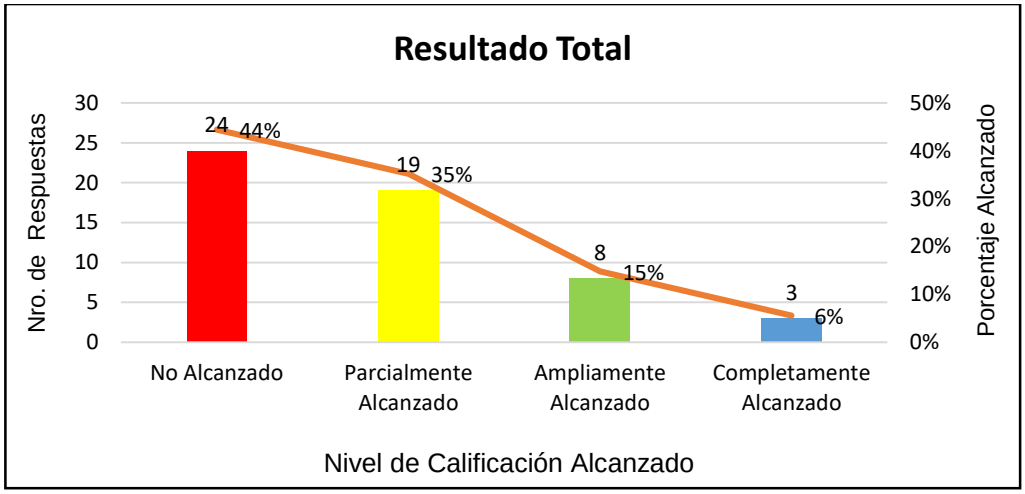
7.1.3 Análisis e interpretación de la información obtenida con el cuestionario

Los siguientes son los resultados del cuestionario (Anexo B) aplicado, según el diseño del instrumento que hace parte del Anexo A. La aplicación se realizó a seis personas de la institución de educación superior, como se había definido en la ficha técnica. Los resultados se mostrarán en gráficas estadísticas, de acuerdo con el resultado aritmético obtenido para cada control. El nivel y rango porcentual de

calificación, se asignará según los criterios definidos para la evaluación del cuestionario (Tabla 3).

7.1.3.1 Control legislación, principios, políticas y marcos de referencia

- **Gráfica 14. Resultado control 1, cuestionario (anexo 2)**



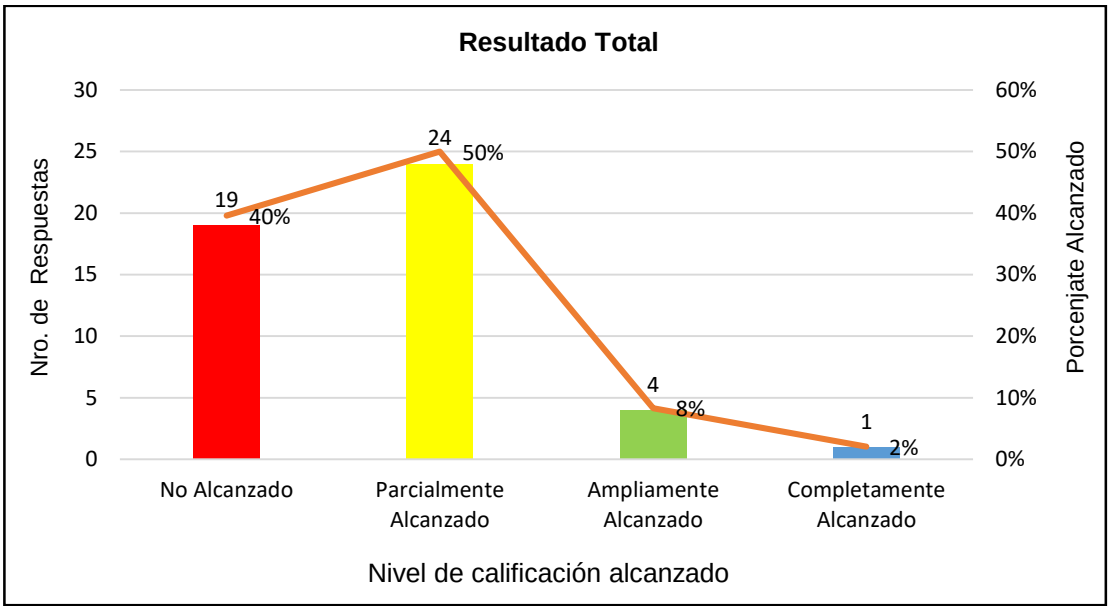
Fuente: Elaboración propia

- **Análisis:** El 44% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 19% qué está implementado y alcanza su propósito. El 8% qué está implementado de forma gestionada (planificado, supervisado y ajustado) y el 6% que está implementado usando un proceso definido, que es capaz de alcanzar sus resultados de proceso.

- **Hallazgo**: Se identifica que no existen políticas de seguridad de la información formales; se tienen documentos que están en proceso de aprobación por parte del gobierno universitario. Existe una política de Ley de Protección de Datos Personales, publicada en el sitio Web Institucional, sin embargo, un porcentaje de los entrevistados desconoce su contenido. Se interpreta que no ha sido divulgado entre la comunidad; situación que motiva a que los procesos de gestión que dan origen a la información, se ejecuten sin su aplicación. Este suceso alarma, al detectar que se podría estar incumpliendo disposiciones de ley en el tratamiento de datos personales. La Política Nacional de Seguridad Digital, aprobada para Colombia en 2016; no es conocida por ningún de los encuestados. Se identifica que se valora la pertinencia de incluir la seguridad de la información como un ítem relevante en la gestión del gobierno universitario y de la institución en general, a pesar de ello no se refleja en el desempeño regular.

7.1.3.2 Control estructura organizacional

- **Gráfica 15. Resultado control 2, cuestionario (anexo 2)**



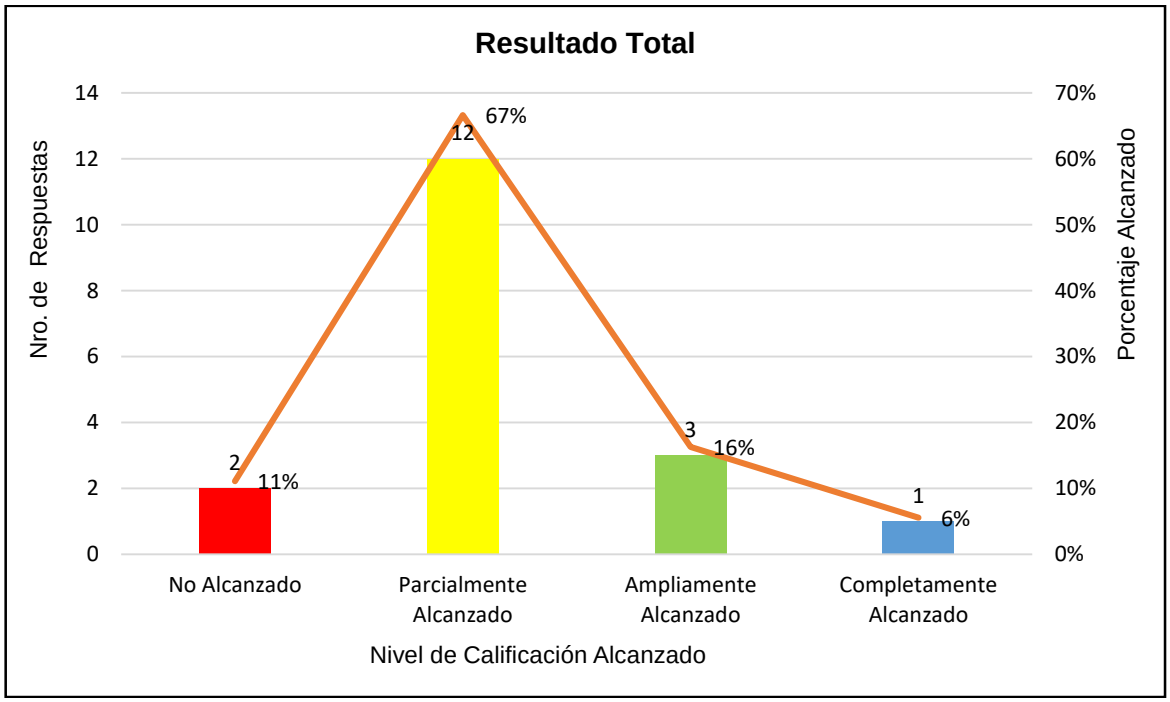
Fuente: Elaboración propia

- **Análisis:** El 40% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia El 50% qué está implementado y alcanza su propósito. El 8% qué está implementado de forma gestionada (planificado, supervisado y ajustado) y el 6% que está implementado usando un proceso definido, que es capaz de alcanzar sus resultados de proceso.

- **Hallazgo:** La población evaluada, reconoce que la información está siendo valorada en un nivel muy bajo, como activos de la institución. Se evidencia actividades para detectar vulnerabilidades de seguridad que no pueden ser considerados procedimientos, debido a la informalidad; también porque no están alineados con los procesos de valor. Se reconoce que la institución ha definido e implementado mecanismos para protección de los activos de información, no obstante, la mayoría carecen de robustez y rigurosidad. Se detecta que no todos los contratos de los empleados que tienen acceso a información relevante están formalizados a través de cláusulas de confidencialidad. No se haya directrices formales para dar acceso a los recursos tecnológicos a proveedores. No se tiene procedimientos para el reporte de incidentes. Los canales para reportar incidentes son la mesa de servicio o el correo institucional. No se identifica un plan de continuidad del negocio.

7.1.3.3 Control disponibilidad de recursos

- **Gráfica 16. Resultado control 3, cuestionario (anexo 2)**



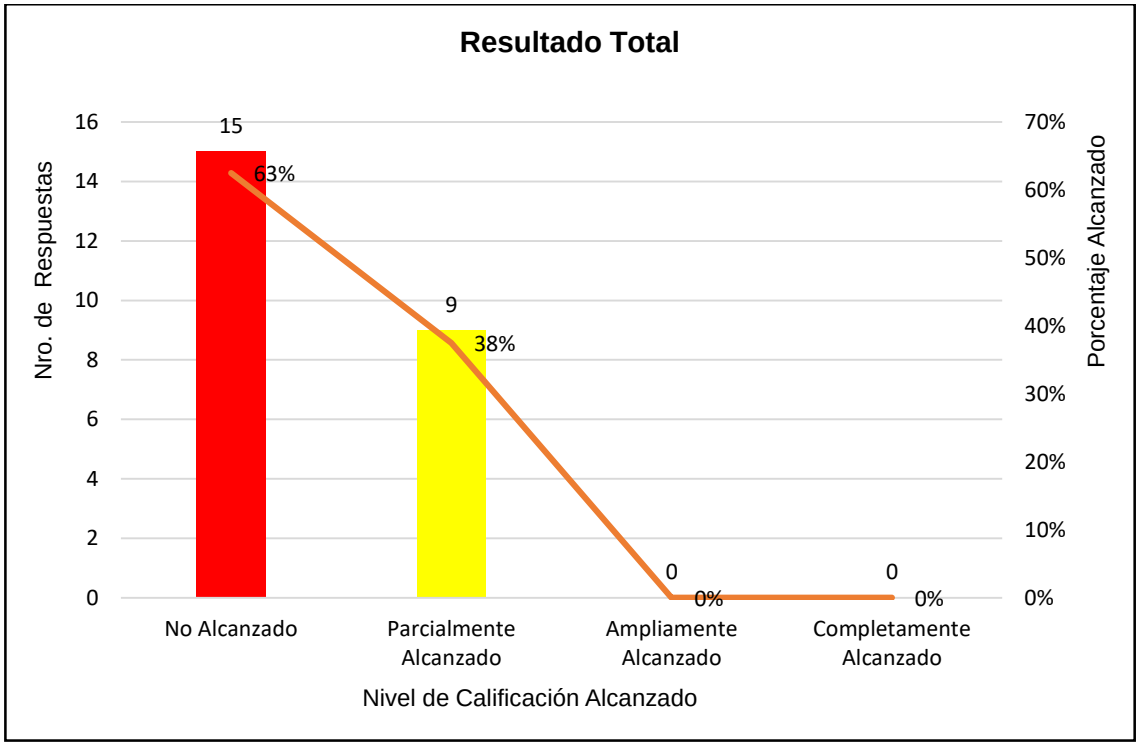
Fuente: Elaboración propia

- **Análisis**: El 11% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 67% qué está implementado y alcanza su propósito. El 16% qué está implementado de forma gestionada (planificado, supervisado y ajustado) y el 6% que está implementado usando un proceso definido, que es capaz de alcanzar sus resultados de proceso.

- **Hallazgos**: La población entrevistada, identifica que la institución destina recursos económicos para la gestión de la seguridad de la información, sin embargo, estos son limitados, se atribuye a que es un área relativamente nueva y dispone de un profesional asignado de tiempo completo. Se evidencia herramientas tecnológicas para la gestión de la información e inventarios de los activos de información. También un lineamiento de renovación de tecnología por obsolescencia, que no incluye los sistemas de información. Se recomienda que la institución asigne mayor talento humano profesional y especializado en gestión de sistemas de información, los empleados que actualmente son responsables de implementar, sostener y mantener los recursos tecnológicos es muy bajo en comparación con el alto grado de tecnológica incorporada a la institución.

7.1.3.4 Control procesos de valor

- **Gráfica 17. Resultado control 4, cuestionario (anexo 2)**



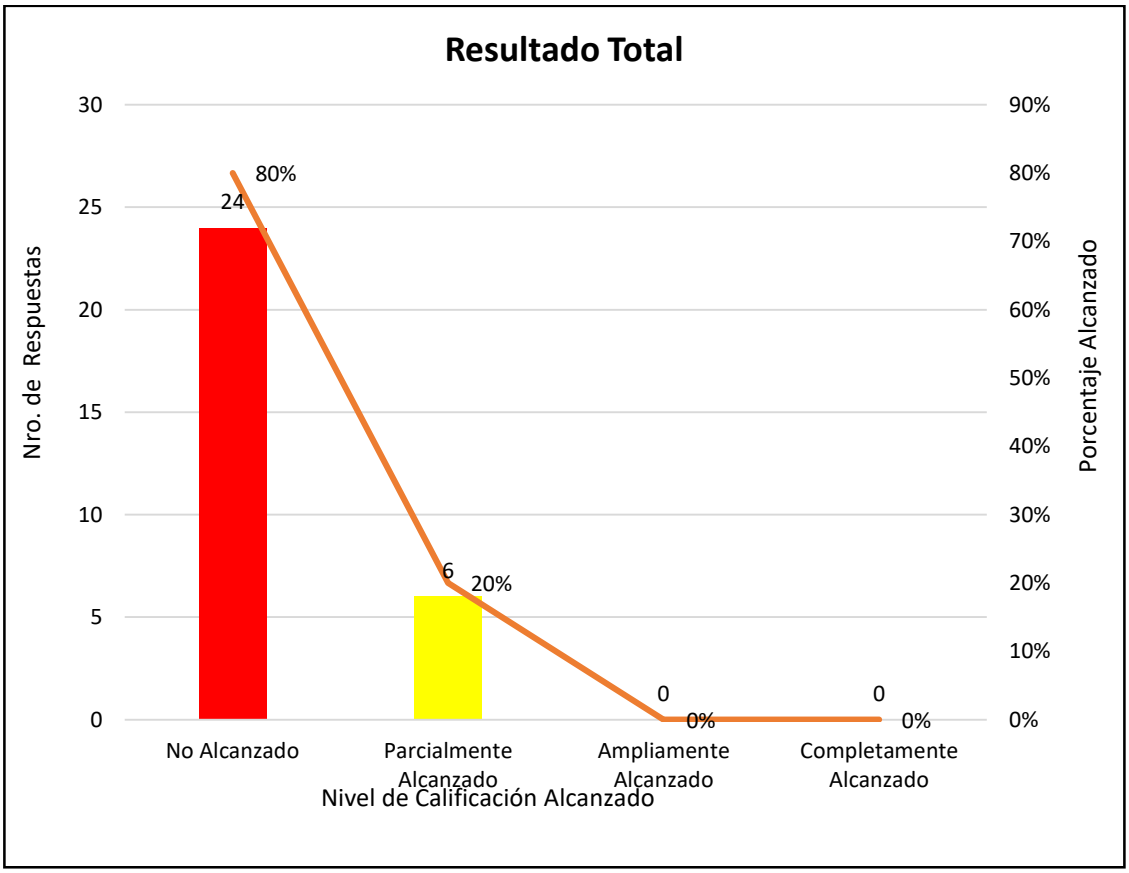
Fuente: Elaboración propia

- **Análisis**: El 63% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 38% qué está implementado y alcanza su propósito.

- **Hallazgo**: Se identifica ausencia de relación entre la gestión de la seguridad de la información y el gobierno universitario. En los procesos de valor no se detecta influencia de la seguridad. Existen algunos manuales y guías documentados de forma inadecuada e insuficiente; hecho que impide que sean sustentados ante los órganos directivos, para estudio con fines de aprobación y formalización como procesos. Al no existir procesos formales, no ha hay posibilidad que sean socializados entre la comunidad. Las respuestas dejan evidenciar una opinión es generalizada, en cuando a que hace falta mayor gestión en la implementación de procesos que conlleven a la gestión adecuada y coherente con las necesidades de la institución. La documentación con relación a las áreas de tecnología y sus servicios carece de normalizaicón y manejo de estándares.

7.1.3.5 Control Cultura, ética y comportamiento

- **Gráfica 18. Resultado control 5, cuestionario (anexo 2)**



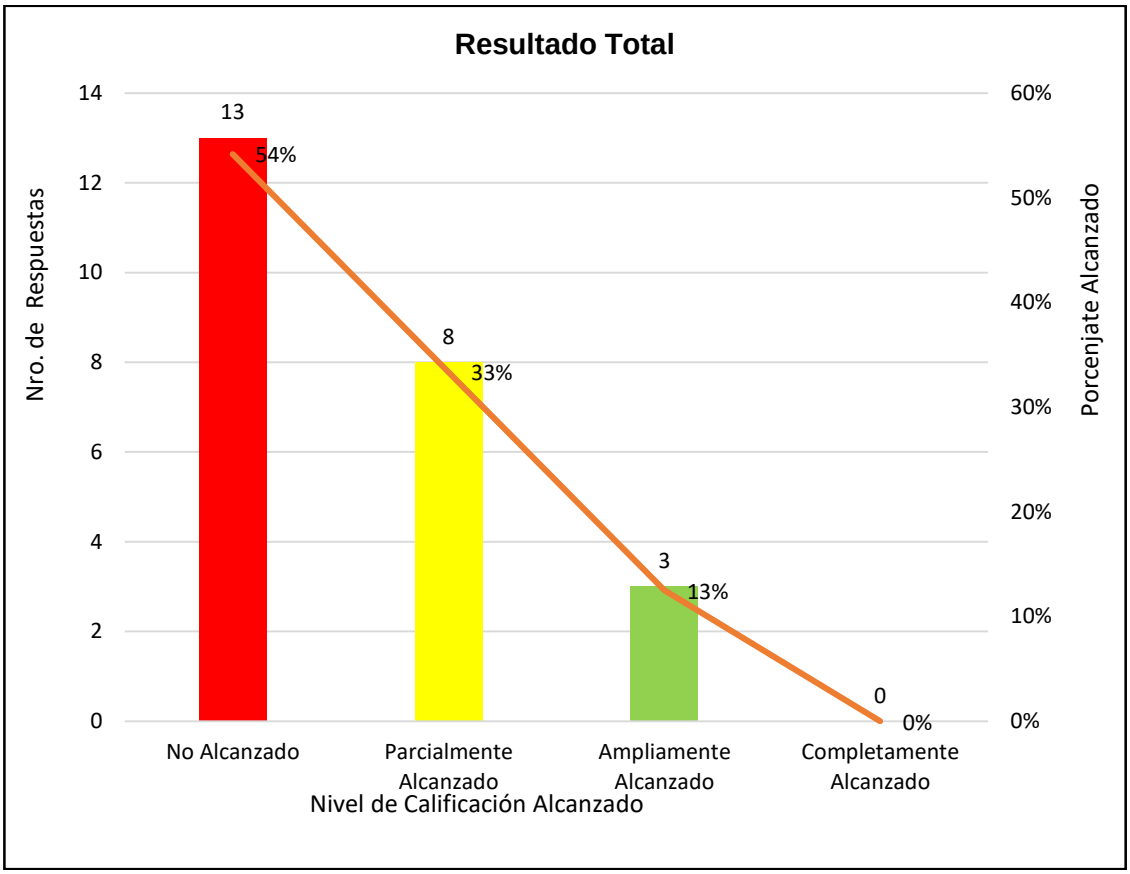
Fuente: Elaboración propia

- **Análisis**: El 80% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 20% qué está implementado y alcanza su propósito.

