UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

MODELO DE GESTIÓN GERENCIAL DE LA SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA EN LA ORGANIZACIÓN

Caso: Instituto Universitario de Tecnología de Valencia

.

Autora: .Ing. Jennyfer Karla Briceño.

Tutor: MSc. Ing. Nelson López.

San Diego, Octubre 2021

.

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

MODELO DE GESTIÓN GERENCIAL DE LA SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA EN LA ORGANIZACIÓN

Caso: Instituto Universitario de Tecnología de Valencia

Trabajo de Grado presentado para optar al grado académico

de Magíster en Gerencia y Tecnología de la Información

Autora: Ing. Jennyfer Karla Briceño.

Tutor: MSc. Ing. Nelson López

San Diego, Octubre 2021

UNIVERSIDAD JOSE ANTONIO PAEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

CONSTANCIA DE ACEPTACIÓN DEL TUTOR

Mediante la presente hago constar que he leído el Trabajo Final de Grado, elaborado por el(a) ciudadano(a) **Jennyfer Karla Briceño** titular de la cédula de identidad Nº **V-14.719.535**, para optar al grado académico de **Magíster en Gerencia Tecnología de la Información**, cuyo título es "**Modelo de Gestión Gerencial de la Seguridad de la Información y Tecnología en la Organización. Caso: Instituto Universitario de Tecnología de Valencia",** adscrito a la línea de investigación: **La Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas**

Y declaro que acepto la tutoría del mencionado proyecto durante su etapa de desarrollo hasta su presentación y evaluación por el jurado evaluador que se designe; según las condiciones del Reglamento de Estudios de Postgrado de la Universidad José Antonio Páez.

_____
MSc. Ing. Nelson López
C.I. V-11.895.825

San Diego, a los **15** días del mes de **Octubre** del año 20**21**

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO

VEREDICTO

Nosotros, miembros del Jurado designado para la evaluación del Trabajo de Grado **Modelo de Gestion Gerencial de la Seguridad de la Informacion y Tecnologia en la Organización,Caso:Instituto Universitario de Tecnologia de Valencia,** presentado por la ciudadana, Jennyfer Karla Briceño Titular de la Cedula de Identidad V-14.719.535 , elaborado bajo la supervisión del Tutor: Mcs. Nelson Lopez, CI. V-11.895.825, adscrito a la línea de Investigación: La Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas, para optar al grado académico de Magister en Gerencia y Tecnología de la Información, estimamos que el mismo reúne los requisitos académicos para considerarlo APROBADO.

Nombres y apellidos	C.I	Firma del Jurado
Prof.Mcs Cesar Alvarez	CI: 18.167.045	Presidente
Dra Jenny Matilde Guillen Celis	CI: 9.672.516	Miembro
Prof. Mcs Jesus Yanez	CI: 19.000.349	Miembro

UNIVERSIDAD JOSE ANTONIO PAEZ UJAP VICERRECTORADO ACADEMICO

En San Diego, a los veinte días del mes de Octubre del año dos mil veintiuno

DEDICATORIA

El presente trabajo de grado va dedicado a Dios, quien como guía estuvo presente en el caminar de mi vida, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer.

A mis padres que con apoyo incondicional, amor y confianza permitieron que logre culminar mi carrera profesional.

A mi familia por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida.

A mi esposo

En el camino encuentras personas que iluminan tu vida, que con su apoyo alcanzas de mejor manera tus metas, a través de sus consejos, de su amor, y paciencia me ayudo a concluir esta meta.

ÍNDICE GENERAL

LISTA DE CUADROS **Pág.**

LISTA DE GRÁFICOS **Pág.**

	UNIVERSIDAD JOSÉ ANTONIO PÁEZ **VICERRECTORADO ACADÉMICO** **DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO** **MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN**

MODELO DE GESTIÓN GERENCIAL DE LA SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA EN LA ORGANIZACIÓN

Caso: Instituto Universitario de Tecnología de Valencia

AUTORA: Ing. Jennyfer Briceño
TUTOR: MSc. Ing. Nelson López
Octubre, 2021

RESUMEN

La seguridad de la información no se gestiona adquiriendo solo herramientas de software o hardware sino que cada organización debe establecer su propia normativa de seguridad que contemplen políticas, normativas, procedimientos y funciones. El presente estudio tiene como objetivo proponer un Modelo de Gestión estratégico para la Seguridad de la información y Tecnología favorable a la sustentabilidad de la cultura gerencial en la organización educativa IUTVAL como coformadora de capital social, que contribuya a fomentar las actividades de protección, integridad, confiablidad y control de ella, basado en estándares internacionales, que garantice sus atributos, dicho estudio se realizó en el Departamento de Tecnología de Sistemas e Información (DTSI) del Instituto Universitario de Tecnología de Valencia (IUTVAL), donde no existen políticas relacionadas a la seguridad de la información, enmarcadas en las Normas ISO 27000. En la construcción del modelo se incluye como un principio a seguir al Balanced Scorecard (Sistema de Balanceo de Indicadores), que implica un enfoque de 4 fases. Dicho estudio, se sustenta en la Teoría de Gestión de Cuadro de Mando Integral (CMI) y Árbol Estratégico, la cual viabiliza que desde cada cargo o puesto de trabajo en el entorno interno institucional, se marca la gestión gerencial estratégica. El estudio en cuestión, se basa en un enfoque cuantitativo, enmarcado en un nivel descriptivo, integrado con un diseño de campo, no experimental, bajo un enfoque de Proyecto Factible. Se utilizaron como técnicas de recolección de datos el cuestionario escrito, diseñado bajo un instrumento tipo Likert de cinco opciones a la selección de una. Los resultados de esta investigación permitieron el constructo del modelo de gestión gerencial de seguridad de la información y tecnología, hacia la consecución de los objetivos de la organización. Todo esto, bajo el marco de la línea de investigación: La Información como valor agregado en el seno de las organizaciones públicas y privadas.

Descriptores: Modelo, Gestión Gerencial, Seguridad, Información, Tecnología .