- **Hallazgo**: En la variable Cultura, ética y comportamiento, se detecta que el gobierno universitario no incluye en sus líneas estratégicas de cualificación de personal, la capacitación y formación en seguridad de la información y la prevención del riesgo informático. Acción que constituye un riesgo alto, al tener responsables de la información que no tienen la formación, concientización y culturización necesaria para el tratamiento y manejo adecuado de la información. Se recomienda que en los planes instituciones hayan líneas específicas que orienten el desarrollo de proyectos de tecnología, el diágnostico de en la necesidad de adquirir tecnología de una forma mas efectiva y eficiente, de acuerdo con las necesidades, prioridades y disponibilidad presupuestal.

7.1.3.6 Control personas, habilidades y competencias

- **Gráfica 19. Resultado control 6, cuestionario (anexo 2)**



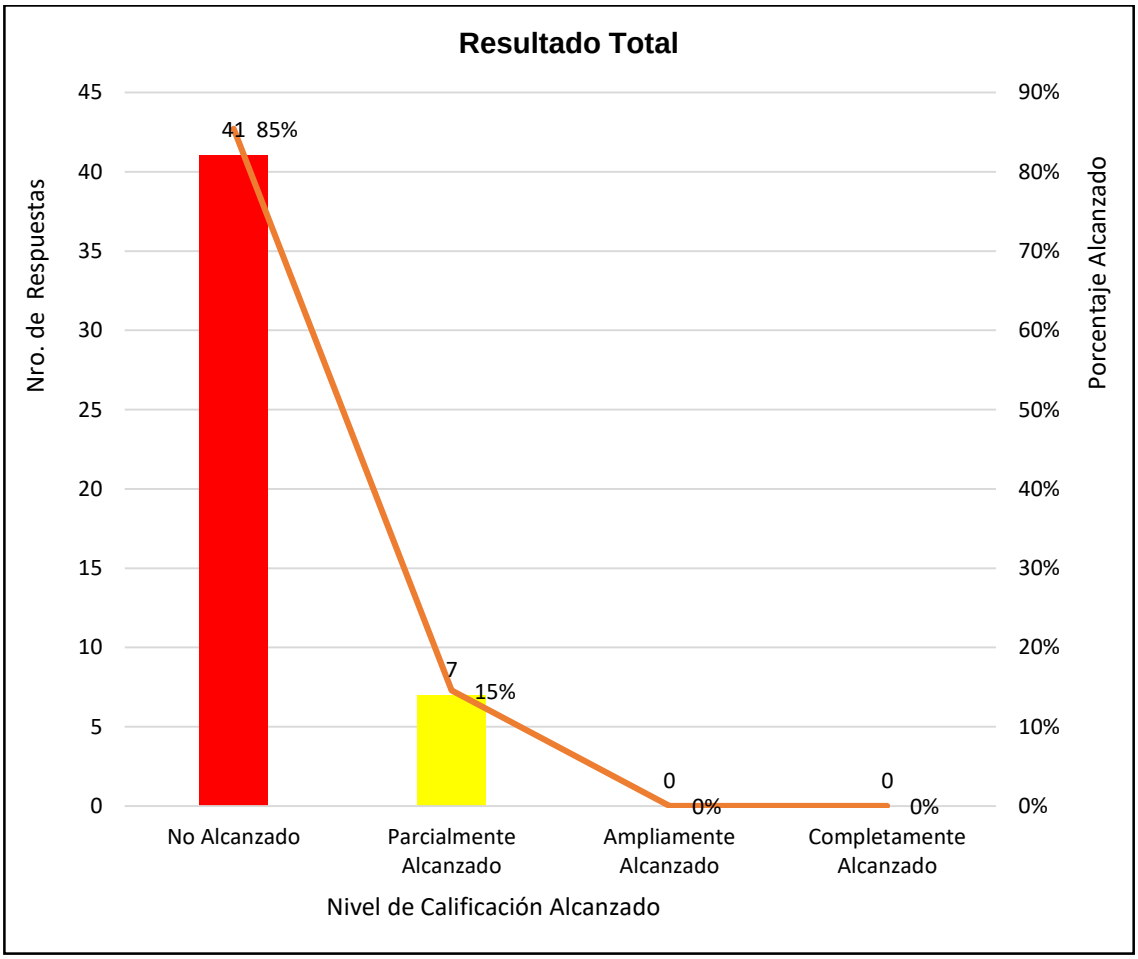
Fuente: Elaboración propia

- **Análisis:** El 64% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 33% qué está implementado y alcanza su propósito. El 13% qué está implementado de forma gestionada (planificado, supervisado y ajustado).

- **Hallazgo**: En el departamento de TIC, se tiene vinculado un profesional con especialización en seguridad informática. Esta situación representa un bajo porcentaje de talento humano dedicado a la gestión de la seguridad de la información, con relación al tamaño total de la población; que está representada en un aproximado de 6.500 usuarios entre estudiantes, docentes, personal administrativo y proveedores. Todos generadores y consumidores de información.

7.1.3.7 Control perfil de aceptación del riesgo

- **Gráfica 20. Resultado control 7, cuestionario (anexo 2)**



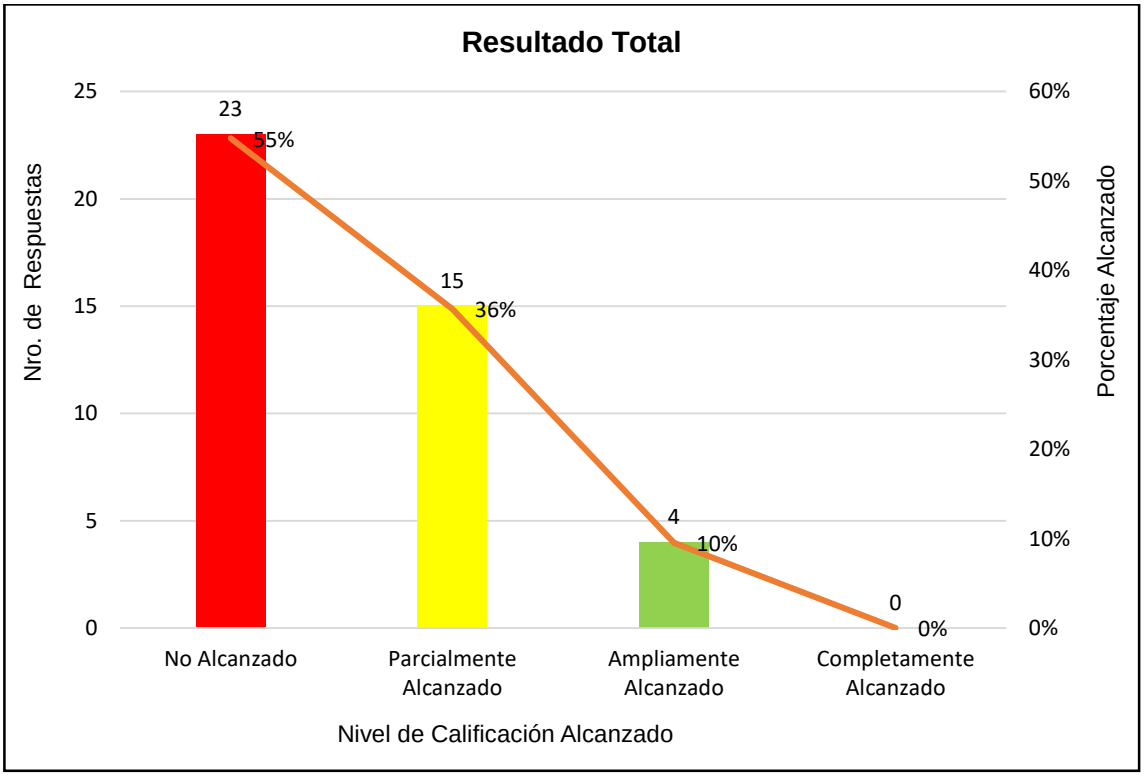
Fuente: Elaboración propia

- **Análisis**: El 85% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 15% qué está implementado y alcanza su propósito.

- **Hallazgo:** La institución, no gestiona el riesgo. No se identifica un programa de prevención y concientización. Los riesgos asociados a seguridad de la información, no son identificados; situación que hace imposible el reporte, análisis y gestión de estos. Este hallazgo genera incertidumbre sobre la brecha existente entre los procesos de valor y la seguridad de la información, según la criticidad de los activos de información.

7.1.3.8 Control Arquitectura de Seguridad de la Información

Gráfica 21. Resultado control 8, cuestionario (anexo 2)



Fuente: Elaboración propia

- **Análisis:** El 55% de los entrevistados afirma que el control no está implementado o no alcanza su propósito. Hay muy poca o ninguna evidencia. El 36% qué está implementado y alcanza su propósito. El 10% qué está implementado de forma gestionada (planificado, supervisado y ajustado).

- **Hallazgo:** No existe una arquitectura de seguridad de la información configurada por procesos sistemáticos, que dé la posibilidad de detectar amenazas y vulnerabilidades de forma oportuna y eficaz. Tampoco un plan de continuidad de negocio formal, que haya sido revisado y aprobado por los órganos directivos. Existen actividades parciales, que no reflejan en su totalidad las necesidades actuales de la institución. Se evidencia baja documentación y los procedimientos se ha elaborado al interior la dependencia de TIC, a criterio propio; careciendo de revisión y aprobación formal. Estos no son conocidos en los organismos de control interno. No todos los sistemas de información tienen matriz de roles y perfiles; los que la tienen, no se actualiza sistemáticamente. No se realizan pruebas de penetración en las plataformas tecnológicas.

- **Tabla 8. Resultados generales, aplicación del cuestionario**

Los siguientes es la calificación asignada a cada control, con base en los criterios de evaluación definidos (tabla 3) y los datos analizados, según las respuestas obtenidas por el grupo de entrevistados.

Control	Valoración	Rango
Legislación, principios, políticas y marcos de referencia	No Alcanzado	> 0% - 25%
Estructura organizacional	Parcialmente Alcanzado	> 25 % - 50%
Disponibilidad de recursos	No Alcanzado	> 0% - 25%
Procesos	No Alcanzado	> 0% - 25%
Cultura, ética y comportamiento	No Alcanzado	> 0% - 25%
Personas, habilidades y competencias	No Alcanzado	> 0% - 25%
Perfil de aceptación del riesgo	No Alcanzado	> 0% - 25%
Arquitectura de seguridad de la información	No Alcanzado	> 0% - 25%

Fuente: Elaboración propia

7.1.3.8 Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión universitaria

A continuación, se mencionan los principales hallazgos encontrados, durante las entrevistas realizadas y patrón general de la evaluación, a partir de resultados de la aplicación del cuestionario.

- No hay políticas definidas para garantizar que la información que se genera y consumen en la institución, está siendo tratada con confidencialidad, fiabilidad y autenticidad. Si bien existen documentos; estos no han sido aprobados por los organismos directivos. Se observa baja injerencia del cuerpo directivo en los temas de seguridad de la información.

- No se tiene certeza que se esté cumpliendo con los aspectos de ley; es posible qué por omisión o desconocimiento no se esté realizando la debida gestión. Aunque existe una Dirección Jurídica que se encarga de velar por el cumplimiento de toda la parte legal; su intervención sería reactiva y no preventiva, ante algún suceso. Preocupa de forma significativa el cumplimiento de la Ley 1581 de 2012, activa para Colombia y estrechamente relacionada con la seguridad de la información en el manejo de datos personales.

- No se tiene mecanismos formales de seguir un programa de gestión de seguridad de la información; si bien se ejecutan recomendaciones de organizaciones formales como ISO e ISACA, en ISO - 27000, COBIT 5, ITIL y otros, no son prácticas estandarizadas, implementadas, ejecutadas y documentadas bajo el lineamiento de un marco de referencia.

- No existe una política de manejo de permisos y/o perfiles de los usuarios, que indique como asignar y/o retirar accesos a los usuarios de los diferentes sistemas de información. También se identifica ausencia de procedimientos para esta responsabilidad.

- En la estructura organizacional, no se visualiza una jerarquía específica para la seguridad de la información, solo existe un cargo y depende de la Jefatura de TIC; generando ineficacia al ejercer en la línea de operación y soporte. En los órganos directivos, no se evidencia que la seguridad de la información tenga relevancia en la línea estratégica institucional; a pesar tener contexto e impacto transversal a la institución.

- A pesar de identificarse un presupuesto y algunas herramientas para la gestión de la seguridad; se evidencia carencia de recursos; principalmente para abordar estrategias de culturización, concientización, prevención y detección de vulnerabilidades y amenazas en los sistemas de información. Llama la atención que el grupo de talento humano dedicado a la gestión de los sistemas de información, no esté formado en seguridad de la información; también el desconocimiento en las regulaciones de ley que le implican.

- No existe procesos formales relacionados con la gestión de la seguridad de la información y prevención del riesgo informático. Existen documentos que se ha ido creando dentro de la cotidianidad del ejercicio del personal responsable.

- Los programas de culturización, concientización y formación en aspectos relevantes en seguridad de la información, son totalmente ausentes de los planes estratégicos y de operación del gobierno universitario.

- La institución carece de personal formado en seguridad de la información en sus cargos estratégicos, de operación y técnicos. Solo, el Oficial de Seguridad de la institución, tiene formación especializada. Los demás funcionarios han adquirido alguna formación básica por motivación personal o requerimientos específicos.

- La institución no tiene implementado un programa de prevención y análisis, del riesgo informático; no se identifica vulnerabilidades ni amenazas, en consecuencia, no se hace gestión del riesgo.

- No existe un modelo sistemático de arquitectura de seguridad; aunque se tiene una herramienta tecnológica, no se han definidos políticas, procesos, procedimientos que pudieran dar respuesta efectiva la gestión a través de un sistema integrado y prevención del riesgo.

7.2 Instrumento Dos (matriz de análisis de riesgo, Criterio 2)

Tiene el propósito de detectar las vulnerabilidades y amenazas a las que se encuentran expuestos los activos de información; así como la probabilidad de ocurrencia de eventos y magnitud del daño que tendrían los posibles eventos.

- **Tabla 9. Ficha Técnica**

Resume la información relevante la aplicación del instrumento y el análisis de resultados con base en los datos obtenidos.

Dimensión	Sistemas de Información
Criterio	Calidad de los criterios de seguridad de la información en ambientes de producción.
Controles	Manejo de Errores y de eventos de registro
	Tratamiento de usuarios y contraseñas de acceso
	Políticas y técnicas de autenticación
	Transporte de Datos
	Administración de sesiones de trabajo
	Gestión de cambios
	Gestión de la capacidad
	Segregación de los ambientes de desarrollo. Pruebas, preproducción y producción
	Protección contra código malicioso
	Controles criptográficos
	Gestión de las vulnerabilidades técnicas
	Gestión de técnicas anti robo de información
Método de recolección de datos	Formato de matriz de riesgo
Método de aplicación	Entrevistas y criterio de experto en seguridad de la información
Método para selección de la muestra	No probabilístico
Muestra	Plataformas tecnológicas
Población objeto de medición (categorías)	Equipo administrador de la plataformas tecnológicas
	Oficial de seguridad de la Información
	Líder Funcional – ERP Institucional
	Ingeniero de Soporte Técnico Sistemas de Información
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

Fuente: Elaboración propia

7.2.1 Muestra de activos de información

Toda organización, está expuesta a múltiples riesgos de seguridad, razón por la cual debe considerar y dar importancia a los cambios o alteraciones que lleguen a afectar los activos de información, evitando acciones negativas al normal funcionamiento. Para la aplicación y análisis, se determinó seleccionar plataformas tecnológicas con clasificación diferente, según el nivel de criticidad del servicio académico que soporta y el impacto que tendría su indisponibilidad para los procesos de valor.

Tabla 10. Sistemas de información para evaluación

Tipo	Plataforma tecnológica	Clasificación	Bases de datos	Lenguaje de desarrollo
Aplicaciones de software	Sistema de información para la gestión académica	Crítico	ORACLE	PL / SQL. JAVA
	Sistema de gestión financiera	Crítico	ORACLE	PL / SQL. JAVA
	Sistema de pagos en línea	Crítico	ORACLE	PL / SQL. JAVA
	Audiovisuales	Bajo	MYSQL	PHP
	Biblioteca	Medio	MYSQL	PHP
	Publicación de horarios	Medio	MYSQL	PHP
	Prácticas empresariales	Bajo	MYSQL	PHP

Fuente: Elaboracación propia, a partir del inventario de activos de valor de la institución

Criterios de seguridad para la valoración de activos de información

Se utiliza para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en un criterio de seguridad especifico, corresponde a la medida de perjuicio para la institución, si el activo se ve dañado por la falta de este criterio.

Tabla 11. Criterios de evaluación

D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de la información
A	Autenticidad

Fuente: Metodologia MAGERIT Versión 3

7.2.1 Valoración activos de información en función de la magnitud del daño

Se utilizará para elaborar una matriz guía de la magnitud del daño sobre la afectación de un activo, según la importancia de este y en caso que una amenaza se materialice por ausencia o manejo inadecuado de uno o varios criterios de seguridad de la información. Esta guía, es referente durante la identificación y valoración de riesgos informáticos; no es de estricto cumplimiento, considerando que cada activo opera diferente, según el servicio académico que atiende y su criticidad.

- **Tabla 12. Matriz para escala de valoración de la magnitud del daño**

Magnitud de Daño			Aplicación de Software	Criterios			
				D	I	C	A
1	Bajo	B	Sistema de información para la gestión académica	C	C	C	C
2	Medio	M	Biblioteca	A	A	B	M
3	Alto	A	Sistema de pagos en línea	C	C	C	C
			Publicación de horarios	B	M	M	M
4	Critico	C	Sistema de gestión financiera	C	C	C	C
			Audiovisuales	B	B	B	M
			Prácticas empresariales	B	M	B	B

Fuente: Elaboración propia, a partir de la metodología magerit versión 3.0

7.2.2 Escala de valoración de controles de seguridad en función de la probabilidad de amenaza

Se utilizará para elaborar una matriz guía de la probabilidad de amenaza con base en el control evaluado, según la importancia de este en la operación e impacto en un activo de información, por ausencia o manejo inadecuado de uno o varios criterios de seguridad. Esta guía es un referente para la identificación y valoración de riesgos de informáticos; no es de estricto cumplimiento, considerando que cada control actúa según las condiciones de exposición al riesgo del activo, la relevancia del servicio académico y su criticidad.

Tabla 13. Escala para valoración de la probabilidad de amenaza

Probabilidad de Amenaza			Control	Criterios			
				D	I	C	A
1	Insignificante	I	Manejo de errores y de eventos de registro	A	A	A	A
2	Baja	B	Tratamiento de usuarios y contraseñas de acceso	A	A	A	A
3	Mediana	M	Políticas y técnicas de autenticación	A	A	M	A
4	Alta	A	Transporte de Datos	A	A	A	A
			Administración de sesiones de trabajo	B	M	M	M
			Gestión de cambios	I	B	I	B
			Gestión de la capacidad	A	M	M	I
			Segregación de los ambientes de desarrollo, pruebas, preproducción y producción	I	I	I	I
			Protección contra código malicioso	A	A	A	A
			Controles criptográficos	M	A	A	A
			Gestión de las vulnerabilidades técnicas	M	A	M	M
			Gestión de técnicas anti robo de información	A	A	M	M

Fuente: Elaboracación propia, a partir de la Metodología MAGERIT Versión 3.0

Variables y componentes de medición instrumento 2

Las variables se han determinado para que el instrumento se aplique a la población objeto. Los resultados serán sometidos a análisis en coherencia con los datos obtenidos en la matriz de riesgo. En el proceso de identificación y evaluación de riesgos se tendrá en cuenta la clasificación asignada a cada plataforma tecnológica según su nivel de criticidad (tabla 10), los criterios de seguridad para la valoración de activos de información (tabla 11), las escalas de valoración de activos en función de la magnitud del daño y valoración de controles de seguridad en función de la probabilidad de amenaza; descritas en las tablas 12 y 13 respectivamente.

Los componentes para la medición de la matriz de riesgo son: variable 1, compuesta por los controles de seguridad de la información, con los conceptos que definen la pertinencia e injerencia de cada control en los activos de información y la escala de probabilidad de amenaza. La variable 2, la integra las plataformas tecnológicas y la escala de la magnitud del daño. La operación aritmética, es la multiplicación de la probabilidad de amenaza por la magnitud de daño, cuyo resultado es el riesgo. Otro aspecto, es el umbral del riesgo que define la clasificación, entre las opciones: bajo, medio o alto, según el rango definido en la composición de la matriz.

- **Tabla 14. Escala de componentes**

Criterio 2												
Control	**Variable 1**											
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Elementos (verificación de cumplimiento del control)	16	13	9	5	8	9	5	10	9	7	11	6
Escala probabilidad de amenaza	1			2			3			4		
	Insignicane			Bajo			Medio			Alto		
Criterio 1												
Sistema de Información	**Variable 2**											
	S1	S2	S3	S4	S5	S6	S7					
Escala magnitud del daño	1			2			3			4		
	Bajo			Medio			Alto			Critico		
Fórmula												
Riesgo	**(probabilidad de amenaza) x (magnitud de daño)**											
Umbral del riesgo												
	Categoría			**Mínimo**			**Máximo**					
	Bajo			1			2					
	Medío			3			6					
	Alto			8			16					

Fuente: Elaboracación propia, a partir de la Metodología MAGERIT Versión 3.0

- **Tabla 15. Matriz de clasificación del riesgo**

Zona Verde	1	Bajo
	2	
Zona amarilla	3	Medío
	4	
	6	
Zona roja	8	Alto
	9	
	12	
	16	

Fuente: Elaboracación propia

Según los valores mínimos y máximos del umbral de riesgo, se definen la zona de clasificación que puede tomar cada control de seguridad, de acuerdo al resultado obtenido durante la evaluación de los componentes.

7.2.5 Caracterización de resultados

A continuación, se presentará la medición obtenida después de aplicar el instrumento 2 denominado matriz de riesgo. Todo hallazgo que se encuentre en la zona roja, será considerado como el apetito de riesgo, es decir, el riesgo con el que se está dispuesto a convivir en las operaciones normales diarias. Todo riesgo en la zona amarilla, será interpretado como tolerancia al riesgo, es decir, el nivel aceptable del riesgo. Todo riesgo en la zona verde, se considerará como la capacidad de riesgo, es decir, el riesgo que la institución puede aceptar.

Resultado matriz de riesgo, evaluación de sistemas de información

- **Tabla 16. Resumen análisis de riesgo**

Plataforma Tecnológica	C1		C2		C3		C4		C5		C6		C7		C8		C9		C10		C11		C12	
	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%
Sistema de Información para la Gestión Académica		88		100		100		100		100		100		100		100		100		100		100		100
Biblioteca		50		54		78		60		63		67		60		50		78		100		91		50
Sistema de Pagos en Línea		88		100		100		100		100		100		100		100		100		100		100		100
Publicación de Horarios		50		54		78		60		63		67		60		50		66		100		91		50
Sistema de Gestión Financiera		88		100		100		100		100		100		100		100		100		100		100		100
Audiovisuales		81		100		89		100		100		78		100		63		78		57		91		83
Práticas Empresariales		81		100		89		100		100		78		100		63		78		57		91		83

Fuente: Elaboración propia, a partir de los resultados de la matriz de riesgo (instrumento 2).

En la tabla 16, se expone el resultado del nivel de riesgo alcanzado, con base en la aplicación del instrumento, que consistió en obtener información de cada plataforma tecnológica durante la entrevista con funcionarios del área de TI responsables de la administración y operación, con los usuarios que actúan como líderes funcionales de los sistemas seleccionados y la verificación de evidencias. Con la información que se recopiló, se procedió a valorar los elementos de cada control, de acuerdo a las variables y componentes de medición definidos. Previamente se asignó el valor de magnitud de daño a cada plataforma tecnológica, según el servicio que presta, criticidad de operación y el impacto que tendría para la institución su indisponibilidad o daño.

7.2.6 Análisis de riesgo

La evaluación de los controles de seguridad en los sistemas de información gestión académica, pagos en línea y gestión financiera; se ubicó en una valoración de riesgo

alto. En el resultado se halló una situación de riesgo superior al 85%, teniendo como referencia la criticidad que representan las tres plataformas tecnológicas en la prestación de los servicios académicos. Ante la materialización de la amenaza, la magnitud del daño sería critica para la institución e impactaría los procesos de valor.

En las plataformas tecnológicas: Biblioteca y Publicación de Horarios, al igual que en los sistemas descritos anteriormente, se identificó ausencia de los elementos que considerados relevantes, para preservar las condiciones de seguridad; sin embargo, estos sistemas están clasificados dentro de la criticidad de operación y servicio en un nivel medio. El umbral de riesgo, se ubicó entre los valores 3 y 16 de acuerdo con la valoración asignada para cada componente. La clasificación del riesgo predomina en la zona amarilla, con tendencia a ubicarse en una clasificación de riesgo alto, al obtener en la evaluación un porcentaje entre el 50% y el 100% (tabla 13). La indisponibilidad de las plataformas o daño, no impactaría los procesos de valor, no obstante, si la calidad del servicio; al afectar toda la población institucional.

Las plataformas tecnológicas: Audiovisuales y Prácticas Empresariales, están clasificados en criticidad del servicio baja. La probabilidad de amenaza es media y la magnitud del daño mediana; al predominar la clasificación del riesgo en la zona amarilla. A pesar de ser soluciones tecnológicas, clasificadas en el nivel más bajo del servicio; se identificó ausencia de los controles y componente evaluados; siguiendo la línea de las demás soluciones. La indisponibilidad del servicio afectaría a un grupo minoritario en comparación con el total de la población; sin posibilidad de impactar los procesos de valor y con una afectación del servicio baja.

- **Tabla 17. Clasificación del riesgo soluciones tecnológicas**

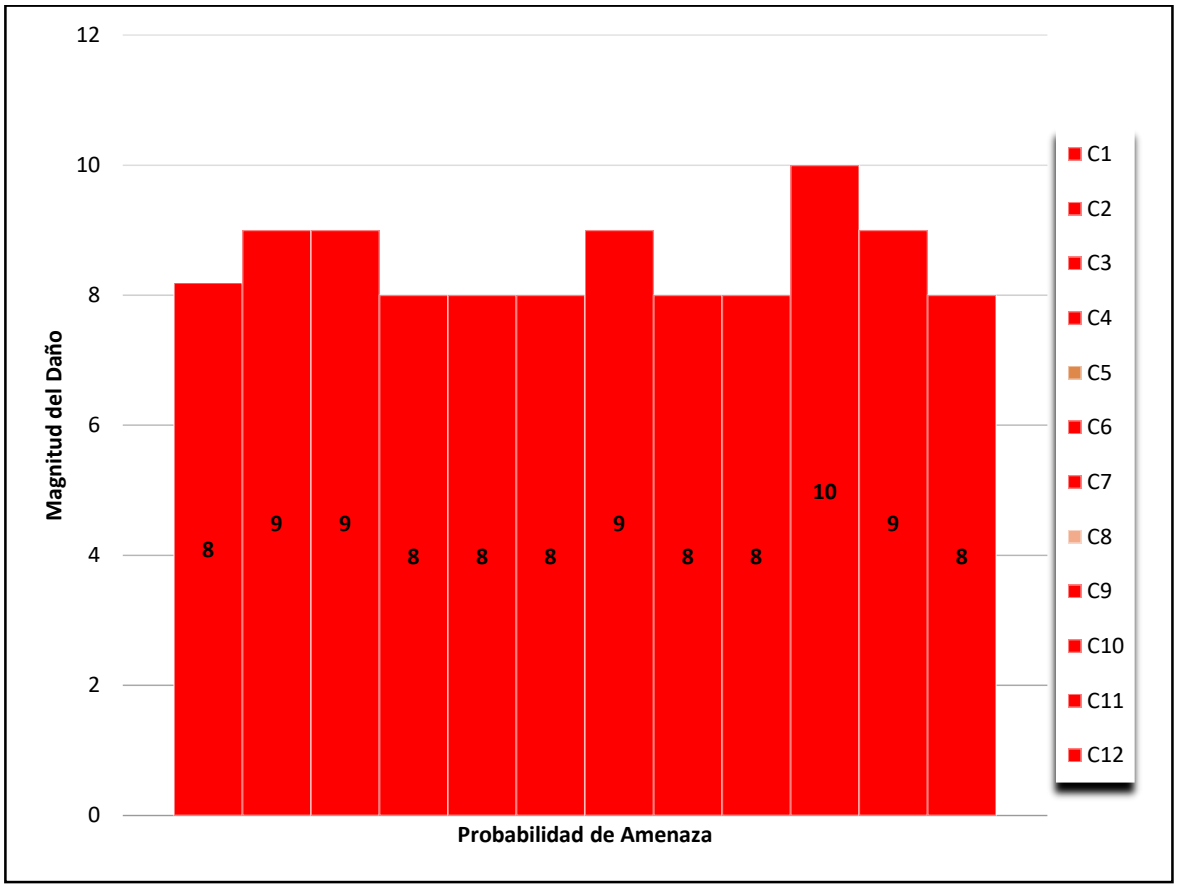
Plataforma tecnológica	Zona de clasificación del riesgo	Impacto procesos de valor
Sistema de Información para la Gestión Académica		SI
Biblioteca		NO
Sistema de Pagos en Línea		SI
Publicación de Horarios		NO
Sistema de Gestión Financiera		SI
Audiovisuales		NO
Prácticas Empresariales		NO

Fuente: Elaboración propia

En la tabla 17, se visualiza la clasificación del riesgo alcanzada para cada plataforma evaluada; conforme en la valoración realizada, el umbral definido para la matriz de riesgo. 3 de las 7 plataformas obtuvieron una calificación de riesgo alta;

situación que debería alarmar al gobierno universitario, al Director de TI, al grupo de administración, operación y soporte de las plataformas tecnológicas. También a los usuarios que son responsables del tratamiento los activos y la emisión de información para detectar, proponer e implementar planes de mejora de forma urgente.

- **Gráfica 22. Análisis promedio de riesgo**



Fuente: Elaboración propia

El análisis promedio de riesgo, producto de la evaluación cuantitativa a cada control de seguridad de la información, proyecta un escenario para la institución en situación de riesgo alto. La probabilidad de amenaza es alta y ante la materialización de un daño su impacto sería crítico. El resultado evidencia carencia de gestión de la seguridad de la información, del riesgo informático y baja garantía de la inclusión y calidad de los criterios que definen la información como: fiable, confidencial, integra y disponible.

7.2.7 Calidad de los criterios de seguridad de la información en ambientes en producción

.

A continuación, se mencionan los principales hallazgos encontrados, durante las entrevistas realizadas y patrón general de la evaluación, a partir de los resultados del análisis de riesgo.

- No se evidencia políticas, procesos ni procedimientos para: el manejo de errores, el registro de eventos, la funcionalidad de las aplicaciones, el tratamiento de usuarios, el control de acceso, el transporte de datos, las sesiones de trabajo, el control de cambios, el seguimiento de recursos y la segregación de ambientes para reducir los riesgos de acceso no autorizado. Tampoco para la protección contra código malicioso, uso de controles criptográficos, gestión de las vulnerabilidades técnicas e intervención de vulnerabilidades.

- Las aplicaciones que prestan servicio a las comunidades académica y administrativa, tiene autenticación básica. Las medidas de seguridad carecen de solidez para protección de posibles ataques. La falta de mayor robustez en los controles de seguridad, compromete la integridad, disponibilidad y autenticidad de las plataformas tecnológicas y de la información. La evaluación se califica baja, porque las medidas tomadas no son las mejores, ni las más eficientes, se deben mejorar los procesos para cifrar las contraseñas en los sistemas de información y los lineamientos para la creación, mantenimiento y uso en las mismas.

- No existen políticas claras para que una nueva plataforma entre en funcionamiento. Como consecuencia es vulnerable a explotación por condiciones de negación de servicio, situación que tampoco es ajena a las plataformas que están en producción actualmente.

- No existen mecanismos de detección de intrusos ni de alertas tempranas por fallos. La institución ha realizado inversión en algunas herramientas, sin embargo, no están 100% configuradas y no se hace trazabilidad a las métricas que ofrecen; razón por la que no se hace análisis de los datos recopilados y no se gestiona la información para que apoye la toma de decisiones.

- La estructura organizacional del equipo que trabaja técnicamente para las plataformas, es plana y no existen cargos por jerarquía, perfiles y roles. Todos los funcionarios del área de administración, mantenimiento y soporte; tienen el mismo cargo. La responsabilidad del funcionamiento operativo recae sobre el Director de TI, quien también tiene bajo su responsabilidad otras áreas, situación propicia para reducir la calidad de la eficacia y eficiencia del equipo de trabajo y de las plataformas.

- No existe un esquema de protocolos de autenticación para generar claves privadas, claves públicas y sistemas de firmas digitales. Ninguna plataforma tecnológica tiene implementado mecanismos para el cifrado por intermedio de funciones hash.

7.3 Instrumento tres (matriz de análisis de riesgo, criterio 3)

Tiene el propósito de detectar las vulnerabilidades y amenazas a las que se encuentran expuestos los activos de información; así como la probabilidad de ocurrencia de eventos y magnitud del daño que tendrían los posibles eventos.

- **Tabla 18. Ficha técnica**

En la ficha técnica se resume la información relevante para desarrollar las actividades en la aplicación del instrumento y el análisis de resultados.

Dimensión	Mantenimiento y soporte
Criterio	Calidad de los criterios de seguridad en el soporte y mantenimiento
Controles	Estructura organizacional
	Clasificación de la información
	Gestión de la prestación de servicios de proveedores
	Seguridad en los equipos de procesamiento de activos de información
	Control operacional del software
	Gestión de copias de respaldo
	Gestión de las comunicaciones y seguridad de las redes
Método de recolección de datos	Formato de matriz de riesgo
Método de aplicación	Entrevistas y criterio de experto en seguridad de la información
Método para selección de la muestra	No probabilístico
Muestra	Plataformas tecnológicas
Población objeto de medición (categorías)	Equipo de soporte técnico plataformas de información e infraestructura tecnológica.
	Oficial de seguridad de la información
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

Fuente: Elaboración propia

7.3.1 Servicios técnicos para evaluar

Se describe los principales servicios que se han considerado relevantes para atender la administración, mantenimiento y soporte técnico de las plataformas tecnológicas que están dispuestas para prestar servicios académicos.

Tabla 19. Servicios seleccionados

Tipo	Servicio
Servicios técnicos para plataformas tecnológicas	Gestión de activos de información
	Gestión de proveedores
	Gestión de la infraestructura y comunicaciones tecnológicas
	Gestión de planes de continuidad
	Gestión de copias de respaldo

Fuente: Elaboración propia

Para la valoración se tuvo en cuenta los mismos criterios de seguridad que se vienen manejando en las dos evaluaciones anteriores (confidencialidad, autenticidad, integralidad y disponibilidad). Se utiliza para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en un criterio de seguridad especifico, corresponde a la medida de perjuicio para la institución, si el servicio se ve dañado por la falta de este criterio.

7.3.2 Valoración servicios tecnológicos en función de la magnitud del daño

Corresponde a una matriz guía de la magnitud del daño sobre la afectación en la prestación de un servicio tecnológico, según la importancia de este y las consecuencias ante una amenaza que se materialice por ausencia o manejo

inadecuado de uno o varios criterios de seguridad de la información. Esta guía, es un referente para la identificación y valoración de riesgos informáticos durante la evaluación de la matriz de seguridad.

Tabla 20. Escala de valoración servicios tecnológicos

Magnitud de daño			Aplicación de software	Criterios			
				D	I	C	A
1	Bajo	B	Gestión de proveedores	A	A	A	A
2	Medio	M	Gestión de la infraestructura y comunicaciones tecnológicas	C	C	C	C
3	Alto	A	Gestión de planes de continuidad	C	A	A	A
4	Critico	C	Gestión de copias de respaldo	A	C	C	C

Fuente: Elaboracación propia, a partir de la Metodología MAGERIT Versión 3.0

7.3.3 Valoración de controles de seguridad en función de la probabilidad de amenaza

Se utilizará para elaborar una matriz guía de la probabilidad de amenaza con base en el control evaluado, según la importancia de este en la operación e impacto en un activo de información, por ausencia o manejo inadecuado de uno o varios criterios de seguridad. Esta guía es un referente para la identificación y valoración de riesgos de informáticos; no es de estricto cumplimiento, considerando que cada control actúa según las condiciones de exposición al riesgo del servicio, la relevancia del servicio académico y su criticidad.

- **Tabla 21. Escala de valoración servicios informático**

Probabilidad de Amenaza			Control	Criterios			
				D	I	C	A
1	Insignificante	I	Gestión de activos de información	A	A	A	M
2	Baja	B	Gestión de proveedores	A	A	A	A
3	Mediana	M	Gestión de la prestación de servicios de proveedores	A	A	A	M
4	Alta	A	Gestión de la infraestructura, redes y comunicaciones tecnológicas	A	A	A	A
			Gestión de planes de continuidad	A	A	A	M
			Gestión de copias de respaldo	A	A	A	A

Fuente: Elaboracación propia, a partir de la Metodología MAGERIT Versión 3.0

7.3.4 Variables y componentes de medición

Las variables se han determinado para la aplicación del instrumento. Los resultados serán sometidos a análisis en coherencia con los datos obtenidos en la matriz de riesgo. En el proceso de identificación y evaluación de riesgos se tendrá en cuenta la clasificación asignada a cada servicios tecnológico, según su nivel de criticidad (tabla 9), los criterios de seguridad para la valoración de activos de información (tabla 10), las escalas de valoración de activos en función de la magnitud del daño y valoración de controles de seguridad en función de la probabilidad de amenaza; descritas en las tablas 15 y 16 respectivamente.

Los componentes para la medición de la matriz de riesgo son: variable 1, compuesta por los controles de seguridad de la información, con los conceptos que definen la pertinencia e injerencia de cada control en el servicio y la escala de probabilidad de amenaza. La variable 2, la integra las plataformas tecnológicas y la escala de la magnitud del daño. La operación aritmética, es la multiplicación de la probabilidad de amenaza por la magnitud de daño, cuyo resultado es el riesgo. Otro aspecto, es el umbral del riesgo que define la clasificación, entre las opciones: bajo, medio o alto, según el rango definido en la composición de la matriz.

Tabla 22. Elementos para valoración de la matriz de riesgo

Criterio 3							
Control	**Variable 1**						
	C1	C2	C3	C4	C5	C6	C7
Elementos (verificación de cumplimiento del control)	6	5	9	20	8	5	6
Escala probabilidad de amenaza	1		2		3		4
	Insignicane		Bajo		Medio		Alto
Servicio Tecnológico	**Variable 2**						
	S1	S2	S3		S4		S5
Escala magnitud del daño	1		2		3		4
	Bajo		Medio		Alto		Critico
Fórmula							
Riesgo	**(probabilidad de amenaza) x (magnitud de daño)**						
Umbral del riesgo							
	Categoría		**Mínimo**		**Máximo**		
	Bajo		1		2		
	Medío		3		6		
	Alto		8		16		

Fuente: Elaboracación propia, a partir de la Metodología MAGERIT Versión 3.0

7.3.5 Resultados matriz de riesgo, evaluación sistemas de información

A continuación, se presenta la evaluación de la aplicación del instrumento 3 a través del formato matriz de riesgo. Los hallazgos entre el umbral de riesgo alto, serán considerados como el apetito de riesgo, es decir, el riesgo con el que se está

dispuesto a convivir en las operaciones normales diarias. Todo riesgo en el umbral medio, será interpretado como tolerancia al riesgo, es decir, el nivel aceptable del riesgo. Todo riesgo en el umbral bajo, se considerará como la capacidad de riesgo, es decir, el riesgo que la institución puede aceptar.