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

MODEL OF MANAGERIAL MANAGEMENT OF THE SECURITY OF THE INFORMATION AND TECHNOLOGY IN THE ORGANIZATION
Case: University Institute of Technology of Valencia

AUTHOR: Ing. Jennyfer Briceño
TUTOR: MSc**.** Ing. Nelson López
October, 2021

Summary

Information security is not managed by acquiring only software or hardware tools, but each organization must establish its own security regulations that include policies, regulations, procedures and functions. The aim of this research is to propose a strategic Management Model for Information Security and Technology favorable to the sustainability of the managerial culture in the educational organization IUTVAL made of social capital, which contributes to promoting activities of protection, integrity, reliability and control of it, based on international standards, which guarantees its attributes, this research was carried out in the Department of Systems and Information Technology (DTSI) of the University Institute of Technology of Valencia (IUTVAL), where there are no policies related to the Information security, delimited in the ISO 27000 Standards. In the construction of the model, the Balanced Scorecard is included as a principle to follow, which implies a 4-phase approach. This research is based on the Balanced Scorecard Management Theory (BSC) and Strategical Tree, which makes it possible for each position or job in the internal institutional environment to sign strategic managerial management. The study in question is based on a quantitative approach, framed at a descriptive level, integrated with a non-experimental field design, under a Feasible Project approach. The data collection techniques used were the written questionnaire, designed under a Likert-type instrument with five options to the selection of one. The results of this research allowed the construction of the information security and technology management t model, towards the achievement of the organization's objectives. All this, under the framework of the research line Information as added value within public and private organizations

Descriptors: Model, Management, Security, Information, Technology

INTRODUCCIÓN

El mundo actual cada vez más globalizado, exige de parte de las organizaciones un mayor y mejor acceso a la información. En este sentido, las tecnologías de la información han abierto una serie de posibilidades para las pequeñas y grandes organizaciones, dándoles nuevas oportunidades y haciéndolas más competitivas.

Ante estos nuevos cambios tecnológicos, aparecen los riesgos y el problema de contar con una plataforma informática segura. En base a esta premisa, la forma de enfrentar los problemas de seguridad de la información que se presentan en la actualidad, es que las organizaciones entiendan lo importante, que es proteger sus sistemas de información de intrusos, usuarios o daños fortuitos, que ponen en peligro el desempeño informático de la empresa.

Ahora bien, la velocidad con que ocurren los cambios, sobre todo en el área tecnológica, hace difícil la planeación estratégica, que permita asegurar el capital intelectual representado por la información dentro de una organización. Por lo que se hace necesario integrar las estrategias de negocio con las estrategias tecnológicas en materia informática, lo que traerá como consecuencia un diseño de políticas de seguridad que se ajusten a la organización.

En este sentido, la seguridad de la información involucra la protección de los activos de la información, para lo cual es necesario identificar las situaciones de riesgo que se puedan determinar, los cuales estos activos son vulnerables ante las amenazas, tanto internas, como externas a la empresa. Tomando en cuenta que entre los objetivos de la seguridad de la información, se encuentran el acceso, confiabilidad e integridad de la información, es necesario determinar qué herramientas o controles pueden ayudar a reducir y monitorear los riesgos detectados en las plataformas informáticas de las organizaciones.

Entre este tipo de medidas se deberían emplear un marco de trabajo que les permita implementar de una manera sistemática y efectiva un mayor control sobre la seguridad de la información y activos informáticos que involucre a todo el personal, desde la alta dirección hasta los operarios de los sistemas. Este marco es conocido como un Sistema de Gestión de la Seguridad de la Información y está basado en estándares, modelos y normas internacionales que a través de una serie de mejores prácticas aseguran una adecuada gestión de la seguridad de la información. Una de las normas más reconocidas es la ISO/IEC 27001 que establece las guías, procedimientos y procesos para gestionarla apropiadamente mediante un proceso de mejoramiento continuo

En base a lo anteriormente señalado, el Departamento de Tecnología de Sistemas e Información (DTSI) del Instituto Universitario de Tecnología de Valencia (IUTVAL) soporta la infraestructura tecnológica que ayuda al desarrollo normal de los procesos y toma de decisiones de la institución. Por consiguiente se hace necesario evaluar los riesgos a los que están expuestos los activos informáticos y emplear un enfoque metodológico que permita mitigarlos o mantenerlos a un nivel aceptable, además de establecer un plan de mejoramiento continuo.

La presente investigación tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información para la oficina del Departamento de Tecnología de Sistemas e Información del IUTVAL, que sirva como punto de partida para su implementación mediante un análisis de la situación actual de los dominios, objetivos de control y controles que sugiere la norma ISO 27001, la selección de una metodología de evaluación de riesgos informáticos, el establecimiento de una política de seguridad informática institucional que sea liderada por la alta gerencia, además de generar la documentación respectiva para los Planes de Continuidad de Negocio con el fin de mantener y/o restaurar los servicios críticos y el análisis y

selección de un modelo de Gobierno de Tecnología Informática que se ajuste a las necesidades institucionales.

Bajo este enfoque, el estudio está estructurado en V Capítulos. En este sentido, en el primer Capítulo se describe la situación problemática presente en en el el Departamento de Tecnología de Sistemas e Información, así como los objetivos y justificación de la investigación. Posteriormente se desarrolla el Capítulo II se refiere al Marco Teórico, basado en investigaciones ya realizadas previamente así como los fundamentos teóricos que sustentan el estudio,

Seguidamente el Capítulo III viene representado en el Marco Metodológico, en el cual se recogen los aspectos metodológicos de la Investigación, donde se describirán los procedimientos que se utilizarán para abordar el problema planteado, así como también la población y muestra y la forma como serán analizados los resultados obtenidos. Posteriormente en el Capítulo IV se presentan los resultados, en base a los objetivos específicos con sus correspondientes tablas y gráficos, derivados de la recogida de datos del instrumento utilizado. Consecutivamente se plantea el Capítulo V, con la Propuesta desarrollada, seguida de las respectivas conclusiones obtenidas en la investigación, así como las Recomendaciones necesarias

Para finalizar, se recogen las Referencias Bibliográficas utilizadas en la investigación y los anexos correspondientes.

CAPÍTULO I

I EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El mundo digital se ha integrado en toda la sociedad de tal manera que se ha hecho imprescindible, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre ip, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. Las “transacciones” electrónicas nos permiten ahorrar tiempo y recursos, pagar los servicios públicos, transferir de una cuenta bancaria a otra, participar en una subasta para comprar un vehículo, pagar un boleto de avión etc. En todos estos ejemplos hay algo en común, el dinero, y cuando hablamos de tan escaso, pero tan apreciado bien las empresas deben garantizar la implementación de políticas de seguridad informática. (Amaro, 2016).

Por consiguiente, los que trabajan en el mundo empresarial, deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios. Cada vez encontramos más gerentes interesados en entender las reglas del negocio, entre ellas las referentes a las políticas de seguridad de la información. El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia (o desconocimiento), sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio.

En este mismo orden de ideas, como lo señala Amaro (2016), países como Cuba han creado la Oficina de Seguridad para las Redes Informáticas (OSRI), emitida por el Acuerdo 3736/2000 del Comité Ejecutivo del Consejo de Ministros (CECM), adscrita al Ministerio de la Informática y las Comunicaciones (MIC), con el objetivo de prevenir, evaluar, investigar y dar respuesta a las acciones tanto internas como externas que afecten el normal funcionamiento de las Tecnología de la Informática y las Comunicaciones (TIC) en el país. De igual forma, países como España crean a finales del año 2006 el CCN-CERT donde su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). Todo lo cual nos refleja que no solo el mundo empresarial se preocupa por la seguridad de la información, sino también los entes gubernamentales.

En lo que respecta a Venezuela, el gobierno dando cumplimiento a la norma constitucional, aprobó la Ley Orgánica de Ciencia, Tecnología e Innovación (2014), que tiene por objeto en su artículo 1: “desarrollar principios orientadores que, en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela” (p.3).

Sin embargo para que este esfuerzo de incorporar a Venezuela en la era de la tecnología y de la información, alcance un nivel adecuado, se hace necesario la difusión de un conjunto de instrumentos legales que proporcionen el marco institucional a lo interno de las organizaciones y la población usuaria de cada sector , el desarrollo armonioso del conocimiento en asuntos de Gestión de Seguridad de la Tecnología (GST) y a su democratización y, que precisamente para lograr los objetivos tanto de la norma constitucional como de la Ley Orgánica de Ciencia, Tecnología e innovación, se ha hecho necesario promover al mismo tiempo las condiciones de seguridad que inspirarán suficiente confianza tanto a los administradores de las plataformas que brindan servicios tecnológicos como al usuario en general, incluso en su diario hacer.

Por otra parte, en el contexto de Venezuela, el gerente de Soporte y Capacitación en el país de la marca ESET, un reconocido software de seguridad y antivirus, considera que los usuarios más vulnerables son los que tienen desconocimiento sobre la seguridad informática. Al respecto, mediante entrevista corta en los medios de comunicación, el gerente López (2020) ha dicho que “En Venezuela somos bastante curiosos… Hay que educarse sobre el tema, tener cuidado y desconfiar”. Además, señala que los venezolanos “tenemos debilidad por las cosas gratuitas. Por ejemplo, una red inalámbrica de un centro comercial, y debemos ser precavidos porque no sabemos quién está detrás de ese wifi”. La anterior es una gran reflexión del experto en seguridad.

Ahora bien, con la imparable evolución tecnológica, la seguridad de la información se ha convertido en una necesidad para cualquier organización para la toma de decisiones e implementación de nuevas estrategias de negocio, tomando como negocio en este caso la prestación del servicio tecnológico. Es por ello que, al operar la información, se deben considerar las vulnerabilidades existentes en las plataformas tecnológicas conformadas por un conjunto de equipos físicos, como lo son los rack, servidores, switches, cableados o señales inalámbricas, equipos y demás dispositivos; así como también el software que compone el funcionamiento de los protocolos de comunicación, sistemas, programas, entre otros y las posibilidades de ataques por parte de los llamados cibercriminales o hackers. En efecto, es común la existencia del espionaje, tráfico y robo de información: en este sentido, empresas como eBay, Heartland, Adobe, Sony y PlayStation Network, cada una con más de 100.000 millones de cuentas de usuario, fueron objeto de ataques informáticos, dando como resultado el robo de información como: cuentas bancarias, número de tarjetas, listas de correos electrónicos y contraseñas, información anterior que fue confirmada mediante la fuente de noticias en Economía Digital (2017).

Dentro de este mismo contexto, las instituciones educativas no escapan de ser potenciales víctimas de violaciones a la seguridad de la información.

Pagnotta (2016), señala que la Universidad de Virginia de Estados Unidos (EEUU) fue víctima de un *phishing* (puerta de entrada para los cibercriminales, para robar credenciales e información), de robó datos tributarios, la fuente afirmo que "de los formularios tributarios de 1.400 empleados de la Universidad de Virginia se filtraron cuando los criminales obtuvieron acceso al sistema de Recursos Humanos (RRHH)". Estos formularios W-2 se usan en EEUU para reportar los salarios pagados a los empleados y los impuestos retenidos a ellos.

Cabe considerar que las universidades de Venezuela, entre ellas de la Universidad Experimental de las Artes (UNEARTE) registró el primer ataque con ransomware, Alí Rojas, su Rector, denunció ante la División Contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC) que el sistema de registro de información académico de la UNEARTE, conocido como Sistema Interno de Gestión Universitaria (SIGEU) fue atacado por fuentes desconocidas y toda la información que contenía esta base de datos fue secuestrada, pidiendo a cambio una recompensa en moneda digital o bitcoins. En este sentido, el director de Tecnología, Información y Telecomunicaciones de la universidad UNEARTE, Freddy Benedetti, identificó que el dominio que fue utilizado por los hackers es «gratuito, pero de nivel superior», que la identificación de la IP procede de la República de Malí, y que «el uso del correo asociado tiene posible origen, bajo huella de Internet, en Pakistán». Esto probablemente implica que, simplemente, los cibercriminales utilizaron programas para enmascarar su dirección IP.

Con estos antecedentes, se requiere considerar a la seguridad de la información como un requisito primordial para cada organización educativa, con énfasis en el sector universitario por tener datos de ciudadanos que están insertos en el ámbito global con responsabilidades de adultos, por ejemplo, pago de impuestos, documentación personal internacional como pasaportes, ciudadanos activistas, próximos profesionales o egresados de titulaciones

profesionales, entre otras atribuciones personales. Todo ello conlleva a pensar en formular un conjunto de medidas, internas a cada organización educativa, de resguardo que tienen el ecuánime objetivo de prevenir, resguardar y proteger la información, y de esta manera asegurar los tres pilares de la seguridad: disponibilidad, integridad y confidencialidad.