Tabla 23. Resumen análisis de riesgo por plataforma tecnológica

SERVICIO TECNOLÓGICO	CONTROLES													
	C1		C2		C3		C4		C5		C6		C7	
	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%
Gestión de activos de información		83		60		67		80		63		60		83
Gestión de proveedores		83		60		67		80		63		60		83
Gestión de la infraestructura y comunicaciones tecnológicas		100		100		55		55		100		100		83
Gestión de planes de continuidad		83		60		67		80		63		60		83
Gestión de copias de respaldo		100		100		55		55		100		100		83

Fuente: Elaboración propia

La tabla 23, muestra los resultados de la matriz de riesgo, con base en la aplicación del instrumento 3; que consistió en obtener información de cada servicio durante la entrevista con funcionarios del área de TI responsables del soporte técnico y mantenimiento, y la verificación de evidencias. Con la información que se recopiló, se procedió a valorar los elementos de cada control, de acuerdo a las variables y componentes de medición definidos. Previamente se asignó el valor de magnitud de daño a cada servicio, su criticidad e impacto que tendría para la institución su indisponibilidad o daño.

7.3.6 Análisis de riesgo

En el 100% de los servicios informáticos, se observa qué para su operación, se carece de políticas y procedimientos formales para la prestación del servicio. Si bien existente algunos documentos de apoyo que se han elaborado dentro de la dependencia de TI, no se pueden considerar como documentación formal; por su baja calidad y claridad, por ser insuficientes y porque no han sido revisados por los organismos del gobierno universitario para su aprobación. Las ausencias más relevantes, se dan en lineamentos para el plan de continuidad de operaciones ante posibles circunstancias de desastre, el plan de copias de respaldo, los procedimientos y flujos de proceso para la gestión de los activos de información y la gestión de proveedores. En lo que respecta a los servicios de Infraestructura y Comunicaciones, se hallan manuales e instructivos que deberían ser restructurados como procedimientos. Es urgente establecer una política general de prestación del servicio tecnológico.

7.3.7 Valoración de la situación de riesgos de seguridad en servicios tecnológicos

Con base en la matriz de clasificación del riesgo (tabla 15), este se ubica en una zona de riesgo alta para el 100% de los servicios tecnológicos; es decir de mitigación inmediata.

- **Tabla 24. Clasificación del riesgo servicios tecnológicos**

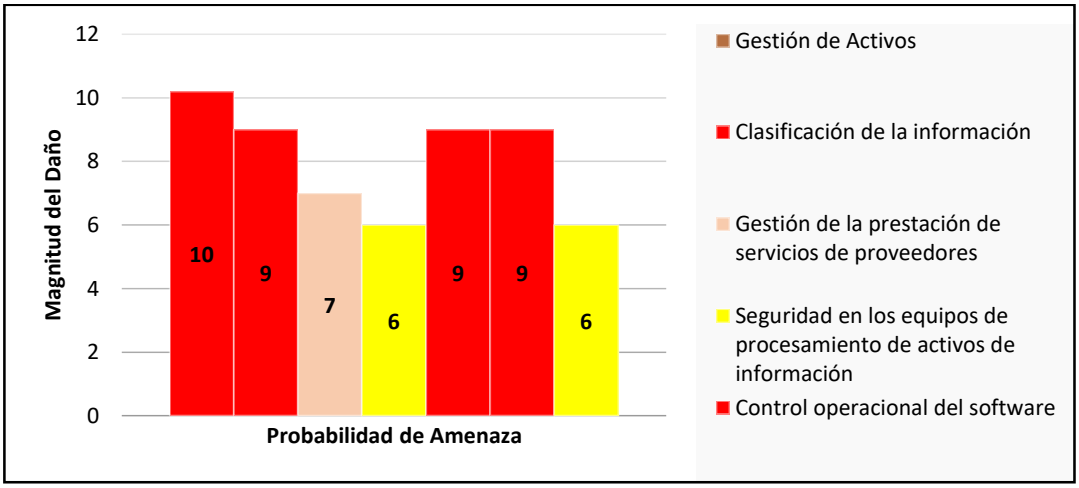
SERVICIO TECNOLÓGICO	ZONA DE RISGO	IMPACTA PROCESOS DE VALOR
Gestión de activos de información		SI
Gestión de proveedores		SI
Gestión de la infraestructura y comunicaciones tecnológicas		SI
Gestión de planes de continuidad		SI
Gestión de copias de respaldo		SI

Fuente: Elaboración propia

En la tabla 24, se visualiza la clasificación del riesgo para cada servicio, en coherencia con la valoración realizada. Se detecta qué, a pesar que la institución hace inversiones importantes en recursos tecnológicos, mantiene una situación de informalidad en la forma de desempeñarse.

7.3.8 Análisis promedio de riesgo

- **Gráfica 23. Resultado promedio evaluación matríz de riesgo**



Fuente: Elaboración propia

El análisis promedio de riesgo, producto de la evaluación cuantitativa a cada control de seguridad de la información, proyecta un escenario para la institución en situación de riesgo alto. La probabilidad de amenaza es alta y ante la materialización de un daño a través de uno de los servicios evaluados, su impacto sería crítico. El resultado evidencia carencia de gestión de la seguridad de la información en el servicio tecnológico, no obstante, se diferencia la calificación obtenida por los controles de seguridad en los equipos de procesamiento de activos de información, gestión de las comunicaciones y seguridad de las redes. El motivo, obedece a las inversiones que se realizan en el Área de Infraestructura Tecnológica en equipos hardware, comunicaciones, firewall y herramientas de software para mitigar riesgos de seguridad informática; sin embargo, es relevante la ausencia de políticas, protocolos, procesos y procedimientos, que incluye de manera importante para que la calificación, se situé en una zona roja (riesgo alto).

7.3.9 Calidad de los criterios de seguridad en el soporte y mantenimiento

A continuación, se mencionan los principales hallazgos encontrados, durante las entrevistas realizadas y patrón general de la evaluación, a partir de los resultados del análisis de riesgo.

- La institución no tiene una política de respaldo de la información bien definida. Existe una plataforma tecnológica (software), aun así, los usuarios no realizan el procedimiento para almacenar la información en la partición asignada; suceso que impide la completitud e integridad del procedimiento automático y la información a respalda. No se tiene cultura de practicar pruebas de verificación del sistema de respaldo, ni del estado de los datos. No se han diseñado políticas, protocolos ni tablas de retención de destrucción de la información.

- Se detecta riesgo latente en el almacenamiento de los backups a cinta. Se recomienda subcontratar el servicio de almacenamiento de cintas con las características técnicas que emiten los fabricantes, ante la ausencia de un espacio adecuado en el campus universitario.

- No existe un protocolo estándar de registros y actualización de novedades. La institución tiene una política de gestión de activos que está orientada en todo sentido a los activos físicos, contiene información mínima de los activos lógicos.

- Existen una clasificación básica de los activos de información más relevantes, que no está regulada por políticas ni procedimientos. Se requiere dar formalidad a la clasificación para asignar responsabilidades de administración, manejo, uso y actualización con base en el desempeño diario.

- Se detecta alto riesgo por unidades portables (USB) con información sin cifrado; no se controla su uso, ni existen políticas ni procedimientos de restricción de acceso de estos elementos en los equipos que manejan información sensible y

crítica. Está condición origina exposición al riesgo de fuga de información sensible, infección de los equipos por virus informático, manejo inadecuado de datos críticos, entre otros.

- Se detecta limitación de personal, los cargos profesionales están supeditados a una persona por responsabilidad; ante ausencias o retiros las operaciones se pueden ver altamente afectadas, por falta de personal calificado que dé continuidad a la operación tecnológica institucional. Se debe definir e implementar los roles y responsabilidades asociados a la gestión, adecuado mantenimiento y sostenimiento de la infraestructura, de igual forma contratar el personal requerido.

- No existe una política, ni procedimientos formales para gestión de proveedores que tengan que intervenir en las plataformas tecnológicas, no obstante, la Dirección Jurídica apoya esta labor con la elaboración de contratos de respaldados por pólizas de cumplimiento, calidad y la firma de cláusulas de confidencialidad. No se observa registros de evaluación de los proveedores a la finalización de contratos.

- No se evidencia un procedimiento documentado para las actualizaciones de sistemas operativos, versiones de software, librerías antes de su ejecución; tampoco una jerarquía de aprobación y supeprvisión de las actualizaciones.

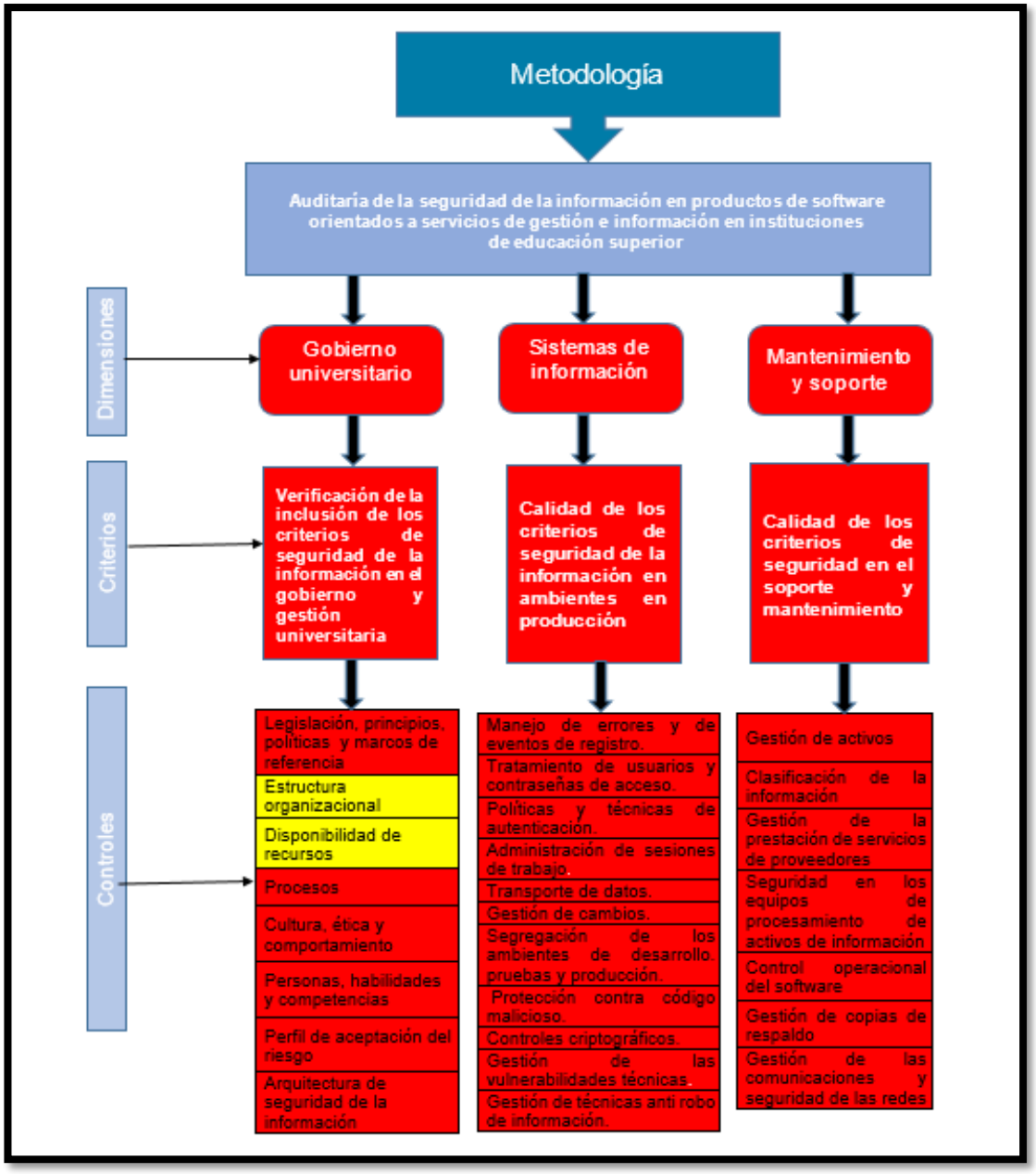
- No se detecta una política de gestión de redes y comunicaciones que asegure que las actividades que se realizan son conocidas y reguladas por el gobierno universitario. La institución debe establecer, documentar e implementar políticas de gestión las comunicaciones y redes para asegurar el desempeño óptimo en los sistemas de información que se encuentran en producción.

7.4 Informe ejecutivo

A continuación, se presenta un resumen de la situación de los activos de información y condiciones generales de los criterios de seguridad de la información con base en la medición y evaluación practicada. Con el programa de auditoria realizado, se detectó riesgos en el proceso de gestión de la información, que podrían ser mejorados a través de la reingeniería e implementación de políticas y procedimientos. Se analizó la situación actual de la universidad para verificar la inclusión de los criterios de seguridad de la información en la gestión del gobierno corporativo, los sistemas de información, mantenimiento y soporte técnico e impacto en los procesos de valor y en la calidad la prestación de servicios académicos por un evento de indisponibilidad; con el objetivo que la institución conozca el nivel de madurez de los procesos asociados a la gestión de los activos de información y la brecha a superar para alcanzar una alineación entre las buenas prácticas y los servicios prestados. La evaluación se realizó mediante la medición de controles de

seguridad que se consideran debieran existir con base en lo que recomienda la norma ISO 27000 y su familia, para identificar vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los planes de mejorar adecuados para aceptar, disminuir, transferir o evitar la ocurrencia

Ilustración 10. Resultado Situación de Riesgo, Resultado de Auditoria



Fuente: Elaboración propia

7.4.1 Hallazgo Generales

- Las condiciones de riesgos que se describen en la gráfica 51, fueron obtenidas en su totalidad mediante la auditoria en seguridad de la información en productos de software orientadas a servicios de gestión académica e información en instituciones de educación superior. Al analizar el conjunto de la evaluación, se determina que la institución, no cumple con ningún criterio de seguridad de la información; los resultados arrojan un eminente hallazgo de riesgo alto sobre sus activos de información, continuidad de negocio, compromisos con terceros y cumplimiento de la legislación colombiana. Situación que expone a la institución a riesgos financieros, fuga de información, ineficiencia productiva, pérdida de prestigio y competitividad.

- Los principales hallazgos negativos, se dan por falta de políticas, procesos, procedimientos y documentación insuficientes; es decir por ausencia de formalización de las actividades, que denota una brecha entre el gobierno universitario y la gestión tecnológica; poniendo de manifiesto la carencia de controles de seguridad en la gestión de la información.

- Un aspecto relevante que se identificó, es la falta de inversión en programas de formación y capacitación en seguridad de la información en todas las dimensiones evaluadas.

- La organización no tiene cultura de auditar los procesos estratégicos ni operacionales de las tecnologías de información y comunicación. Si bien existe un departamento de control interno; su ejercicio se enfoca a los procesos financieros y contables. Dentro de su planta de personal, no tiene funcionarios formados ni capacitados para realizar auditorías internas en la operación de la estructura gerencial y operativa del departamento de TI, mucho menos en seguridad de la información.

- No existen métricas definidas para medir la operación y el desempeño de la dependencia de TI. Se han adquirido herramientas, no obstante, no se han definido las estratégicas de utilización, la funcionalidad y las métricas para evaluar el desempeño y apoyar la toma de decisiones de tipo estratégico, gerencial, funcional y operacional.

- El tráfico en la red pasa sin protección criptográfica. Como consecuencia es posible interceptar y modificar información sensible; situación que puede ser inadvertida por falta de controles que generen alarmas de forma oportuna. Este suceso compromete la confidencialidad de la información de toda la institución y el aprovechamiento de terceros.

- Los funcionarios dedicados a la administración, operación, mantenimiento y soporte de las tecnologías de información y comunicación, no realizan actividades de I+D; hecho que hace que las soluciones para la institución sean aportadas en alto porcentaje por los proveedores; sin verificación robusta que cumple con la necesidad de la institución.

- El Área de Seguridad de la Información, está conformada por un profesional y es relativamente nueva (2 años de conformada), situación que aporta para que la calificación de la seguridad de la información institucional se determine en un nivel de inmadurez y para que los controles de seguridad no estén definidos.

- Se concluye que la institución no tiene implementado un sistema de gestión de seguridad de la información; realiza una serie de actividades de seguridad descentralizadas e individuales que no pueden ser consideradas un sistema, al no estar integradas, articuladas y no funcionar como un todo en la búsqueda de un beneficio común.

7.4.2 Recomendaciones

Las recomendaciones que se emitirán a continuación se basan en la propuesta de buenas prácticas que propone ISACA en su marco de referencia COBIT 5, en la recomendación de la norma ISO 27.001: 27.013 y en la regulación de la ley 1581 de 2012 (Ley de Protección de Datos Personales); sobre las características que se estima debe contemplar un Sistema de Gestión de Seguridad de la Información (SGSI).

- En la estructura de la Organizacional, constituir un Comité de Gestión de Seguridad y Riesgo Corporativo (ERM - Enterprise Risk Management), que se encargue de establecer las políticas, niveles de riesgo aceptable, los planes de continuidad del negocio y episodios de crisis relacionados con los activos de información y de las tecnologías informáticas. De acuerdo con lo que recomienda COBIT 5, sus principales responsabilidades serían; definir y dirigir el sistema de seguridad y prevención del riesgo, definir el marco de gestión y la metodología, la estructura de gobierno del riesgo, revisar la exposición al riesgo, supervisar las actividades, priorizar los riesgos y la estrategia, revisar el estado de la respuesta a los riesgos y coordinar con los responsables del negocio la asignación de recursos.

- Desde el gobierno universitario, crear los medios y programas que ayuden a alcanzar los objetivos estratégicos; influyendo en la conducta, la aplicación de normas, el comportamiento de la comunidad universitaria y en la apropiación de una cultura de seguridad de la información. Los programas de sensibilización deben tener un espacio, pero no son suficientes por sí mismos. Más que ser conscientes del riesgo de la información, las personas necesitan ser formadas acerca de los riesgos y de su papel con ellos. Los diferentes niveles de gestión

en una empresa pueden promover la concienciación a través de los medios de comunicación internos.

- Propender por la puesta en operación de buenas prácticas, para crear, fomentar y mantener comportamientos deseados en la administración, mantenimiento y soporte de las plataformas tecnológicas; garantizando el uso adecuado y ético, con relación a la seguridad de la información. Las buenas practicas deben generar un estándar y un marco de gestión para la institución, constituido por el cumplimiento de la legislación, la creación de políticas útiles y aplicables en coherencia con el desempeño organización, la formalización de reglas y normas que orienten el comportamiento deseado, con vinculación clara de los principios y políticas que una institución requiere poner en práctica.

- Crear políticas, lineamientos y procedimientos enfocados a generar tolerancia cero hacia el incumplimiento de requisitos legales y regulatorios. La normalización alrededor de la seguridad debe ser de conocimiento y dominio de toda la comunidad universitaria; garantizando que todo el personal comprende la importancia de mantener una conciencia de seguridad de la información y prevención del riesgo informático.

- Desde el gobierno universitario, articular las partes relevantes para acordar acciones y seguimiento de los planes de acción, para asegurar la oportuna solución de problemas y el logro de los planes de negocio.

- Desde el gobierno universitario, mantener actitud de supervisión y seguimiento proactivo al riesgo y al avance de los planes de acción. Culturizar y concientizar a los equipos de trabajo en la necesidad e importancia de los procesos de auditoria como oportunidad de detección temprana del riesgo y mejora continua.

- Establecer las metas y las estructuras de desempeño, a fin de poner en ejecución los planes de acción que den razón de la mitigación de los hallazgos de seguridad y riesgo informático.

- Definir el ciclo de vida de la información y su clasificación, para diseñar el modelo de gestión de la Información e identificación de perfiles y roles de acceso; se deben utilizar dimensiones del ciclo de vida de la información. Esto significa los planificadores, receptores y usuarios de la información.

- Establecer la política de copias de respaldo por la institución y con base en ella realizar programas de capacitación y formación para motivar la generación de conciencia en el buen manejo de copias de respaldo. El programa debe ser monitoreado contantemente mediante aplicación de pruebas de fiabilidad, integridad y disponibilidad de la información. Se debe hacer trazabilidad diaria

de las herramientas de software que se tienen implementadas para la gestión de copias de respaldo.

- Incentivar entre el personal de TI, actividades de I+D, que brinde la capacidad de aportar a la adquisición de tecnología de punta para el desarrollo de su misión corporativa, basados en las necesidades de la institución, en las buenas prácticas implementadas y en la generación de valor agregado; para contribuir al cumplimiento de los objetivos estratégicos y procesos de valor, bajo el concepto de inversiones justas, suficientes y razonables.