Por lo tanto, considerando la información como el activo más preciado dentro de las organizaciones, se han desarrollado mecanismos no sólo para proteger sistemas computacionales, sino para reducir los riesgos de pérdida de la información a través de la Gestión de la Seguridad de la Tecnología (hardware y software) que contiene la información. En este sentido, para que exista un adecuado Sistema de Gestión de la Seguridad de la Tecnología e Información (GST) dentro de las organizaciones, es necesario crear un modelo que oriente esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de gerencia en asuntos de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. (Susanto, Nabil Almunawar & Chee Tuan, 2017)

En otro orden de ideas, es importante mencionar que la gerencia en los tiempos actuales enfrenta factores de cambios culturales, tecnológicos y económicos repentinos. Las empresas se encuentran atravesando un periodo de permutaciones que las empujan a informatizar con sistemas digitales todos sus ámbitos organizativos. Razón por lo que las personas responsables de dirigir la seguridad de la información en las organizaciones, deben estar preparados con un particular método para gestionar, planear, organizar, dirigir, controlar y corregir todo lo relacionado a los activos organizacionales.

Ante este problema, las compañías han invertido en seguridad. Según un estudio realizado por Gartner, las empresas a nivel mundial invertirán un aproximado de 96.296 millones de dólares en ciberseguridad. Esto quiere decir que en 2018 se invirtió un 8 % más que en 2017. La tendencia es clara, firme y preocupante. No obstante, las tecnologías por más sofisticadas que ellas sean

requieren del factor humano y entonces entra en acción el capital social humano de una organización, quienes son garantes de poner en marcha las soluciones técnicas institucionales al problema de la gestión de la seguridad tecnológica.

Cabe resaltar, que una buena gestión de la información en una organización, contribuye notablemente a reducir los costos e incrementar la productividad en las empresas, reducir la obsolescencia, aumenta la fiabilidad, mejora la usabilidad, por lo que se inicia entonces, todo un proceso para gestionar la seguridad de la información a través de normas internacionales y/o estándares, teorías con técnicas de gestión administrativa, lineamiento de políticas orientadas a garantizar confidencialidad, integridad y disponibilidad de la información y de los sistemas que la procesan, con el fin de reducir riesgos.

Ahora bien, las organizaciones que no pongan en práctica una gestión adecuada a la eficiencia de las exigencias, se encuentran más vulnerables ante cualquier tipo de ataque, al manejo y control de la información. Tal es el caso de la organización contexto que ocupará el objeto de este trabajo de grado, se trata del Instituto Universitario de Tecnología de Valencia (IUTVAL), el cual es una institución de educación universitaria que está comprometida con el proceso de enseñanza-aprendizaje, siendo su leit motiv egresar ciudadanos profesionales en carreras técnicas, y como toda organización educativa de avanzada contemporánea, posee sistemas de información que soportan sus procesos académicos y administrativos.

Dicha organización , en lo sucesivo abreviada IUTVAL, está soportada por una serie de departamentos operativos de gestión , adscritos a la gerencia principal del Director de la Institución educativa, entre ellos el Organigrama señala el Departamento de Tecnología de Sistemas e información , sin embargo al revisar in situ la documentación de manuales operativos del nombrado departamento, se encontró que no existe formalmente aprobada una política actualizada de seguridad de la información claramente definida, lo cual es una debilidad que genera riesgos y amenazas que pueden causar una afectación

nociva en el hardware o software que funge como plataforma tecnológica de infraestructura física y soporte al desarrollo de los procesos ligados al desempeño institucional de la mencionada organización educativa universitaria.

En el mismo orden de ideas, los recursos tecnológicos de los cuales dispone IUTVAL (equipos tecnológicos), carecen de criterios de seguridad, en cuanto a su uso, así como de herramientas tecnológicas adecuadas que faciliten el trabajo experto, y coadyuven a la protección protocolar del mantenimiento del hardware y software instalado, lo cual acarrea una arbitraria colocación de restricciones y/o prohibiciones que en general no son las más adecuadas para detener el problema de inseguridad tecnológica o vulnerabilidad de la información. Lo antes señalado repercute en malas praxis técnicas y hace inferir el desconocimiento de teorías adecuadas a las soluciones tecnológicas requeridas por la organización , ya que de igual manera al revisar los procedimientos al respecto del traslado, transferencia de la información o respaldo, no existe ninguna política, que garantice y asegure de forma adecuada el proceso operativo, considerándose esto un alto riesgo para la institución que amenaza la sustentabilidad de la ecología digital de la organización y a su poderoso capital de información ligada al factor social y humano que es el más preciado valor de negocios para la gestión de la cultura de gestión en una universidad.

Para reforzar la idea final del párrafo anterior se agrega que el ambiente organizacional educativo actual público y privado está caracterizado por precedentes y actuales decisiones en las recientes décadas de gestión en el servicio público de la educación para todos, sustentado en criterios de ética, corresponsabilidad y responsabilidad social, al ser establecido en reformas del ordenamiento jurídico y del texto constitucional, que rige esta estructural materia, esencialmente en la LOE-2009, y por Ley Habilitante, del Decreto-Ley Orgánica de la Administración Pública (2008), del Decreto-Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras (2012-2013), la Ley del Estatuto

de la Función Pública. (2002). Esencialmente de la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (2005). En este ordenamiento, también se preceptúa la protagónica participación de vocerías vecinales por la reforma de la Ley Orgánica de los Consejos Comunales (2010), y de la Ley Orgánica de Contraloría Social (2010), que, por esos u otros mandatos jurídicos, las universidades nacionales, tienen la jurídica obligación de cumplir «por las sanciones a su no-cumplimiento». Es por todo ello que en este trabajo se vinculan esas actualizaciones en lo que se trata de conocer como cultura de gestión para pretender establecer como parte del trabajo el establecimiento de unas políticas nuevas cabe preguntarse entonces ¿existe la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como coformadora de capital social en el IUTVAL? Como lo exigen los estatutos de las universidades.

Desde esta arista en el factor educacional está siempre presente el fortalecimiento a la ética organizacional, evitando que la gerencia no se convierta en un muro inerte, sino que se interese en la comprensión, dirección y optimación de las organizaciones que efectivamente quieren aprender, y cuyo elemento verdadero elemento clave son los individuos que integran a la organización, con su poderosa experticia; esto palabras de González y Belino (1995) es la “cultura centrada en las personas”.

En Venezuela se les exige a las universidades que, en función a sus compromisos, se renueve el principio de corresponsabilidad por las Metas Educativas del 2021(2008): “La educación que queremos para la generación de los Bicentenarios”, firmado por Venezuela en El Salvador junto a otros países Iberoamericanos, donde se hace hincapié en el carácter intersectorial de las acciones internas de las organizaciones para el logro de sus fines.