- Se recomienda la intervención de los hallazgos de forma inmedita; al realizarlo la situación de seguridad de la institución cambiaría significataivamente; debido a que los hallazgos que emitieron la clasifican en riesgo alto (zona roja), está altamente relacionado con la ausencia de buenas prácticas, políticas, procedimientos, tecnologías y recomendaciones sobre medidas adecuadas para proteger los activos de información.

- Se recomienda implementar un programa de auditoria interna en seguridad de la información y seguridad informática que actué de forma permanente como apoyo a la prevención del riesgo información, la inclusión y evaluación constante de los criterios de seguridad y los controles implementados.

8. VERIFICACIÓN COMPLETITUD Y VALIDEZ DE LA METODOLOGÍA

8.1 Completitud

A continuación, se describirá el desarrollo metodológico, que permitió diseñar la propuesta, para auditar la seguridad de la información en productos de software orientados a servicios de gestión e información académica en instituciones de educación superior. Los conceptos que se describen a continuación tienen por objeto sustentar que la metodología fue diseña bajo el estándar de ser un proceso sistemático e independiente; guiado por los requisitos para evaluar la seguridad en activos de información.

- Con base en el objetivo general y los objetivos específicos, se definieron los criterios que se consideraron indispensables para dar sustento al desarrollo de la propuesta. Antes de llegar a la definición de los criterios fue necesario consultar, identificar y estudiar fuentes de información sobre trabajos ya desarrollados en el universo académico, que fuesen de contexto similar o con características que brindaran aportes a la tesis. La literatura estudiada se compuso de dos partes. Primera parte: artículos científicos producidos a partir del año 2012. Segunda parte: Fundamentos teóricos, basados en la producción de libros, normas ISO, estándares de buenas prácticas, estudios (encuestas) sobre seguridad, que pudieran ampliar el concepto sobre la problemática a resolver y aportar en la materialización de la propuesta.

- La definición de los criterios, estuvo enmarcada en brindar un esquema que brindara la posibilidad de evaluar la seguridad de la información en un contexto universitario. Por tal motivo se planteó los escenarios organizacionales que se deberían intervenir, con el propósito de recopilar la información necesaria, para el análisis de los criterios que se pretendían evaluar. A estos escenarios se le denominó dimensiones.

- Habiendo definido los criterios a auditar, con base en las propuestas de la norma ISO:27.000 y COBIT 5 sobre buenas prácticas; se definió los controles necesarios para evaluar, si la información de una organización cumple con los estándares de seguridad denominados: confidencialidad, integridad, disponibilidad y autenticidad, para ser reconocida como activo seguro.

- La norma ISO:27.000, determina que, para aplicar una evaluación de seguridad de la información, cada control debe cumplir con una serie de requisitos propios, que al evaluar en conjunto determina si hay o no cumplimiento. Para el desarrollo de la tesis, se tomó como referencia los controles y requisitos estrictamente vinculados a la seguridad de la información; teniendo en cuenta a que la norma es robusta en el cubrimiento de todas las áreas de TI. Los requisitos asociados para cada control, se determinaron como componentes.

- Con los elementos de la metodología, se diseñó dos formatos como instrumentos de evaluación para los 3 criterios. El primer instrumento fue un cuestionario que específicamente va dirigido a medir la gestión del gobierno universitario en temas relacionados con seguridad de la información. Para los criterios 2 y 3, se diseñó una matriz de riesgo y estuvo enfocada a medir la aplicación de controles en los sistemas de información existentes, y el soporte técnico y mantenimiento de los mismos.

- Los instrumentos fueron revisados por dos expertos. Se realizaron los ajustes recomendados y posterior se hizo la aplicación en una institución de educación superior, con el apoyo de un especialista en el tema, que está certificado en auditoria de seguridad de la información. Con base en la norma ISO 19011, segunda edición 2011 – 11 – 15 (directrices para la auditoría de sistemas de gestión) se estructuró el ciclo de vida de la auditoria.

- Con la información recopilada, se realizó análisis estadístico de los resultados obtenidos en el cuestionario y en las matrices de riesgo. Junto con los resultados se presentó el concepto de evaluación por criterio, con base en los hallazgos.
- Por último, se realizó el informe ejecutivo, que consistió en un resumen de la situación general de seguridad de los activos de información y las recomendaciones para mitigar la situación hallada.

- El diseño de la metodología, fue ejecutado en su totalidad, durante el desarrollo del programa de auditoría; al aplicar todos los componentes propuestos, evaluarlos y emitir concepto técnico sobre la situación de seguridad en una institución de educación superior a través de los hallazgos obtenidos.

8.2 Validez

Como se ha mencionado durante el desarrollo de la tesis, en la actualidad la gestión y evaluación de la seguridad de la información se acepta y considera relevante en escenarios universales; el auge tecnológico conlleva a que a la par, haya proliferación de riesgos informáticos y a una necesidad especifica de proponer nuevos esquemas de verificación y evaluación de la seguridad para las organizaciones; que complementen las existentes y genere nuevas propuestas en aras de enriquecer las opciones de gestión, evaluación y control. Los estándares internacionales y nacionales emanan directrices y recomendaciones de propósito general, no obstante, la naturaleza de las organizaciones conlleva a que la exposición al riesgo informático sea diferente; según el sector de operación, la naturaleza, el contexto de desempeño y el tipo de usuarios que predomina. En consecuencia, como ya se ha puesto de manifiesto con anterioridad la metodología propuesta, aporta a auditar la seguridad de la información en ambientes de

desempeño universitario, tras haber identificado una necesidad de evaluación de la seguridad de la información en este sector específico.

El diseño, se centró en identificar y desarrollar los componentes necesarios para estructurar un esquema con condiciones similares, repetibles y aplicables con base en la legislación que están obligadas a cumplir las organizaciones, los estándares formalmente aceptados y los requerimientos de las instituciones de educación superior en materia de seguridad de la información. La metodología la integran tres componentes principales con sus respectivos subcomponentes, que en suma brindan una perspectiva específica para facilitar el desarrollo de un programa de auditoria en seguridad. La metodología se centra en las siguientes características:

- **Sistémica:** Ofrece una estructura interrelacionada y completa de los principales componentes que configuran los elementos y variables para auditar la seguridad de la información, a través de la aplicación de conceptos intelectuales validados y aceptados por escenarios académicos, científicos y empresariales.

- **Abierta:** Presenta una estructura relacionada con los sujetos que integran el entorno de la organización. Este principio ofrece, en suma, más de una perspectiva. Se puede optar por evaluar la seguridad en la totalidad de las tres dimensiones propuestas, como se realizó durante el desarrollo de la tesis; inclinarse por la evaluación de cada dimensión por separado o solo dos de ellas, es decir ofrece diversas alternativas, dependiendo de los recursos, necesidades e interés particular de evaluación.
- **Dinámica:** Pretende ofrecer un conjunto de elementos y variables, relacionados, que deben permitir la observación y el diagnostico, con el objetivo de ir reuniendo elementos de juicio, para emitir un concepto técnico justo y objetivo sobre la situación real de la seguridad de la información en universidades.

- **Repetible:** La metodología está diseñada para que se pueda aplicar en diferentes instituciones, debido a que las instituciones en términos generales están integradas por los tres escenarios intervenidos (gobierno universitario, sistemas de información, y mantenimiento y soporte); incluso con adaptaciones menores podría ser aplicarse a otro tipo de organizaciones; es necesario probar la metodología para validar la hipótesis propuesta.

- **Flexible:** Los controles y componentes propuestos pueden ser ordenados y aplicados de forma diferenciada a tenor de las necesidades de la institución, según sea la estrategia, el modelo de gestión y la relevancia de los activos de información; en función de procesos de valor y los objetivos estratégicos, de su tamaño, antigüedad, propiedad o finalidad. Estas razones pueden determinar que algunos controles y componentes de los propuestos, no se consideren relevantes durante el programa de auditoria, para diagnosticar la situación de seguridad de la

información en determina institución. Por ello se hace indispensable antes de iniciar el programa de auditoria, conocer el contexto a auditar y la finalizada.

- **Adaptativa**: La flexibilidad explicada en el ítem anterior, obliga a conocer el proceso, la estrategia y a definir si la aplicación de la metodología se realizará en su totalidad o de forma parcial. Depende de los recursos de auditoria disponibles, del tiempo estimado y de los resultados esperados.

- **Innovadora:** Reúne una serie de conceptos y componentes de seguridad formales con un diseño especifico; cuyo propósito es generar una herramienta de auditoria para seguimiento y control interno en las instituciones de educación superior; haciendo uso de las dependencias de control interno y los profesionales expertos en seguridad de la información, que ya están vinculados a las entidades. Un precedente para que las organizaciones se limiten en realizar procesos de auditoria, está relacionado con los costos que representa una contratación externa; por ello se abstienen de realizarlas o las realizan en periodos de tiempo muy prolongados en donde se pierde la continuidad y trazabilidad. La metodología, facilitará la labor a quien realice el proceso de auditoría y orientará el paso a paso como una guía especifica y aplicable.

9. CONCLUSIONES

- El desarrollo de la tesis, fue el resultado de la materialización de una necesidad identificada, relacionada con la falta de procesos de auditoria de seguridad de la información en instituciones de educación superior. La propuesta desde su planteamiento estuvo enfocada en aportar a este sector, un patrón de buenas prácticas a través de un diseño metodológico, que facilite y motive los procesos de auditoría para verificar la calidad e inclusión de los criterios de seguridad de la información, en las plataformas tecnológicas, que se utilizan durante el desempeño de las actividades cotidianas en las instituciones universitarias.

- Las organizaciones en general, apoyan su desempeño en la tecnología; siendo los sistemas de información las herramientas en las que confían el procesamiento de información para la toma de decisiones. Infortunadamente algunas empresas dentro de sus estrategias corporativas, no consideran primordial incorporar una cultura organizacional de autoevaluación, para detectar de forma temprana los riesgos a los que cotidianamente se ve expuesta; entre ellos los de seguridad de la información.

- Para el desarrollo de la tesis, fue necesario revisar la literatura formal, con el propósito de identificar los avances de investigación en materia de seguridad de la información, riesgo informático y auditoria. Con la revisión de casos de estudio, nuevos modelos y metodologías; sé validó cómo se está interviniendo el tema y qué propuestas han surgido como contribución, para que el universo corporativo pueda tomar medidas a tiempo y mitigar amenazas de tipo informático, evitando que se materialicen y conlleven a desastres en cualquier momento.

- Con la elaboración del marco conceptual, quedó evidenciado que el estudio de la seguridad de la información es un tema de interés entre la comunidad académica, que se dedica a la investigación. Se identificó que la literatura es robusta, al destacar trabajos que motivan al aprovechamiento de repositorios de redes semánticas; al incentivar el uso de las bases de datos de los centros especializados en detección y prevención del riesgo informático; al profundizar en el estudio de casos que se basan en el análisis reales en diversos sectores productivos; al proponer nuevos modelos y metodologías que integran los requerimientos de seguridad en las etapas de desarrollo de software y en el ciclo productivo de los sistema de información, entre otros trabajos.

- En los trabajos estudiados, también se identifica el interés por analizar los patrones de comportamiento de los gobiernos corporativos y la alta dirección frente a la gestión de la seguridad de la información; mediante la aplicación de instrumentos para recopilar datos que permitan diagnosticar, medir y evaluar la

participación de los órganos directivos. Adicional, se indaga sobre el conocimiento que posee los equipos de trabajo de desarrollo de software en materia de seguridad y la inclusión de los criterios en las etapas del ciclo de vida del desarrollo, manteamiento y soporte de las plataformas tecnológicas. Se halló investigaciones que se enfocan en estudios más específicos y especializados a partir de trabajos anteriores y experimentos en laboratorios.

- Para el desarrollo de la tesis se destacó, el artículo *"Information Security Management in academic institutes of Pakistan"*; producto de una investigación enfocada a diseñar un marco de referencia para implementar el sistema de gestión de seguridad de la información en las universidades de Pakistán. Por su enfoque directamente relacionado con la gestión de la seguridad en instituciones de educación superior, tuvo especial relevancia; aportando elementos conceptuales relacionados con buenas prácticas, políticas, procedimientos, tecnologías y recomendaciones sobre medidas adecuadas para proteger los activos de información.

- Desarrollar esquemas que apoyen la detección de los riesgos de seguridad, mitiga la posibilidad que las organizaciones, sean víctimas de ataques informáticos. Aportando a la estabilidad corporativa y al cumplimiento de sus objetivos de valor. Por ello es necesario que continuamente se trabaje en concientizar y culturizar a los funcionarios para convertir la gestión de la seguridad y prevención del riesgo, en una cultura institucional.

- Una metodología para auditar los criterios de seguridad a través del análisis del gobierno corporativo, los sistemas de información y el mantenimiento que reciben estas plataformas; permite identificar las amenazas y las vulnerabilidades que afectan a los activos y calcular el nivel de riesgo a partir de los hallazgos. Existen diversos mecanismos para realizar este proceso; lo importante es que los métodos utilizados determinen la situación de seguridad y el riesgo en que se encuentran los activos de información y que a partir del diagnóstico se intervengan de forma adecuada. La ventaja que ofrece la metodología propuesta, es el diseño de un esquema que estructura los elementos necesarios para auditar la seguridad de la información y emitir un concepto técnico basado en las entrevistas a los actores principales y la verificación de evidencias; a través de la aplicación de instrumentos de medición, la cuantificación y cualificación de los datos obtenidos.

- La metodología diseñada, se basó en extraer de la norma ISO 27000 los controles considerados relevantes en una auditoria de seguridad de la información; combinado con el aporte del marco de referencia COBIT 5, sobre prácticas previamente probadas y estandarizadas. En menor proporción, se incluyó conceptos de otros organismos internacionales, que al igual que ISO e ISACA, dedican esfuerzos y recursos al estudio del tema de forma rigurosa como

NITS y OWAPS. También se tuvo en cuenta las propuestas de auditorías que ha desarrollo diversos autores para medir y evaluar sistemas de gestión de seguridad de la información.

- En el desarrollo de la propuesta, se incluyó elementos como dimensiones, que hacen referencia a los escenarios corporativos a evaluar, criterios, enfocados al concepto a evaluar, controles, relacionados con las categorías de seguridad a auditar en cada escenario y componentes que se refiere al concepto explícito del cumplimiento o no, de un control. Todos elementos fueron considerados para dar origen la estructura de la metodología. Dentro del diseño de los instrumentos se incorporó mecanismos que permitieran probar cada hito propuesto en el diseño metodológico.

- El diseño de la metodología se desarrolló, pensado para que sea adaptativo, flexible, repetible e innovador; para que, en las diversas aplicaciones responsada a instituciones de educación superior de diferentes modelos, tamaños y condiciones; según los requerimientos particulares sujetos de evaluación. La estructura metodológica, permite que la aplicación se realice de forma completa o parcial; bien sea para evaluar todos los escenarios, criterios y controles; o cada uno de ellos de forma descentralizada, según la disponibilidad de recursos y necesidades de las instituciones. Al incluir conceptos de seguridad estándares, se podría consideran su aplicación en otros esquemas corporativos diferentes a los modelos universitarios, no obstante, sería necesario realizar pruebas que validen su aplicación y la obtención de resultados conforme a la situación de seguridad de la organización a evaluar.

- La metodología, aportar al cumplimiento de la legislación colombiana relacionada con seguridad de la información. Específicamente a la Ley 1581 de 2012. La Súper Intendencia de Industria y Comercio, estima que con la implementación de un sistema de gestión de la seguridad de la información bajo el estándar de la norma ISO 27000 y su familia; se cubre mínimo el 90% de los requisitos que exige la Ley de Protección de Datos Personales. Está regulación, rige para todos los sectores que por su naturaleza deben tratar datos personales. La metodología está ampliamente diseñada bajo el estándar de la ISO, por ende, si se hace la intervención e implementación de los planes de mejora con base en los hallazgos de la auditoria, se estará aportando al cumplimiento de las regulaciones y disposiciones de ley.

- El desarrollo de la tesis, cumplió con el objetivo principal y los objetivos específicos propuestos; al desarrollarse en su totalidad. El trabajo de investigación que se inició, tiene posibilidades de ser continuado, a través de otras líneas de investigación que sean parte del aseguramiento y calidad de los productos de software transaccionales.

10. FUTURAS LÍNEAS DE INVESTIGACIÓN

- Tomando como base el cumplimiento de los criterios de seguridad: disponibilidad, integridad, confidencialidad y autenticidad; es posible continuar con el desarrollo de una segunda versión, en donde el enfoque principal sea la evaluación de los criterios de seguridad de la información en el ciclo de desarrollo del software. Verificando que desde la etapa de requerimientos hasta la puesta en producción se haya contemplado la inclusión de la seguridad y prevención del riesgo informático.

- Desarrollar un nuevo diseño, en donde el enfoque no sea la audioria sino la implementación del sistema de gestión de seguridad de la información, en ambientes universitarios o corporativos de propósito empresarial.

- Con las dos líneas propuestas, se completaría el esquema, al evaluar la producción del software, los sistemas de información e implementar los planes de mejora para la corrección de los hallazgos.

11. BIBLIOGRAFÍA

ACIS. 2016. “Sistemas Fraude Informático:: Viejos Trucos, Nuevos Entornos.”

Ahmad, Atif, Sean B. Maynard, and Graeme Shanks. 2015. “A Case Analysis of Information Systems and Security Incident Responses.” *Int. J. Inf. Manag.* 35(6):717–23.

Alberts, Crhistopher; Dorefee, Audrey; Stevens, James; Woody Carol. 2003. “Introduction to the OCTAVE Approach.”

Alqahtani, Sultan S., Ellis E. Eghan, and Juergen Rilling. 2016. “Tracing Known Security Vulnerabilities in Software Repositories - A Semantic Web Enabled Modeling Approach.” *Science of Computer Programming* 121:153–75.

Analysis, Zrugv et al. n.d. “Risk Analysis in Security of Information ¡¢£¤¥¦§ ¨© ¢ £¤ ©.” 39–53.

Anon. n.d. “A Case-Based Management System for Secure Software.pdf.”

Anon. n.d. “A Novel Security Information and Event Management System for Enhancing Cyber Security in a Hydroelectri Dam.pdf.”

Anon. n.d. “Capturing Security Requirements for Software.pdf.”

Anon. n.d. “Current Practices and Challenges in Industrial Control.pdf.”

Anon. n.d. “Estimation of Deficiency Risk and Prioritization of Information Security Co.”

Anon. n.d. “Evaluation of the Patter-Based Method for Secure Development a Controlled Experiment.pdf.”

Anon. n.d. “Ministerio de Educación Nacional.” Retrieved (http://www.mineducacion.gov.co/1759/w3-article-235585.html).

Anon. n.d. “The Relationship between Internal Audit and Information Security.pdf.”

Baca, Dejan and Kai Petersen. 2013. “Countermeasure Graphs for Software Security Risk Assessment: An Action Research.” *J. Syst. Softw.* 86(9):2411–28.

Barton, Kevin Andrew. 2014. “Information System Security Commitment: A Study of External Influences on Senior Management.” 109.

Congreso de Colombia. 2012. “Ley Estatutaria 1581 de 2012 | Protección de Datos Personales.” 167.

Feng, Nan. 2014. “A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis.”

Information Sciences 256:57–73.

Glen, Cecilia Álvarez-correa. 2016. “C Onpes.”

Hamidovic, Haris, Independent Researcher, and Information Sec. 2015. “Fundamentos Del Gobierno de TI Basados En ISO/IEC 38500.” (November).

Herath, Hemantha S. B. and Tejaswini C. Herath. 2014. “IT Security Auditing: A Performance Evaluation Decision Model.” *Decision Support Systems* 57(1):54–63.

Isaca. 2013. *A Business Framework for the Governance and Management of Enterprise IT*.

ISACA. 2015. “State of Cybersecurity : Implications for 2015.” 22.

Iso, Referencia. 2011. “Norma Internacional Iso 19011.” 2011.

Knowles, William, Alistair Baron, and Tim McGarr. 2016. “The Simulated Security Assessment Ecosystem: Does Penetration Testing Need Standardisation?” *Computers & Security* 62:296–316.

Makori, Abanti Cyrus and Laban Oenga. n.d. “A Survey of Information Security Incident.” 19–31.

Manuel, Carlos, Fernández Sánchez, and Piattini Velthuis. 2012. *Modelo Para El Gobierno de Las TIC Basado En Las Normas ISO*.

McCallister, E., T. Grance, and K. Kent. 2010. “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).” *Recommendations of the National Institute of …* 1–59.

Ntc-iso-iec, Norma Técnica. 2013. “Norma Técnica Ntc-Iso-Iec Colombiana 27001 2013-12-11.” (571).

Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz, Mar. 2008. *Auditoría de Tecnologías Y Sistemas de Información, Ra – Ma Editorial*.

REDCLARA; TICAL. 2015. *Las Tecnologías de La Información Y La Comunicación Potenciado La Universidad Del Siglo XXI*.

Rehman, Huma, Ashraf Masood, and Ahmad Raza Cheema. 2013. “Information Security Management in Academic Institutes of Pakistan.” *2013 2nd National Conference on Information Assurance (NCIA)* 47–51.

Saint-Germain, R. 2005. “Information Security Management Best Practice Based on ISO/IEC 17799.” *Information Management Journal* 39(4):60–66.

Shamala, Palaniappan, Rabiah Ahmad, and Mariana Yusoff. 2013. “A Conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA).” *Journal of Information Security and Applications* 18(1):45–52.

Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2016. “Taxonomy of Information Security Risk Assessment (ISRA).” *Computers & Security* 57:14–30.

Shaw, R. S., Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. 2009. “The Impact of Information Richness on Information Security Awareness Training Effectiveness.” *Computers & Education* 52(1):92–100.

Soediono, Budi. 1989. “No Title No Title.” *Journal of Chemical Information and Modeling* 53(1991):160.

Software Engeneering Institute (SIE) at Carnegie Mellon University, OCTAVE. 2009. “The OCTAVE Approach to Information Security Risk Assessment.”

Sohrabi Safa, Nader, Rossouw Von Solms, and Steven Furnell. 2016. “Information Security Policy Compliance Model in Organizations.” *Computers and Security* 56:1–13.

Solic, Kresimir, Hrvoje Ocevcic, and Marin Golub. 2015. “The Information Systems’ Security Level Assessment Model Based on an Ontology and Evidential Reasoning Approach.” *Computers & Security* 55:100–112.

Store, Rahman I. S. O. 2013. “INTERNATIONAL STANDARD ISO / IEC Information Technology — Security Techniques — Code of Practice for Information Security Controls.” 2013.

Tøndel, Inger Anne, Maria B. Line, and Martin Gilje Jaatun. 2014. “Information Security Incident Management: Current Practice as Reported in the Literature.” *Computers & Security* 45(SEPTEMBER):42–57.

Webb, Jeb, Atif Ahmad, Sean B. Maynard, and Graeme Shanks. 2014. “A Situation Awareness Model for Information Security Risk Management.” *Computers & Security* 44(March 2016):1–15.

Yu, Yijun, Virginia N. L. Franqueira, Thein Than Tun, Roel J. Wieringa, and Bashar Nuseibeh. 2015. “Automated Analysis of Security Requirements through Risk-Based Argumentation.” *Journal of Systems and Software* 106:102–16.

ANEXO 1. CUESTIONARIO

Propósito: Recopilar información para evaluar la apropiación del gobierno universitario en la adopción y aplicación de prácticas adecuadas. Todas las preguntas están dirigidas a diagnosticar el grado de conocimiento e involucramiento. La aplicación del instrumento se realiza dentro del marco de desarrollo de la tesis de maestría: "DISEÑO DE UNA METODOLOGÍA PARA AUDITAR LA SEGURIDAD DE LA INFORMACIÓN EN PRODUCTOS DE SOFTWARE ORIENTADOS A SERVICIOS DE GESTIÓN E INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR". Propuesta de la estudiante Arelis Gómez Nova de la Universidad Autónoma de Bucaramanga, para optar al título de Magister en Gestión, Aplicación y Desarrollo de Software. La información que se obtenga será tratada bajo estricta confidencialidad y exclusivamente tendrá fines académicos.

El cuestionario está estructurado en ocho controles con los que se pretende cubrir los aspectos relevantes de la gestión del gobierno universitario para abordar la seguridad. Controles y preguntas están diseñados tomando referencia de las recomendaciones de buenas prácticas que propone la norma ISO 27001:27013 e ISACA en su marco de referencia COBIT 5, para realizar un programa de auditoria en seguridad de la información.

Indique su opinión en una escala del 1 al 4 (1 = no alcanzado, 2 = parcialmente alcanzado, 3 = ampliamente alcanzado, 4 = completamente alcanzado).

Cuestionario para verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión corporativa

Datos Generales del Entrevistado: Categoría cargo: Cargo: Fecha de aplicación:					
Controles		**Escala**			
		1	**2**	**3**	**4**
1.	**Legislación, principios, políticas y marcos de referencia**				
1.1.	¿Se reconoce la importancia de la información y se da tratamiento como un activo?				
1.2	¿Se define políticas de seguridad de la información?				
1.3	¿La política de seguridad de la información ha sido diseñada con base en los servicios que se prestan?				
1.4	¿La política de seguridad de la información ha sido elaborada con base en la norma: ISO27000, que rige en Colombia?				
1.5	¿La política de seguridad de la información ha sido elaborada con base en el lineamiento nacional de seguridad digital, que rige en Colombia?				
1.6	¿La política de seguridad de la información está diseñada para cumplir con el manejo de los datos personales que exige la Ley de Protección de Datos Personales, que rige en Colombia?				
1.7	¿La política de seguridad de la información está aprobada por el gobierno corporativo?				
1.8	¿La política de seguridad está publicada y disponible para toda comunidad?				
1.9	¿La política de seguridad de la información ha sido socializada y explicada a la comunidad?				
2.	**Estructura organizacional**				
2.1	¿Se cuantifica el valor de la información según su nivel de sensibilidad y criticidad en los procesos de negocio y servicios que se prestan?				
2.2	¿Se tiene definidos e implementados lineamientos y procedimientos para prevenir y detectar las vulnerabilidades de seguridad en la gestión de los datos corporativos?				
2.3	¿Las responsabilidades y procedimientos de protección de activos de información están definidos e implementados?				

Continuación

Controles		Escala			
		1	2	3	4
2.4	¿Los contratos de los empleados incluyen cláusulas de confidencialidad que han sido dadas a conocer y aceptadas con la firma del documento?				
2.5	¿Los proveedores y contratista que intervienen en los sistemas, conocen las directrices de seguridad de la información con anterioridad a la formalización de contratos y las aceptan con pólizas de respaldo?				
2.6	¿Los empleados conocen el procedimiento de reporte de incidentes?				
2.7	¿Existen canales formales para reportar los incidentes de seguridad?				
2.8	¿Se desarrollan y mantienen planes de continuidad del negocio que incluyen la gestión de recuperación ante desastres?				
3	**Disponibilidad de recursos**				
3.1	¿Se provisiona, presupuesta y ejecuta recursos económicos para gestión de la seguridad de la información?				
3.2	¿El inventario de herramientas para gestionar la seguridad de la información está debidamente inventariado, documentado y controlado?				
3.3	**¿**En los planes de gestión se incorpora y actualiza regularmente tecnología para gestionar la seguridad de la información y los riesgos?				
4.	**Procesos**				
4.1	¿La gestión de la seguridad de la información está integrada a los procesos de valor?				
4.2	¿Los procesos de seguridad de la información están definidos, implementados y documentados?				
4.3	¿Los empleados ha sido informados y formado en los procesos asociados la de seguridad de la información?				
4.4	¿Los procesos de seguridad de la información están disponibles para consulta de los grupos de interés?				
5.	**Cultura, ética y comportamiento**				
5.1	¿Se ha diseñado e implementado un programa activo de culturización, formación y capacitación en seguridad de la información?				
5.2	¿A los empleados se les capacita en seguridad de la información, la política, los lineamientos y los procedimientos?				

Continuación

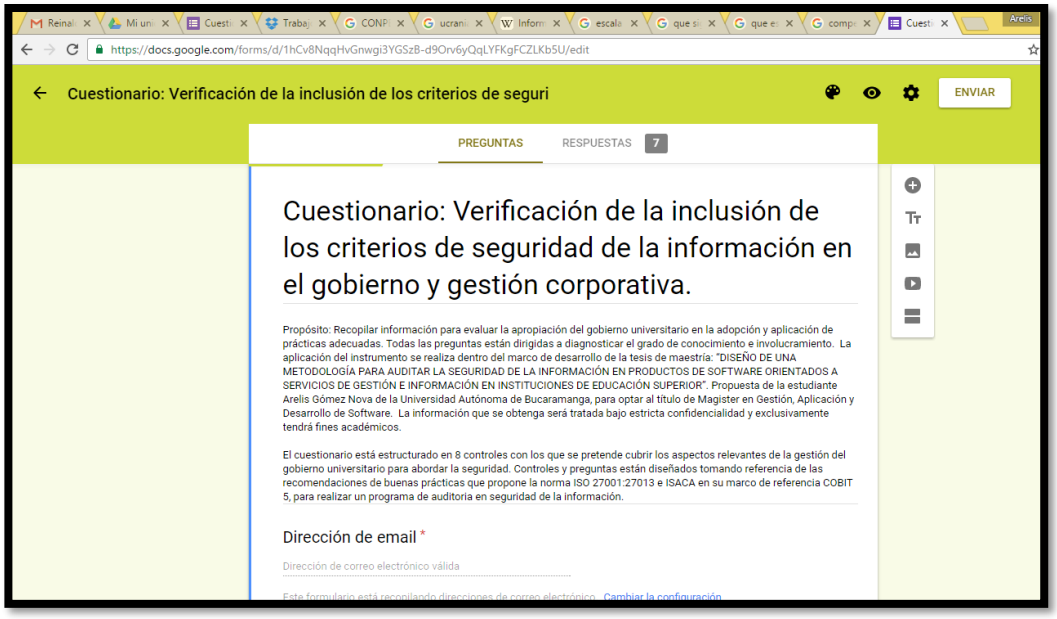
Controles		Escala			
		1	2	3	4
5.3	¿Los usuarios reciben información y formación enfocada a concientizar sobre la necesidad de acoger las directrices de seguridad de la información?				
5.4	¿Los proveedores y contratista que intervienen en los sistemas de información conocen de la política, los lineamientos y procedimientos de seguridad de la información y la acatan?				
5.5	¿la comunidad en general recibe información y capacitación en seguridad de la información y la relación que tiene con los procesos de negocio?				
6.	**Personas, habilidades y competencias**				
6.1	¿Se han definido e implementado perfiles y roles para la selección y contratación de personal con formación en seguridad de la información?				
6.2	¿Los empleados dedicados a la administración, mantenimiento y soporte técnico de los sistemas de información e infraestructura tecnológica, poseen formación y competencias en seguridad de la información?				
6.3	¿Los usuarios de los sistemas de información han sido capacitados en seguridad de la información?				
6.4	¿Los usuarios de los sistemas de información han sido capacitados y conocen de los riesgos asociados a cada sistema de información?				
6.5	¿La formación y capacitación se extiende a proveedores de servicios en sistemas de información?				
7.	**Perfil de aceptación del riesgo**				
7.1	¿Se tiene implementado un sistema de evaluación del riesgo de seguridad en concordancia con los procesos de negocio y los criterios de aceptación?				
7.2	¿Se toman las medidas necesarias para identificar, prevenir e intervenir los riesgos que están fuera de los criterios aceptados?				
7.3	¿La identificación y evaluación del riesgo está bajo de la responsabilidad de un grupo interdisciplinario?				
7.4	¿Se ha diseñado el procedimiento requerido para el reporte de incidentes de seguridad?				
7.5	¿Se ha formado a la comunidad en los procedimientos y el protocolo de reporte de incidentes de seguridad?				
7.6	¿Se ha definido e implementado procedimientos para el reporte de incidentes de seguridad de la información?				

Continuación

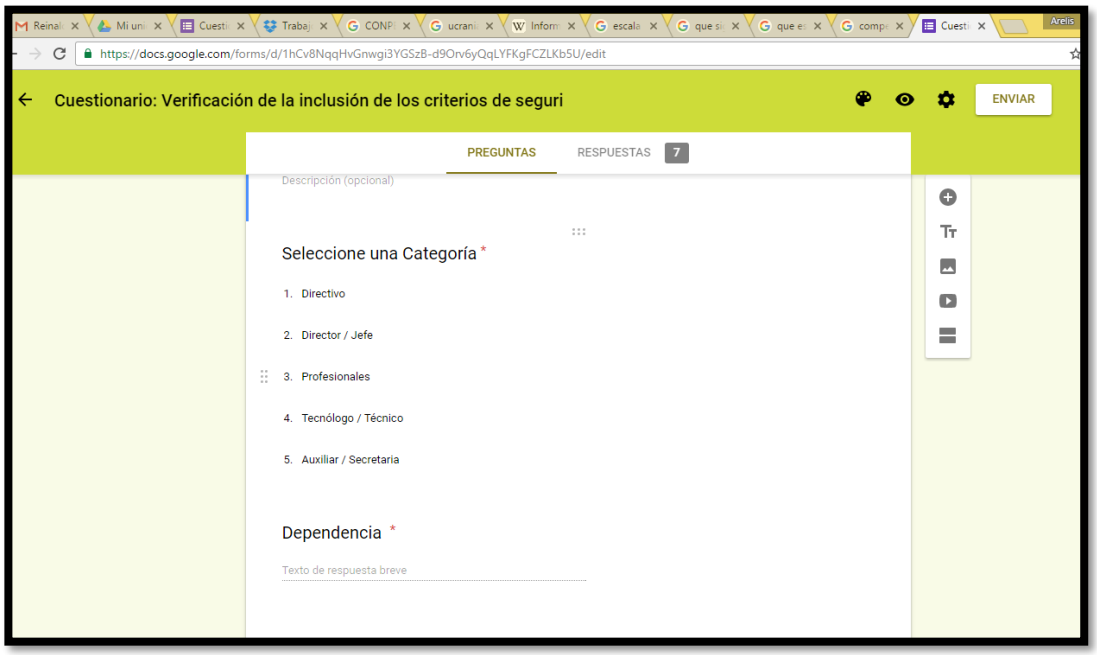
Controles		Escala			
		1	2	3	4
7.7	¿Se ha diseñado e implementado procedimientos para la valoración de las brechas de seguridad de la información, según la sensibilidad y criticidad de la información en los procesos de negocio?				
7.8	¿Los planes de continuidad han sido probados y permiten mantener las operaciones posterior a la ocurrencia de incidentes de seguridad?				
8.	**Arquitectura de seguridad de la información**				
8.1	¿Se ha definido e implementado un proceso sistemático para detectar vulnerabilidades y amenazas de seguridad en los ambientes en donde funcionan sistemas de información?				
8.2	¿Los planes de continuidad del negocio son probados, verificados y actualizados periódicamente?				
8.3	¿El mantenimiento y soporte técnico del software se realiza a través de un procedimiento definido, implementado y documentado?				
8.4	¿El mantenimiento y soporte técnico de los sistemas de información, es desarrollado por personal experto y capacitado?				
8.5	¿El flujo de datos en las redes física e inalámbrica es transportado a través de procesos de cifrados?				
8.6	¿Los sistemas de información funcionan con el esquema de matriz de roles y perfiles, según los procedimientos de negocio y las responsabilidades de cargo de los usuarios?				
8.7	¿Se tiene definido e implementado un procedimiento periódico de aplicación de pruebas de penetración en los sistemas de información?				