Debido a lo expuesto, desde los modelos de la esencia de los espacios universitarios educacionales, donde se ha de emprender un hacer de Gerencia Apreciativa, según Rovira (2014):

> "..La cultura gerencial creada y acordada de esta manera, es una "obra de arte empresarial" que distingue la identidad de la empresa, mediante la cual podría realizar negocios innovadores, rentables, sostenibles, manteniendo a sus colaboradores motivados a siempre buscar mejores maneras de realizar el trabajo...".

A este respecto, la institución al no tener diseñado e implementado un Modelo de Gestión Gerencial de la Seguridad de la Información y tecnología, se expone a riesgos que no solamente afectarían lo técnico, sino también a las personas que se verían afectadas con la interrupción de servicios, como aulas virtuales, cobro de nómina, entre otros ; pero también hay que considerar que para que este trabajo de grado sea útil como propuesta , el cual será su razón fundamental debe enmarcarse la misma en la actualidad gerencial que le es requerida en materia legal, operativa, o de beneficio como a cualquier otro sistema a implantarse desde el ámbito técnico.

Es así como desde el protagonismo que ejercerá el personal encargado del área del departamento de sistemas se requiere en esta investigación estar al tanto, en el marco de la cultura gerencial, ¿en cuan medida la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, es proactiva considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios?

¿Qué criterios están presentando los funcionarios del Departamento de Tecnología de Sistemas e Información para la necesidad de un sustentable modelo estratégico en seguridad tecnológica, considerando la cultura gerencial y el rol educativo del IUTVAL en materia de Gestión de Seguridad Tecnológica? Esta interrogante se planteó parafraseando los principios de gestión de Schein (1994) "De manera interna: El lenguaje común. y de manera externa: misión y estrategia, metas, medios, medición y corrección."

Cabe resaltar que en la seguridad de la información existen las amenazas de carácter técnico, pero también influyen las amenazas de tipo humano,

existen insuficiencias en las definiciones administrativas de acuerdo a los estándares internacionales revisados de las normas ISO 27001-2007, de sus roles y responsabilidades del cargo que les corresponde desempeñar y sobre todo no está normado en función del manejo de la seguridad de la información. El síntoma más elemental de ello es el uso de correos personales para la comunicación interinstitucional que conlleva a establecer la inexistencia de una simple validación de credenciales de acceso al dominio universitario , así mismo esa situación tan sencilla pero importante genera la permisibilidad de uso a múltiples usuarios con múltiples contraseñas para acceder a diferentes servicios, ocasionando el frecuente olvido de sus datos de acceso, además de no tener un sistema de recuperación de contraseña automático, sino de forma manual y personal, lo más relevante para la seguridad es que esas carencias protocolares hacen inauditable los accesos y a partir de allí todo es vulnerable.

Pese a todo lo indicado no se puede perder de vista la cita de Baas (1997) “que el capital social tiene que ver con cohesión social e identificación con las formas de gobierno y con expresiones culturales y comportamientos sociales”; así que la finalidad de proponer un modelo de gestión de avanzada en materia de seguridad tecnológica en este trabajo de grado es la de contribuir en el cambio hacia el enfoque de desarrollo sustentable y estos modelos de gestión y dirección que promueven un camino de gerencia socialmente responsable que tenga como norte la sustentabilidad.

Vinculado a las tendencias teóricas actualizadas expuestas en materia de seguridad y su gestión con basamentos técnicos y administrativos, se considera relevante para la organización educativa en contexto, la propuesta de un Modelo de Gestión Gerencial de la Seguridad de la Información y Tecnología en la Organización IUTVAL, que contemple normas o estándares nacionales, internacionales, y principios administrativos que haga factible realizar en el tiempo y espacio señalado el trabajo pertinente por parte del Departamento de Tecnología de Sistemas e Información (DTSI) del IUTVAL, con la intención

de proteger la información como valor agregado en el seno de las organizaciones públicas alineada al cumplimiento de los objetivos de la de la institución. Dicha propuesta está enmarcada en el área de investigación Ciencia, Tecnología de la Información y Desarrollo de la Economía, precisamente en la Línea de investigación: la Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas.

1.2 OBJETIVOS

Objetivo General

Proponer un Modelo de Gestión estratégico para la Seguridad de la información y Tecnología favorable a la sustentabilidad de la cultura gerencial en la organización educativa IUTVAL como coformadora de capital social.

Objetivos Específicos

1. Identificar la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como coformadora de capital social en el Departamento de Tecnología de Sistemas e Información del IUTVAL.
2. Describir en el marco de la cultura gerencial, la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios en el Departamento de Tecnología de Sistemas e Información del IUTVAL.
3. Determinar las tendencias de la praxis de GST en el Departamento de Tecnología de Sistemas e Información para la seguridad tecnológica, considerando la cultura gerencial y el rol educativo de la organización IUTVAL.

4. Enunciar un conjunto de lineamientos bajo modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL como organización educativa.

1.3 JUSTIFICACIÓN

Actualmente, las organizaciones desafían cada vez más riesgos e inseguridades que pueden dañar de forma alguna el activo más importante como lo es, la información. Ante estas circunstancias es imprescindible que las empresas evalúen los riesgos asociados y establezcan las estrategias y mecanismos adecuados que aseguren permanentemente la protección y salvaguarden la información, con herramientas gerenciales y tecnológicas que permitan la búsqueda de mejoras, eficiencia y calidad para alcanzar los objetivos propuestos.

Bajo esta premisa la investigación se justifica, ya que el modelo de gestión gerencial de la seguridad de la información y tecnología al momento de ser aplicada a la institución, traerá consigo diversos beneficios de relevancia social necesarios para la toma de decisiones acertadas y oportunas, creando una estructura organizativa que garantice y facilite la coordinación entre el personal de la institución, lo que permite el manejo efectivo y estratégico de los procesos relacionados a la seguridad de la información a través de medidas de seguridad eficientes, generando valor agregado a la información, procedimientos y objetivos que permitan establecer controles de seguridad que ayuden a tratar los riesgos en la seguridad de la información y de esta manera optimizar la gestión de aquellas eventualidades que se presenten para generar decisiones apropiadas en función de los objetivos de la organización.

Cabe resaltar, que la propuesta del modelo implica la aplicación y gerencia de medidas de seguridad apropiadas que involucran en los datos, su confidencialidad: protección de la información en contra a su divulgación no

autorizada; integridad: validez de los datos, de acuerdo a los objetivos organizacionales; disponibilidad: en el momento que se requiera para los usuarios autorizados.