ANEXO 2. CUESTIONARIO PARA APLICACIÓN

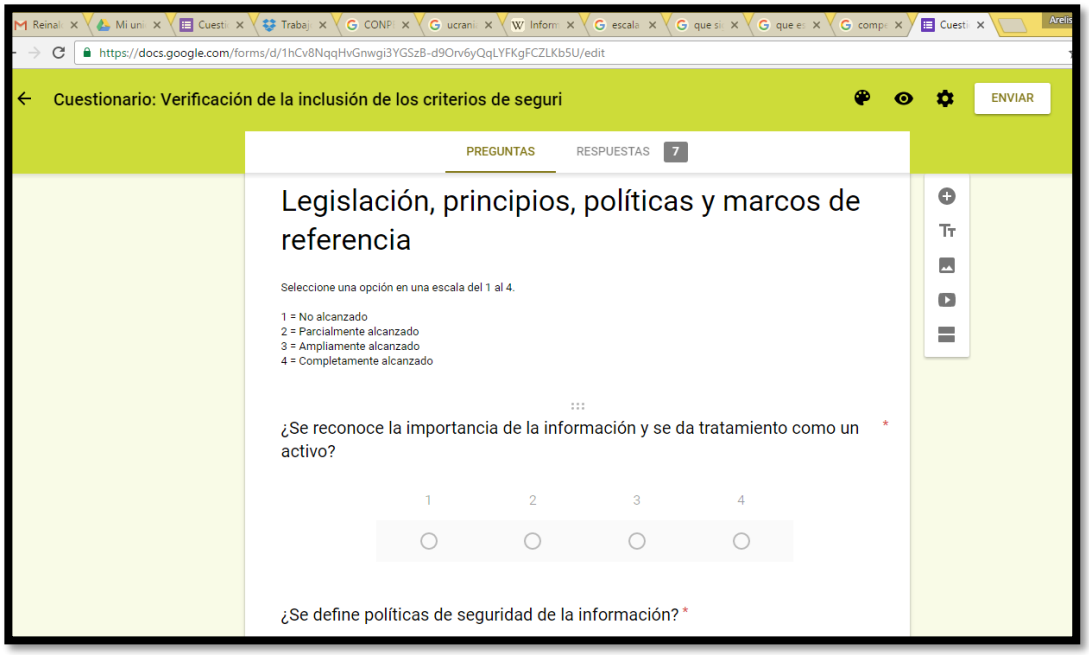
- **Sección 1 de 10**



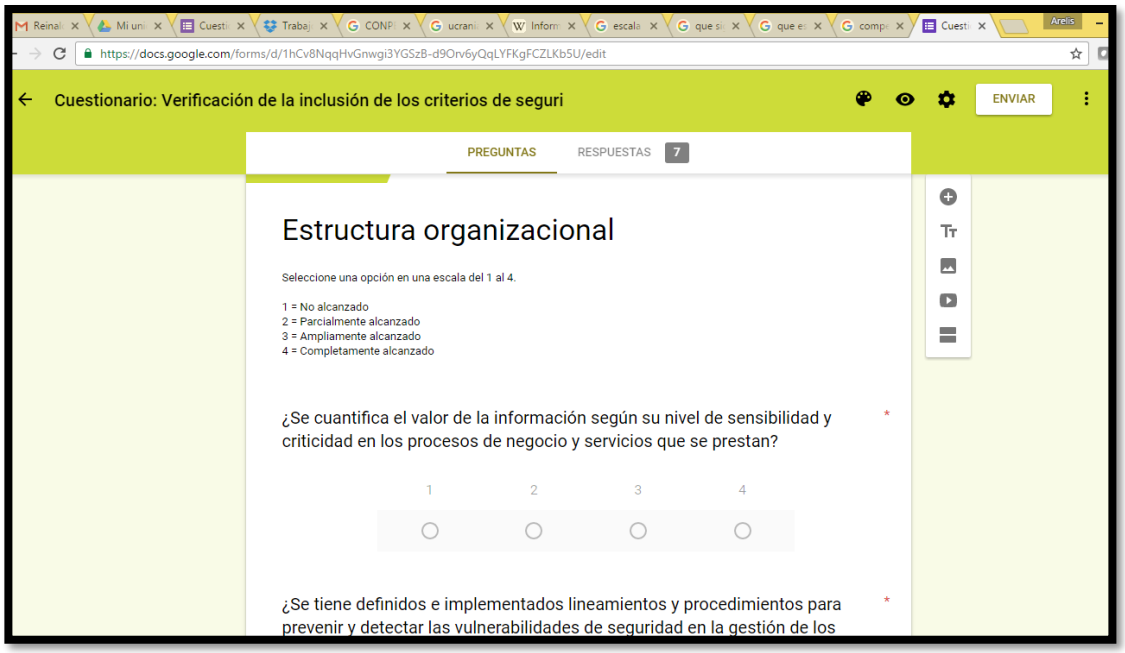
- **Sección 2 de 10**



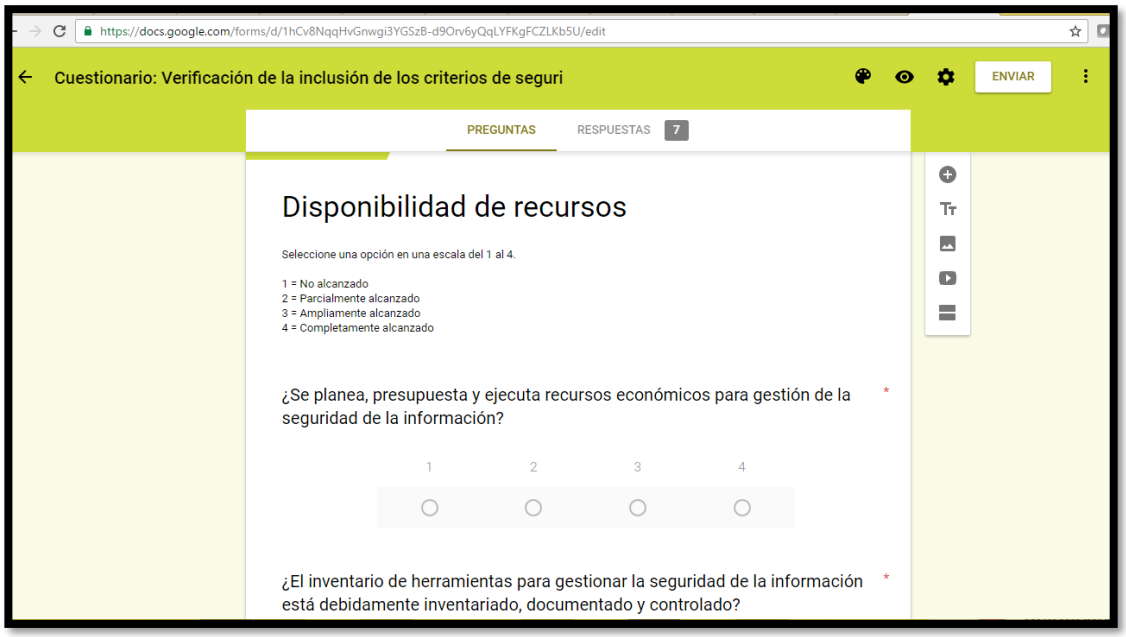
- **Sección 3 de 10**



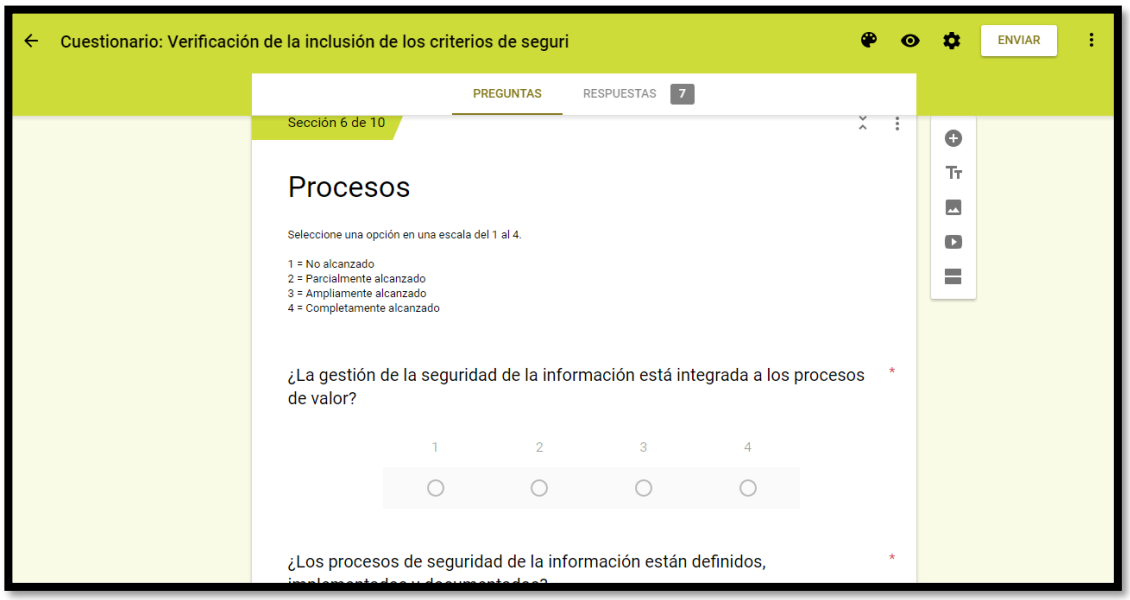
- **Sección 4 de 10**



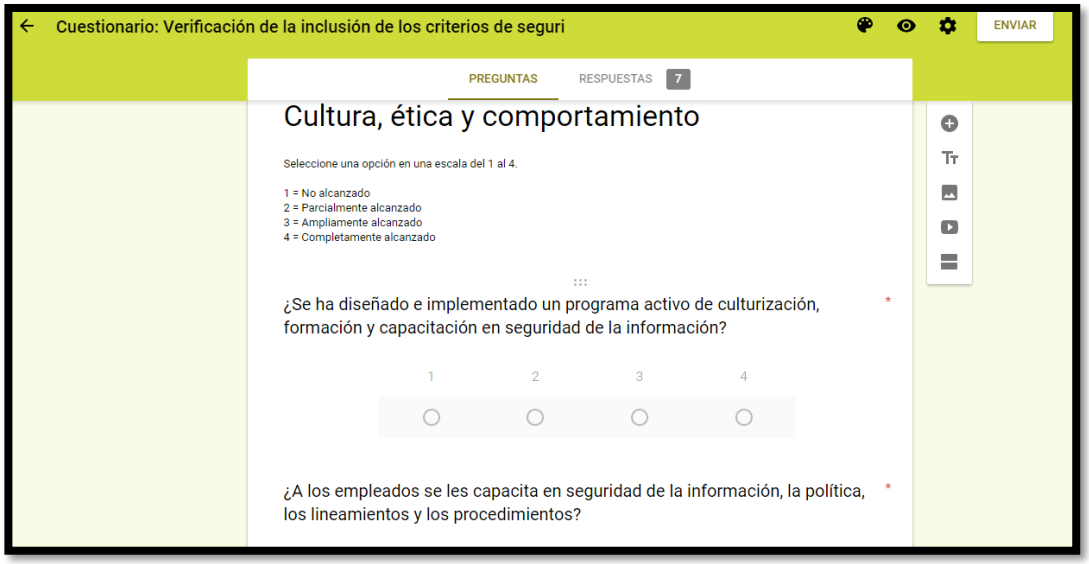
- **Sección 5 de 10**



- **Sección 6 de 10**



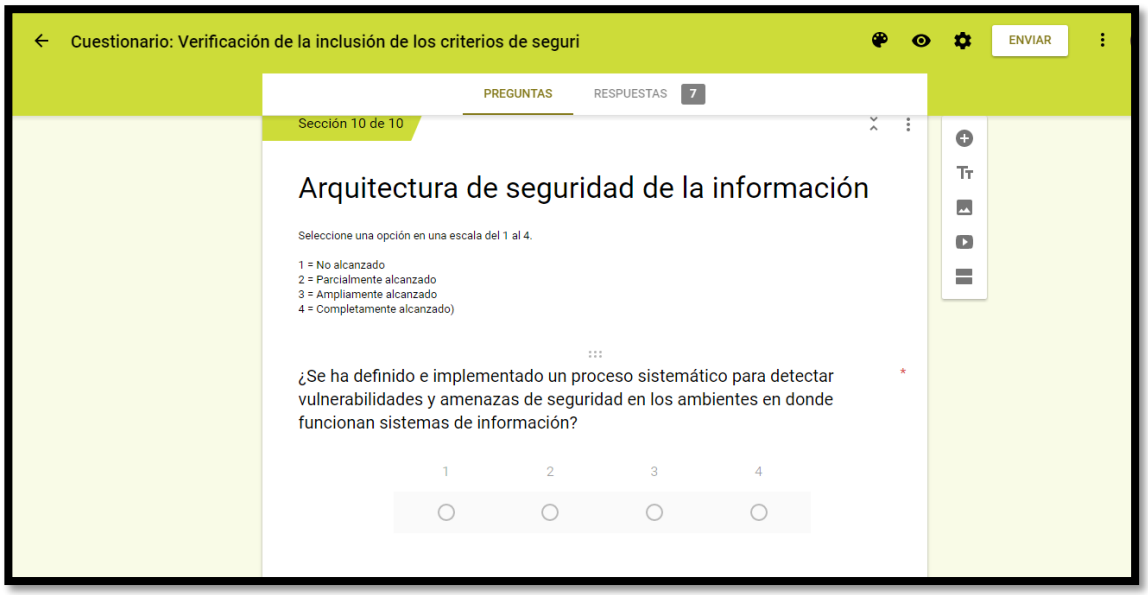
- **Sección 7 de 10**



- **Sección 8 de 10**

- **Sección 9 de 10**

- **Sección 10 de 10**



ANEXO 3. INSTRUMENTO DE EVALUACIÓN II

- **Control 1**

Matriz de Análisis de Riesgo		Probabilidad de Amenaza [1 = Insignificante, 2= Baja, 3 = Mediana, 4=Alta]															
Plataforma Tecnologíca	Magnitud de Daño 1 = Bajo 2 = Medio 3 = Alto 4 = Crítico	C.1 Manejo de Errores y de eventos de registro															
		La organización debe establecer, documentar e implementar políticas de manejo de errores y eventos de registro que respondan a la funcionalidad de las aplicaciones y a la seguridad de la información.	Los mensajes de error no deben revelar detalles acerca del estado interno de la aplicación, ni de las rutas del sistema de archivo. La información de la pila no debe estar expuestas al usuario a través de mensajes de error.	Los manejadores de errores deben estar configurados para detectar errores inesperados y entregar una salida controlada y transparente para el usuario final.	Todo intento de autenticación, exitosa o no, debe generar un log histórico para seguimiento y auditoría.	Toda modificación de privilegios debe quedar registrada, según la novedad realizada.	Toda gestión técnica debe ser controlada para seguimiento y control.	Los registros deben ser mantenidos y almacenados para prevenir perdida de información o manipulación por parte de intrusos.	Las retenciones de los registros deben estar guiados por un lineamiento definido para cumplir con los requerimientos legales y proveer suficiente información para actividades forenses y de respuesta a incidentes	Se debe definir e implementar un protocolo de seguimiento a fechas, horas y detalles de los eventos claves como entradas y salidas de los sistemas de información.	Toda la actividad de acceso de archivos a los sistemas de información deben estar monitoreada y con registros de log de la actividad realizada, sin excepción alguna.	Los mensajes clasificados como confidenciales deben estar cifrados antes de ser registrados, para proteger su integridad.	Todos los sistemas deben tener implementados mecanismos de alarmas accionadas desde el sistema de control de accesos.	La activación y desactivación de los sistemas de protección (antivirus, detección de intrusos) debe ser aprobada por estancias superiores al administrador.	El control de registros de log, debe estar por fuera del alcance del administrador del sistemas, debe hacer una estancia de seguimiento y auditoria que se encargue de su gestión.	Debe haber un seguimiento y control al almacenamiento. Debe preverse capacidad de almacenamiento adecuadas.	El ajuste y sincronización de los relojes deben corresponder con el procesamiento real de la información en los sistemas, todos los sistemas deben ser sincronizados con una única fuente de tiempo.
		4	2	4	1	4	4	3	4	3	3	4	3	4	4	3	1
S1. Sistema de Información para la Gestión Académica	4	16	8	16	4	16	16	12	16	12	12	16	12	16	16	12	4
S2. Biblioteca	2	8	4	8	2	8	8	6	8	6	6	8	6	8	8	6	2
S3. Sistema de Pagos en Línea	4	16	8	16	4	16	16	12	16	12	12	16	12	16	16	12	4
S4. Publicación de Horarios	2	8	4	8	2	8	8	6	8	6	6	8	6	8	8	6	2
S5. Sistema de Gestión Financiera	4	16	8	16	4	16	16	12	16	12	12	16	12	16	16	12	4
S6. Audiovisuales	1	4	2	4	1	4	4	3	4	3	3	4	3	4	4	3	1
S7. Práticas Empresariales	1	4	2	4	1	4	4	3	4	3	3	4	3	4	4	3	1

- **Control 2**

C2. Tratamiento de usuarios y contraseñas de acceso												
La organización debe establecer, documentar e implementar una política de tratamiento de usuarios y control de acceso que responda a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	El cifrado de las entradas y salidas de las contraseñas debe realizarse de forma criptográfica a través de funciones hash, que aseguren la confidencialidad de las contraseñas acceso a las aplicaciones.	La gestión y control de las novedades de usuarios (creación, modificación, eliminación), debe realizarse bajo un procedimiento establecido y quedar documentado según la acción realizada.	El control de actualización periódica de contraseñas para inicio de sesión, debe registrarse en una bitácora para su seguimiento y documentación.	La organización debe implementar un procedimiento para registrar la gestión de bloqueo y desbloqueo de usuarios por parte del administrador del sistema de información.	Las actividades de bloqueo y desbloqueo de usuarios, debe registrarse en una bitácora de seguimiento y documentación.	Debe existir una relación de la matriz de roles de usuario y los grupos de usuarios creados en el sistema.	Secure Sockets Layer (SSL), es un protocolo para permitir que las aplicaciones trasfieran información, debería ser utilizado para los sistemas de información de forma compleja.	Las contraseñas de los usuarios deben almacenarse utilizando técnicas de hash con un algoritmo fuerte como SHA-2.	Las llaves de cifrado intercambiadas o pre-configuradas deben transportarse por un canal seguro.	Las llaves almacenadas en el sistema de información, deben ser apropiadamente aseguradas y solo accesibles al personal adecuado cuando sea necesario.	Los sistemas de información debe ser certificados a través de firmas emitidas por entidades de confianza.	Comprobación de usuarios desarrolladores con usuario y contraseña para hacer modificaciones en ambientes de producción.
4	4	3	4	3	3	4	3	4	4	3	4	3
16	16	12	16	12	12	16	12	16	16	12	16	12
8	8	6	8	6	6	8	6	8	8	6	8	6
16	16	12	16	12	12	16	12	16	16	12	16	12
8	8	6	8	6	6	8	6	8	8	6	8	6
16	16	12	16	12	12	16	12	16	16	12	16	12
4	4	3	4	3	3	4	3	4	4	3	4	3
4	4	3	4	3	3	4	3	4	4	3	4	3

- **Control 3**

c3. Políticas y técnicas de autenticación								
La organización debe establecer, documentar e implementar políticas y técnicas de autenticación que respondan a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	La asignación de información para autenticación debe ser controlada por medio de un proceso de gestión formal.	Se debe establecer un periodo máximo de validez de las contraseñas sin utilización permanente.	El número de entradas deben estar controlados en el historial de contraseñas.	Debe existir un procedimiento definido para la expiración de las contraseñas.	Debe existir un lineamiento que defina la robustez de longitud mínima de la contraseña.	El sistema debe comprobar la contraseña durante el inicio de sesión contra políticas actuales.	Debe existir un lineamiento de número de intentos fallidos de inicio de sesión antes que el sistema se bloquee.	Debe existir un lineamiento de número mínimo de caracteres que tiene que ser diferente con relación a la contraseña anterior.
4	4	4	3	4	4	4	2	4
16	16	16	12	16	16	16	8	16
8	8	8	6	8	8	8	4	8
16	16	16	12	16	16	16	8	16
8	8	8	6	8	8	8	4	8
16	16	16	12	16	16	16	8	16
4	4	4	3	4	4	4	2	4
4	4	4	3	4	4	4	2	4

- **Control 4**

C4.Transporte de Datos				
La organización debe establecer, documentar e implementar para el transporte de datos un procedimiento que responda a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	Las aplicaciones deben tener implementado mecanismos de comprobación de todas las entradas y salidas de datos viajan a través de protocolo HTTPS.	Las aplicaciones deben tener implementado mecanismos de comprobación que todas las entradas y salidas de datos se realizan por una sola conexión host.	Debe haber definido un procedimiento de comprobación que mensajes extensos que viajan a través del protocolo HTTPS se deshabilitan	Debe haber definido un procedimiento de seguimiento de transporte de datos seguros a través del protocolo SSL.
4	3	3	4	3
16	12	12	16	12
8	6	6	8	6
16	12	12	16	12
8	6	6	8	6
16	12	12	16	12
4	3	3	4	3
4	3	3	4	3

- **Control 5**

C.5 Administración de sesiones de trabajo							
La organización debe establecer, documentar e implementar políticas de administración de sesiones de trabajo, que respondan a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	Las claves de sesión deben ser generados por funciones aleatorias seguras y extensas de forma que resistan el análisis y la predicción.	Las claves de sesión debe ser regeneradas cuando el usuario se autentica en la aplicación y cuando los niveles de privilegios del usuario cambian.	Los tokens de sesión deben regenerasen cuando el estado de cifrado cambia.	La aplicación debe tener configurado la finalización de sesión cuando un usuario permanece inactivo en un lapso de tiempo mayor a 5 minutos.	Los usuarios de sesión deben finalizarse definitivamente en un período de inactividad igual o mayor a 2 horas para mitigar el riesgo de que un ataque de secuestro de sesión.	Las sesiones múltiples y en simultanea para un único usuario deben ser controladas y monitoreadas permanentemente, además de justificadas a través de una autorización del dueño de proceso.	Las aplicaciones deben tener implementado mecanismos de detección de intentos de clonación de la sesión, cancelando la sesión y forzando a una nueva entrada.
4	3	4	4	3	3	3	3
16	12	16	16	12	12	12	12
8	6	8	8	6	6	6	6
16	12	16	16	12	12	12	12
8	6	8	8	6	6	6	6
16	12	16	16	12	12	12	12
4	3	4	4	3	3	3	3
4	3	4	4	3	3	3	3

- **Control 6**

C6. Gestión de cambios								
La organización debe establecer, documentar e implementar políticas de control de cambios en los sistemas de información que respondan a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	Para todo cambio debe realizar las pruebas necesarias en ambientes de preproducción y ser aprobadas por las estancias que corresponden y los usuarios de los sistemas antes de pasar al ambientes productivos.	Se debe tener un proceso documentado para identificación, planificación y registro de todo cambio.	Las pruebas de los cambios deben tener un plan de ejecución en donde se documente cada cambio y el resultado obtenido.	Todo cambio debe tener una evaluación de impacto potencial, incluidos los impactos de seguridad de la información en el sistema de información y en la organización.	Todo cambio debe ser aprobado por una estancia superior al administrador de cambios y debe estar registrada en un acta formal de gestión de cambios.	Los cambios deben ser comunicación formalmente a todas las estancias y personas pertinentes.	Debe existir un procedimiento de apoyo para abordar cambios no éxitos y controlar los cambios en caso de ser necesario el regreso a la versión o estado anterior.	Finalizado el cambio, debe quedar un documento formal que contienen todo lo pertinente y referente al cambio realizado.
4	3	3	3	4	2	2	3	4
16	12	12	12	16	8	8	12	16
8	6	6	6	8	4	4	6	8
16	12	12	12	16	8	8	12	16
8	6	6	6	8	4	4	6	8
16	12	12	12	16	8	8	12	16
4	3	3	3	4	2	2	3	4
4	3	3	3	4	2	2	3	4

- **Control 7**

C7. Gestión de la capacidad				
La organización debe establecer, documentar e implementar políticas de seguimiento de recursos, para asegurar el desempeño óptimo en los sistemas de información que se encuentran en producción.	Se debe tener un lineamiento y procedimiento de evaluación de sistemas de información para determinar su capacidad productiva, con base las actualizaciones de los procesos de negocio, los cambios organizacionales y requerimientos de información que exige el contexto.	El cierre definitivo de aplicaciones, sistemas de información, bases de datos que están en ambientes de producción, deben asegurar que se aplicó medidas y procedimientos para el tratamiento correcto de la seguridad de la información.	El plan de gestión de capacidad, debe considerar la capacidad y destinación de recursos para sistemas de información de misión crítica, disponiendo recursos suficientes y con medidas de seguridad calificadas.	Dentro de la gestión de la capacidad se debe considerar talento humano que gestiones de los sistemas de información y la seguridad de los mismo eficientemente.
4	3	4	3	4
16	12	16	12	16
8	6	8	6	8
16	12	16	12	16
8	6	8	6	8
16	12	16	12	16
4	3	4	3	4
4	3	4	3	4