Asimismo, el diseño de un Modelo de gestión de la seguridad de la información favorece en fomentar las actividades de protección de la información en las organizaciones, mejorando su imagen y generando confianza frente a terceros. Todo esto conforme la Norma ISO/IEC 27000, referente internacional para la certificación de la Gestión de Sistemas de información, que establece los requisitos para implantar, documentar y evaluar un sistema de gestión de la seguridad de la información.

Finalmente, presentará un valor potencial al conocimiento ya que a medida que se aplique en el IUTVAL dentro de sus estructuras la metodología de los Sistemas Balanceados de Indicadores, se percatará que puede utilizarse para: clarificar la estrategia y conseguir el consenso sobre ella, comunicar la estrategia a toda la organización, alinear los objetivos generados con los del resto de la estructura por departamentos, con la estrategia, vincular los objetivos a largo plazo y los presupuestos anuales del mantenimiento de la seguridad, identificar y alinear las iniciativas estratégicas, realizar revisiones periódicas y sistemáticas, y obtener información de retorno (evaluación) para la estrategia y mejorarla.

CAPÍTULO II

II MARCO TEÓRICO

Sabino (2002), reseña: "… El marco teórico, también llamado marco referencial… tiene precisamente este propósito: brindar a la investigación un sistema coordinado y coherente de conceptos y proposiciones que permitan abordar el problema…", (p. 47). A continuación, en torno a las características de este trabajo de grado se presentan los siguientes subapartados del capítulo.

2.1 ANTECEDENTES

Zambrano (2017), realizó una investigación en la Universidad Regional Autónoma de Los Andes titulada: **Plan Informático para mejorar la Gestión de Seguridad de Información del Gad Municipal Tosagua.** El objetivo principal proteger los recursos tecnológicos y para fortalecer las políticas y normas con los más altos estándares de calidad y mecanismos de seguridad para el sistema de red, evitando que personas extrañas al trabajo y a la información puedan hackear el sistema, malversando información de única y exclusiva privacidad del local y de quienes estén a cargo de su administración.

La propuesta concluye, que la investigación cubrirá todos aquellos lineamientos a tener en cuenta en relación a estándares, normas, procedimientos y medidas tecnológicas que aseguren la confidencialidad, integridad, y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión, además del aspecto de detección de accesos no autorizados a la información

Este trabajo estará relacionado con la presente investigación, porque ofrece una visión amplia acerca de la implementación de las Normas de regulación vigentes, presente en ISO/IEC 27001 en lo que respecta a estándares, procedimientos, normas y medidas que empleen tecnología, que permitan asegurar las principales características que debe tener la información que son integridad, disponibilidad y confidencialidad.

Yánez (2017), desarrolló un trabajo de investigación denominado **Sistema de Gestión de Seguridad de la Información para la Subsecretaria de economía y empresas de menor tamaño**, en la Universidad de Chile, cuyo propósito fue utilizar herramientas open source y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO27001:2013. El proyecto concluye en una evaluación de la implementación del SGSI y de las políticas y procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias fueron totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información. Ambas auditorias llegaron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance sustancial pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información.

El trabajo sirve de marco de referencia para la investigación ya que la metodología usada consta de un repertorio de documentos que pueden ser clasificados como mejores prácticas generales para el control y seguridad de la información. Tiene que ver con la Seguridad de la Información y la metodología sugerida, lo que permite evaluar el proceso que se siguió durante el establecimiento de dicha metodología y orientar el desarrollo de esta investigación.

Cáceres (2018), presentó un estudio venezolano titulado: **Cómo Incrementar la Competitividad del Negocio mediante Estrategias para Gerenciar el Mantenimiento**; en el cual se desglosan teorías y tendencias, que la literatura experta presenta a las organizaciones de cualquier sector, con énfasis en la Administración Pública venezolana, el alcance a la continua búsqueda de la excelencia. La autora de dicho estudio expresa que en la actualidad, la realidad de gestión efectivamente competitiva, obliga a las organizaciones, evolucionar continuamente para mantenerse competitivas dentro del estatus del mercado vinculado con su distintiva razón social. En ese norte, el tema de ese trabajo se sustentó, en: "…una serie de estrategias en 4 aspectos principales llamados: Confiabilidad Equipos, Confiabilidad de los procesos, Confiabilidad del Talento y Confiabilidad del Valor. (p. 2)." De allí que, desde los reseñados datos historiográficos del citado trabajo de Cáceres (op cit), es posible identificar esa metodología integral, sustentada en la filosofía de Mantenimiento Clase Mundial para el Siglo XXI, cuando al definirla indica a texto: "La definición de Mantenimiento Clase Mundial ha venido evolucionando con el tiempo siendo la más acertada, "mantenimiento sin desperdicio" definiendo a este último como la diferencia entre la manera de hacer las cosas hoy y como deberían hacerse" (p. 3).

La pertinencia del citado trabajo con esta investigación, está en que describe la cadena de valor integrada con procesos medulares en: Procesos de Gerencia del Conocimiento, Calidad de Gestión, Políticas, Planes, Estrategias de Direccionamiento global «Desempeño del talento humano, Sistemas, Tecnologías, Programación, Contratación, Ejecución»; que, entre otros enfoques, son clave al constructo de la propuesta en este objeto estudio.

Quiroz y Zapata (2019), Presentaron en la universidad ITM en Colombia su trabajo de maestría titulado **Modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción Filtro Kalman**. Este proyecto consiste en el desarrollo de un

modelo de gestión de incidentes de seguridad en los sistemas de Supervisión, Control y Adquisición de Datos (SCADA) basado en predicción de eventos, es decir, a través de la recolección de información de posibles ataques informáticos, se hace una predicción con el modelo matemático Filtro Kalman (el cual realiza predicciones de variables lineales por medio de mínimos cuadrados recursivos), una vez se genera la predicción del posible evento de seguridad, se activa el proceso de manejo de incidentes; el resultado final, es un modelo de gestión de incidentes de seguridad basado en la detección temprana entregada por el filtro Kalman, caracterizado por niveles de impacto, los cuales definirán el procedimiento adecuado al nivel de criticidad de la predicción, permitiendo así lograr una integración y despliegue de las mejores acciones dependiendo del tipo de alerta que se genere y en este sentido, lograr una posible reducción en los niveles de exposición al riesgo y reducción de posibles impactos.

La relación que guarda dicha investigación con la presente que permitió revisar la metodología para implementar prototipos bajo el diseño de modelos de normalización técnica factible en materia de seguridad y revisar los esquemas.

Diaz, P. (2020), Presentaron en la universidad ITM en Colombia su trabajo de maestría titulado **Modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción Filtro Kalman.** Se puede afirmar que dentro de las entidades de salud nace la necesidad de implementar un sistema de información electrónico para poder enviar datos e información, que en la mayoría de los casos es de carácter privado y confidencial; generalmente esta información es muy sensible para los pacientes porque contiene datos personales e historiales que registran enfermedades que padecen, datos que pueden ser utilizados negativamente si llegan a caer a manos de terceros como delincuentes informáticos, quienes tendrían toda posibilidad para robar su identidad e inclusive estar expuestos a

altos riesgos que podrían incidir en la misma vida de los pacientes o en la perdida de confiabilidad de las entidades que utilizan dichos datos. Es por eso que la empresa HL7 pensando en los problemas de comunicación y envío de información de una entidad a otra en el sector salud crea un estándar llamado HL7 CDA(Clinical Document Architecture) R2 (Release 2) el cual permite realizar esta comunicación pensando en un carácter netamente de interoperabilidad, para que así se puedan realizar envíos de diferentes tipos de archivos y en diferentes plataformas, pero que puedan ser leídos por el sistema de otras entidades transmitiendo historiales médicos. Es así como surge una pregunta: ¿Es seguro el Estándar HL7 CDA en su Confidencialidad?; partiendo de proyectos realizados hace algunos años se puede concluir que se ha trabajado muy poco en la seguridad de este estándar dejando ver algunos riesgos de seguridad que llevan a vulnerabilidades del estándar, de mucha importancia en la confidencialidad de los documentos que se transmiten por este medio, principalmente vulnerabilidades de XSS (Cross site scripting) y vulnerabilidades de obtención de información. Se entrega como resultado final del proyecto desarrollado un Prototipo de framework que permita brindar más seguridad en el estándar HL7 CDA R2, es por ello que se ha iniciado un estudio de varias herramientas de detección y prevención, de trabajo en conjunto bajo características fundamentales como, que sean OPEN SOURCE. Esta investigación se realizó bajo 3 fases metodológicas, primera fase Identificar problemas y Determinar Herramientas, donde se identificaron y caracterizaron los problemas de confidencialidad del estándar, se buscaron las mejores herramientas para detectar y prevenir los problemas que afectaron la confidencialidad del estándar. La segunda fase Desarrollo del prototipo de Framework, donde se recolectaron los historiales médicos electrónicos, se investigó acerca de un visor de documentos CDA web, se identificaron las medidas de seguridad para las vulnerabilidades encontradas y se simuló un envío de historiales médicos para su posterior análisis de vulnerabilidades. Para

desarrollar el prototipo de framework se acoplo dos módulos (IDS, IPS) open source para trabajar en conjunto y de manera equilibrada, mostrando los ataques con su nivel de criticidad en score de CVE vulnerability. La tercera Fase es Evaluar el Prototipo de Framework Propuesto, donde se implementó el prototipo de framework en un servidor Ubuntu y se realizaron las pruebas pertinentes para corroborar que las vulnerabilidades fueron mitigadas, el desarrollo del prototipo se realizó con el fin de brindar confidencialidad de la información en los historiales clínicos, los cuáles son transmitidos por este estándar.

La razón de incorporar dicha investigación fue revisar lo pertinente a estándares de normalización técnica en materia de seguridad y revisar los mejores prototipos.

Escudero Almeida, Eric Emiro (2021), desarrollaron el trabajo de grado en Colombia denominado Red de alertas de eventos de seguridad basada en una arquitectura de Honeynet en IOT, centralizada y monitoreada por un sensor auto-configurable. se trabajó en la construcción de una arquitectura Honeynet, integrando dos componentes principales, servidor y sensor auto-configurable, ambos se diseñan y crean como prototipos para utilizarlos en las redes IoT, usando tecnologías disponibles en el mercado como lo son los dispositivos embebidos en IoT (Raspberry Pi), que conlleve a que cuando un atacante intente ingresar a la Honeynet, esta le responda de manera automática activando o no servicios que un atacante pueda ver atractivos (auto- configurando nuevos servicios), permitiendo a los oficiales de seguridad obtener mayor información y eficiencia en los resultados del aprendizaje.

La relación que guarda con el presente trabajo es la selección de teorías, técnicas y tecnologías utilizadas para resolver problemas en seguridad tecnológica mediante la implementación de esquemas con herramientas de punta y última generación.

Contexto de la Institución Objetivo

Instituto Universitario de Tecnología de Valencia

La reseña histórica del IUTVAL, establece que es una Institución de educación superior, dependiente del Ministerio de Educación, adscrito a la D.G.S.E.S., creado por disposición del Ejecutivo Nacional, según Decreto Presidencial N°. 1977 y publicado en Gaceta Oficial N° 31.140 de fecha 21/12/76. Como Institución que integra el sistema educativo superior del país, se inspira en un definido espíritu de democracia, justicia social y solidaridad humana y estará abierto a todas las corrientes del pensamiento universal en la búsqueda de la verdad, los cuales se investigarán y se divulgarán, con rigurosa objetividad científica, de acuerdo a las políticas fijadas en los planes de la Nación a fin de lograr el desarrollo humano imprescindible para la región carabobeña y el país.

El instituto, se rige por el Reglamento interno vigente que regula su estructura y funcionamiento, así como también por los Reglamentos y Leyes que norman a las Instituciones de Educación Superior. Es una organización de Servicios educativos de formación de profesionales Técnicos Superiores Universitarios, Licenciados e Ingenieros en las áreas de Informática, Química, Procesos Industriales y Electricidad.

Según el Manual de Procesos de la Organización, su misión es:

> "Promover el desarrollo del país en general y de la Región Central en Particular, a través de la formación de profesionales de alta calidad, capaces de actuar efectiva y eficientemente en las actividades profesionales, sociales, económicas y culturales de la sociedad." (p.5)

De igual forma, en la visión indica:

> “La búsqueda y transmisión de conocimientos mediante la investigación, creación y divulgación de conocimiento, participa continuamente en las discusiones y toma de decisiones involucradas con el progreso social, cultural e intelectual de la Región Central y colabora con los diferentes sectores económicos y sociales de nuestro entorno en beneficio de su desarrollo, defiende y promociona los derechos humanos, la justicia social y la dignidad de las personas, dentro de los principios de tolerancia, respeto y libertad.” (p.5)

Para cumplir con su misión y visión, es considerada como una universidad territorial.