- **Control 8**

C8. Segregación de los ambientes de desarrollo. Pruebas, proproducción y producción									
La organización debe establecer, documentar e implementar políticas de segregación de ambientes para reducir los riesgos de acceso no autorizados a los ambientes pre productivos y productivos.	Los ambientes de gestión de los sistemas de producción deben estar separados en ambientes de desarrollo, pruebas, preproducción y producción.	Cada ambiente de gestión de los sistemas de información tener especificado y documento el nivel de separación entre un ambiente y otro.	Se deben definir y documentar los lineamientos para la trasferencia de software de un ambiente a otro.	Cada ambiente de producción debe operar en diferentes esquemas de infraestructura tecnológica.	Se debe definir el procedimiento y los niveles de aprobación para las circunstancias excepcionales, en donde el cambio se debe ejecutar en un ambiente de producción.	Los compiladores, editores, demás herramienta de desarrollo deben tener restricción de acceso desde los ambientes de pruebas, producción y preproducción.	Los usuarios utilizados para los ambientes de prueba y preproducción, deben tener perfiles diferentes a los de los ambientes de producción y tener mensajes de alerta que reduzcan el riesgo de error.	Los datos con denominación sensible se les debe aplicar proceso técnico después de un procedimiento de clonación para reducir el riesgo de fuga de información de misión crítica.	Se debe tener establecido las cláusulas de confidencialidad para el personal que accede a los ambientes de desarrollo, pruebas, preproducción y producción.
3	2	3	4	2	4	4	4	4	3
12	8	12	16	8	16	16	16	16	12
6	4	6	8	4	8	8	8	8	6
12	8	12	16	8	16	16	16	16	12
6	4	6	8	4	8	8	8	8	6
12	8	12	16	8	16	16	16	16	12
3	2	3	4	2	4	4	4	4	3
3	2	3	4	2	4	4	4	4	3

- **Control 9**

c0. Protección contra código malicioso								
La organización debe establecer, documentar e implementar políticas de protección contra código malicioso para reducir los riesgos de acceso no autorizados a los ambientes pre productivos y productivos.	Se deben implementar controles y procedimientos de detección, prevención y recuperación para protección contra código malicioso.	Se debe definir e implementar lineamientos que prohíba el uso de sitios web maliciosos, que se sospecha que son maliciosos software o están incluidos en listas negras	Se debe definir e implementar lineamientos y procedimientos para proteger contra riesgos asociados a la detección de archivos y software, mediante redes externas o cualquier otro medido.	Se debe definir los lineamientos, procedimientos y periodos para revisiones de regulares del software y del contenido datos del sistema de información, que apoyan los procesos críticos y no críticos del negocio.	Todo dato del sistema de información y hardware debe ser escaneado con herramientas tecnológicas de detección y reparación de software malicioso de forma rutinaria.	Se debe tener procedimientos y ambientes de aislamiento para el análisis de ataques con software malicioso.	La organización debe tener preparado un plan de continuidad de negocio apropiado para la recuperación de operación ante ataques de software malicioso, que incluya el 100% de la información, copias de respaldo y las disposiciones que posibiliten el accionar del plan de forma inmediata.	La organización debe conocer y estar en contacto con fuentes de información que emitan advertencias calificadas
4	2	3	4	3	4	3	3	2
16	8	12	16	12	16	12	12	8
8	4	6	8	6	8	6	6	4
16	8	12	16	12	16	12	12	8
8	4	6	8	6	8	6	6	4
16	8	12	16	12	16	12	12	8
4	2	3	4	3	4	3	3	2
4	2	3	4	3	4	3	3	2

- **Control 10**

C10. Controles criptográficos						
La organización debe establecer, documentar e implementar políticas para para el uso de controles criptográficos para toda la organización, bajo el principio que es necesario proteger la información.	Se debe establecida y definida la valoración de riesgos que identifique el nivel de protección requerida que incluya tipo, fortaleza y calidad del algoritmo de cifrado requerido.	Se debe valorar el impacto que genera la utilización de información cifrada y la inspección que realiza a los procesos de negocio.	se debe definir y establecer un lineamiento y procedimiento para el uso de cifrado para la protección de información transportada por dispositivos móviles, removibles y líneas de comunicación.	Se debe definir y establecer un lineamiento y procedimiento para la gestión de llaves, que incluya métodos para la protección de llaves criptográficas y la recuperación de información cifrada.	Se debe definirse los roles y las responsabilidades para la gestión y generación de llaves, también procedimiento y la documentación a generar.	Las llaves generadas deben ser establecidas a través de una política de llaves para asegurar una implementación efectiva, asegurando que son una solución para los procesos de negocio.
4	4	4	4	4	4	4
16	16	16	16	16	16	16
8	8	8	8	8	8	8
16	16	16	16	16	16	16
8	8	8	8	8	8	8
16	16	16	16	16	16	16
4	4	4	4	4	4	4
4	4	4	4	4	4	4

- **Control 11**

C11. Gestión de las vulnerabilidades técnicas										
La organización debe establecer, documentar e implementar políticas de gestión de las vulnerabilidades técnicas para asegurar el desempeño óptimo en los sistemas de información que se encuentran en producción.	Se debe definir e implementar el lineamiento y procedimiento para la prevención, detección e intervención de las vulnerabilidades técnicas en los sistemas de información.	Se debe definir e implementar los roles y responsabilidades asociados a las vulnerabilidades técnicas, incluyendo los mecanismos de seguimiento y valoración del riesgo.	Se debe evaluar permanentemente la exposición de la organización a vulnerabilidades y tomar las acciones apropiadas para el tratamiento del riesgo asociado.	La organización proporcionar los recursos para identificar las vulnerabilidades técnicas, incluyendo herramientas para seguimiento, valoración, control y gestión del riesgo.	Los recursos de gestión de vulnerabilidades técnicas deben actualizarse, según la incorporación de nuevos sistemas de información y la actualización de los existentes.	Se debe establecer una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas y valoración del impacto potencial que tiene sobre los sistemas de información y la organización.	Debe existir un procedimiento para intervenir la vulnerabilidad, una vez esta haya sido identificada y valorada, determinando las acciones de acción correctiva y de mejora necesaria.	La detección de vulnerabilidades debe llevar a una revisión y valoración de los controles definidos para la detección y prevención de vulnerabilidades.	Ante la necesidad de aplicar parches, estos deben ser probados y evaluados en ambientes de prueba y preproducción antes de su implementación en ambientes productivos.	Se debe definir el sistema de seguimientos y evaluación regular del proceso de gestión de vulnerabilidades técnicas, para asegurar prevención eficacia y eficiencia en los sistemas de información.
4	4	4	4	4	4	4	4	4	2	4
16	16	16	16	16	16	16	16	16	8	16
8	8	8	8	8	8	8	8	8	4	8
16	16	16	16	16	16	16	16	16	8	16
8	8	8	8	8	8	8	8	8	4	8
16	16	16	16	16	16	16	16	16	8	16
4	4	4	4	4	4	4	4	4	2	4
4	4	4	4	4	4	4	4	4	2	4

- **Control 12**

C12. Gestión de técnicas anti robo de información					
Los sistemas operativos y sistemas de información se deben mantener el sistema operativo, el navegador y el antivirus con las últimas actualizaciones de seguridad	Los sistemas operativos y sistemas de información se deben tener implementados mecanismos que impidan la gestión de datos desde equipos desconocidos o no autorizados.	Los mecanismos de generación de contraseñas deben tener implementados algoritmos que impidan la creación de claves débiles en los sistemas de información.	Se deben tener implementados soluciones de seguridad antimalware con sistemas de detección proactiva que ayuden a prevenir la proliferación de códigos maliciosos que puedan afectar los activos de la organización.	Se deben tener implementados soluciones de seguridad para detección de phishing que ayuden a prevenir la proliferación de códigos maliciosos que puedan afectar los activos de la organización.	Se debe utilizar mecanismos de generación de imágenes CAPTCHA para prevenir que la autenticación no sea débil.
3	4	4	3	4	2
12	16	16	12	16	8
6	8	8	6	8	4
12	16	16	12	16	8
6	8	8	6	8	4
12	16	16	12	16	8
3	4	4	3	4	2
3	4	4	3	4	2

ANEXO 4. INSTRUMENTO DE EVALUACIÓN II

- **Control 1**

Matriz de Análisis de Riesgo		Probabilidad de Amenaza [1 = Insignificante, 2= Baja, 3 = Media
Servicio	Magnitud de Daño 1 = Bajo 2 = Medio 3 = Alto 4 = Crítico	C1. Gestión de Activos
		La organización debe tener definida la política de gestión de activos de información, de acuerdo con los procesos de negocio y los servicios que presta; asegurando el tratamiento de la seguridad de la información
		2
Gestión de activos de información	3	6
Gestión de proveedores	3	6
Gestión de la infraestructura y comunicaciones tecnológicas	4	8
Gestión de planes de continuidad	3	6
Gestión de copias de respaldo	4	8

La organización debe tener identificados todos sus activos de información, los procedimientos de instalación e inventario con su respectivo control de versiones y actualizaciones.	El inventario de activos de información debe ser exacto, actualizado, consistente y estar alineados con otros sistemas de información.	La organización debe identificar, documentar e implementar reglas para el uso aceptable de los activos de información.	La organización debe implementar lineamientos y procedimientos para la devolución de activos de información que los empleados y terceros tienen a su cargo ante el reporte de novedades de finalización de contratos, traslados internos, licencias, etc.	La organización debe implementar mecanismos de control y prevención para los empleados y/o contratistas que han sido reportados con novedades, durante el periodo de cumplimiento de la
3	3	3	3	4
9	9	9	9	12
9	9	9	9	12
12	12	12	12	16
9	9	9	9	12
12	12	12	12	16

- **Control 2**

ana, 4=Alta]				
C2. Clasificación de la información				
La información se debe clasificar, según su función, los requisitos legales, la valoración crítica, la susceptibilidad de divulgación o modificación; previniendo accesos no autorizados.	Los lineamientos, procedimientos e implementación de mecanismos de control en la clasificación de la información deben ser coherente la legislación, los procesos de negocio, las necesidades de intercambio y a las restricciones de divulgación de la información.	El esquema de clasificación de la información debe estar diseñado bajo el principio que su divulgación no debe causar daños, ni afectar el buen nombre de la organización, de quienes la conforman o de terceros, ni causar impacto negativo.	En el esquema de clasificación la clasificación de la información debe tener una codificación y descripción coherente con el contexto de su aplicación.	La gestión de clasificación de la información debe proporcionar el valor de los activos de información para la organización, dependiendo de su sensibilidad y criticidad.
2	3	2	3	4
6	9	6	9	12
6	9	6	9	12
8	12	8	12	16
6	9	6	9	12
8	12	8	12	16

- **Control 3**

C3. Gestión de la prestación de servicios de proveedores								
La prestación de servicios de proveedores debe estar regulada por la organización a través de una política, lineamientos y procedimientos que delimiten las intervenciones dentro de la operación.	Deben existir mecanismo de seguimiento y control a proveedores que aseguren el cumplimiento de los términos y condiciones de los acuerdos y responsabilidades que están obligados asumir durante sus intervenciones,	Debe existir personal interno responsable de hacer seguimiento y control a los proveedores, junto con la revisión de reportes entregados sobre las actividades ejecutadas.	Los accesos a los sistemas de información y a la información de la organización debe ser mediante la firma de acuerdo de confidencialidad y preservación de la información.	La organización debe tener registro de todos los accesos que se le otorgan a un proveedor y de las operaciones ejecutadas, previa autorización.	Se debe tener establecido un procedimiento para gestión y resolución de conflicto antes cualquier incidente o suceso que pongan en riesgo la operación y seguridad de la organización.	Los contratos de soporte y mantenimiento con terceros deben incluir cláusulas asociadas al cumplimiento de las leyes y normatividad que afecten los sistemas y activos de información, bien sean demandas por entidades de gobierno o directrices institucionales.	La organización debe velar porque el proveedor contratado tenga la capacidad suficiente y experiencia necesaria para para prestar los servicios contratados con eficiencia y eficiencia.	La organización debe implementar mecanismos e instrumentos de evaluación continua de los proveedores y los servicios contratados y tomar las acciones correctiva y de mejora necesarias.
3	2	1	2	3	4	1	1	2
9	6	3	6	9	12	3	3	6
9	6	3	6	9	12	3	3	6
12	8	4	8	12	16	4	4	8
9	6	3	6	9	12	3	3	6
12	8	4	8	12	16	4	4	8

- **Control 4**

C4. Seguridad en los equipos de procesamiento de activos de información																		
La organización debe tener definido claramente las políticas, lineamientos, planes de mantenimiento, soporte y procedimientos necesarios para ejecutar labores de mantenimiento y soporte técnico.	Toda labor de mantenimiento y soporte técnico debe quedar registrada y documentada conforme lo establece las políticas, lineamientos y procedimientos implementados.	La organización debe definir e implementar los perfiles y roles del personal autorizado para realizar labores de mantenimiento y soporte técnico en los equipos de procesamiento de activos de información.	El personal responsable de los planes de mantenimiento y demás actividades debe poseer las competencias y el entrenamiento necesario para realizar labores de mantenimiento correctivo y preventivo.	Todos los mantenimientos realizados deben cumplir con las políticas de seguridad y prevención del riesgo establecida.	Los equipos de cómputo deben estar ubicados en sitios con condiciones físicas y ambientales adecuadas para que estén protegidos y reducir el riesgo de amenazas del entorno y las posibilidades de acceso no autorizados.	Las instalaciones de procesamiento de la información que manejan datos sensibles deben estar ubicadas cuidadosamente para reducir el riesgo de accesos no autorizados y prevenir el abuso en el uso de la información.	Las instalaciones de almacenamiento y respaldo deben contar con las medidas necesarias para evitar accesos no autorizados.	Los activos y demás elementos que son contenedores de información clasificada con valor crítico y sensible, deben tener medidas de protección especiales y extremas reducir el riesgo de instrucciones y acceso no autorizados.	La organización debe adoptar mecanismos y controles de seguridad física y ambiental para reducir el riesgo de impactos negativos sobre los equipos que almacenan los activos de información.	Se deberán establecer mecanismo de control que prohíban el consumo alimentos, líquidos y cigarrillo en las áreas cercanas de operación de los equipos y del procesamiento de activos de información.	Se debe tener implementado sistemas de prevención y control de humedad, temperatura, iluminación, cargar eléctricas y demás factores del entorno que puedan afectar la operación de los equipos y el procesamiento de activos de información.	Los equipos deben cumplir con las regulaciones de ley establecidas para su operación, soporte y mantenimiento.	Los equipos deben cumplir con las especificaciones de fabricantes de equipos y proveedores para asegurar su adecuado uso y tratamiento.	Regularmente se debe evaluar el funcionamiento y el plan de mantenimiento de los equipos de procesamiento de información para las actualizaciones pertinentes.	Los equipos deben tener implementado sistemas de monitoreo y alarmas que permitan la detención temprana de fallas técnicas e incidentes de seguridad en ellos.	Los equipos deben evaluarse permanentemente para determinar la suficiencia de la capacidad para soporta la operación de los procesos de negocio de forma eficaz y eficiente.	Los planes de mantenimiento deben asegurar la disponibilidad, integridad y continuidad de la operación de los equipos de procesamiento de información y de los procesos de negocio.	Los planes de mantenimiento preventivos deben tener establecidos procedimientos técnicos y de comunicación claros de tal modo que no afecten la operación de los activos de información y de la organización en general.	Los equipos de procesamiento de activos de comunicación deben ser mantenidos de acuerdo a las especificaciones e intervalos de mantenimiento recomendados por el proveedor y el fabricante.
3	3	4	1	4	2	2	1	2	1	2	1	1	1	2	1	1	2	2	1
9	9	12	3	12	6	6	3	6	3	6	3	3	3	6	3	3	6	6	3
9	9	12	3	12	6	6	3	6	3	6	3	3	3	6	3	3	6	6	3
12	12	16	4	16	8	8	4	8	4	8	4	4	4	8	4	4	8	8	4
9	9	12	3	12	6	6	3	6	3	6	3	3	3	6	3	3	6	6	3
12	12	16	4	16	8	8	4	8	4	8	4	4	4	8	4	4	8	8	4

- **Control 5**

C5. Control operacional del software							
La organización debe establecer, documentar e implementar políticas de control operacional del software que respondan a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	Las actualizaciones de sistemas operativos, versiones de software, librerías antes de su ejecución deben estar aprobadas en un documento formal por un superior al responsable de la ejecución y solo deben ser ejecutados por personal calificado y entrenado.	Los sistemas de información que están en ambientes de producción, no deben contener código en desarrollo o compiladores.	Los sistemas de información deben tener definido e implementado un procedimiento de retrocesos (rolback) que debe ser conocido y probado por el responsable de implementar cambios antes de las ejecuciones.	Las versiones anteriores a las nuevas implementaciones debes preservarse para atender contingencias y control de cambios de versiones.	De las actualizaciones de versiones en sistemas operativos son intervenidas por proveedores, antes se debió haber firmado cláusulas de responsabilidad, buen manejo, confidencialidad y seguridad de la información; amparadas en pólizas de cumplimiento.	Todos los sistemas de información en ambiente de producción deben tener un sistema de control de configuraciones y la documentación del software implementado y el procedimiento aplicados.	Cuando los sistemas de información proporcionados a través de terceros se debe prever el esquema de control y seguimiento necesario la adecuada operación.
2	2	4	4	2	3	3	3
6	6	12	12	6	9	9	9
6	6	12	12	6	9	9	9
8	8	16	16	8	12	12	12
6	6	12	12	6	9	9	9
8	8	16	16	8	12	12	12

- **Control 6**

C6. Gestión de copias de respaldo				
La organización debe establecer, documentar e implementar una política de copias de respaldo que responda a los requisitos estratégicos, a la funcionalidad de las aplicaciones y a la seguridad de la información.	Los lineamientos y procedimientos de recuperación de información, deben estar claramente definidos y documentados.	Se deben establecer estancias de almacenamiento de copias de respaldo diferentes a las de producción, en condiciones confortables física, lógica y ambientalmente.	La frecuencia y alcance de realización de copias de respaldo debe estar definida por los requisitos de negocio, de seguridad de la información y la criticidad de la información para la operación de la organización de forma continua.	Los medios de copias de respaldo e información deben tener un sistema de pruebas continuas que verifique el medio y la información se preservan en condiciones óptimas.
3	3	2	2	4
9	9	6	6	12
9	9	6	6	12
12	12	8	8	16
9	9	6	6	12
12	12	8	8	16

- **Control 7**

C7. Gestión de las comunicaciones y seguridad de las red					
La organización debe establecer, documentar e implementar políticas de gestión las comunicaciones y redes para asegurar el desempeño óptimo en los sistemas de información que se encuentran en producción.	La organización debe tener establecido e implementado procedimientos para la gestión de la infraestructura tecnológica que soporta la operación en sistemas de información.	Se debe definir e implementar los roles y responsabilidades asociados a la gestión y adecuado mantenimiento y sostenimiento de la infraestructura tecnológica.	Todos los sistemas de comunicación y redes deben tener sistemas de autenticación y seguimientos.	Todas las actividades de monitorización y gestión de la infraestructura deben estar enfocadas a garantizar la disponibilidad de los servicios que presta la organización.	Todos los sistemas de comunicación y redes deben tener procedimientos y mecanismos de restricción de accesos según los perfiles y roles
3	2	2	1	2	2
9	6	6	3	6	6
9	6	6	3	6	6
12	8	8	4	8	8
9	6	6	3	6	6
12	8	8	4	8	8

ANEXO 5. PLAN PROGRAMA DE AUDITORIA

Organización				
Dirección:				
Representante:			Fax:	
Cargo:		Correo electrónico		
Servicios a auditar		Servicios		
		SERVICIOS DE GESTIÓN E INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR		
		Procesos: Gestión académica		
Código referencial de auditoría:				
Tipo de auditoría:				
	PRE - AUDITORIA			SEGUIMIENTO
	AMPLIACIÓN			EXTRAORDINARIA
Reunión de Apertura:		Hora:		
Reunión de Cierre:		Hora:		
Resumen:				

Auditor Líder:		Correo electrónico	
Auditor 1:		Audito 2r:	
Experto técnico:			
Fecha:			