La visión sistémica de la organización. (Ver Gráfico 1)

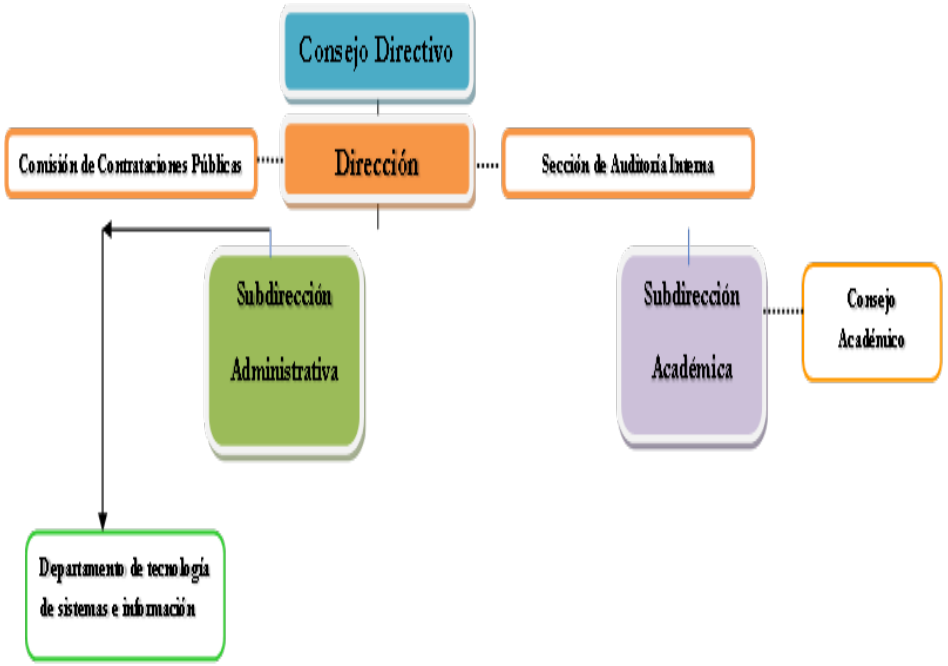


Gráfico 1. Organigrama del IUTVAL.
Fuente: Página Web; Adaptación: Autora (2021)

Departamento de Tecnología de Sistemas e Información.

En palabras del Manual de Normas y Procedimientos (2013):

> “Es el órgano técnico de nivel táctico decisorio, adscrito a la Dirección del Instituto, encargado de planificar la adquisición, la asignación y el mantenimiento de los recursos informáticos, así como de organizar, supervisar y controlar el uso de los mismos, los programas de entrenamiento y el apoyo logístico informático y temático a la gerencia, Hardware y Software) en las actividades administrativas y académicas del Instituto”. (p.25)

El organigrama funcional de dicho Departamento se aprecia a continuación

Gráfico 2: Organigrama del Departamento de Tecnología de S.I.
Fuente: Manual Normas y Procedimientos IUTVAL (2013); Adaptación: Autora (2021)

La Oficina está integrada por el Jefe, designado por el Director, su Secretaría respectiva y dos Secciones: Tecnología e Información (Sección de Páginas WEB, Sección Redes y Telecomunicaciones, Sección de Sistema Unificado de Gestión Administrativa Universitaria (SUGAU), Sección de Soporte Técnico, sección de Desarrollo y Administración y sección de Control de Acceso.

Entre las funciones más importantes que presenta la Dirección de Informática se tienen las siguientes:

- Desarrollar actividades de planificación, organización, dirección y control, de los procesos inherentes a su área, a través de las dependencias a su cargo.

- Dirigir, supervisar y evaluar la formulación de las políticas de seguridad y su mantenimiento, así como la elaboración de las normas y procedimientos inherentes a la Dirección a su cargo.

- Dirigir, supervisar y evaluar la formulación y reporte de indicadores de gestión, cumplimiento de las metas y calidad de los servicios o productos.

- Diseñar, ejecutar y evaluar, los proyectos y planes integrales (Arquitectura e Ingeniería) para el crecimiento, modificación y mejoras de la infraestructura tecnológica y el entorno, conforme a los lineamientos y políticas de regulación de uso, ordenamiento y asignación de espacios de la Universidad.

- Diseñar y elaborar los Planes de ordenamiento tecnológico y de sus implicaciones, siguiendo los lineamientos emanados por la Oficina de Planificación del Sector Universitario (OPSU).

- Planificar, supervisar y evaluar las actividades necesarias para generar políticas y estrategias en materia de seguridad técnica y su mantenimiento en la Universidad.

- Articular acciones tendientes a fortalecer las condiciones y medio ambiente de trabajo en concordancia con lo establecido en la Ley que rige la materia de telecomunicaciones e informática.

- Presentar al Comité de Contrataciones toda la documentación técnica y económica relativa a obras, mantenimiento o servicio a contratar en su ámbito técnico.

- Elaborar el Anteproyecto y Proyecto de Plan Operativo y Presupuesto Anual de la Universidad, en cuanto a la formulación de los productos que se

contemplen en las distintas acciones específicas contenidas en Proyecto Presupuestario que le corresponda.

- Velar por el cabal cumplimiento de las normas y procedimientos que rige la materia de su competencia y evaluar permanentemente los resultados de su aplicación.

- Mantener relaciones con los organismos nacionales e internacionales, públicos y privados, a objeto de lograr intercambios que favorezcan el desarrollo y la realización de estudios y demás actividades institucionales, en el campo de la tecnología, telecomunicaciones y afines.

- Las demás que le sean asignadas por los Reglamentos y las Autoridades competentes.

2.2 BASES TEÓRICAS

Teoría de Gestión de Cuadro de Mando Integral (CMI) y Árbol Estratégico

El modelo que en propuesta de Kaplan y Norton (2000), es: “The Balanced Scorecard”, o “Cuadro de Mando Integral «CMI», mueve el piso cognitivo de actores y biosocioescenarios del contemporáneo hacer gerencial, en lectura de sustentabilidad, encarando el riesgo e incertidumbre, ante el mandato jurídico del control del aparato público u oficial. En estos criterios, con adaptación en aspectos puntuales del CMI, se viabiliza que desde cada cargo o puesto de trabajo en el entorno interno institucional, se signe la gestión gerencial estratégica, a saber del siguiente gráfico descriptivo:

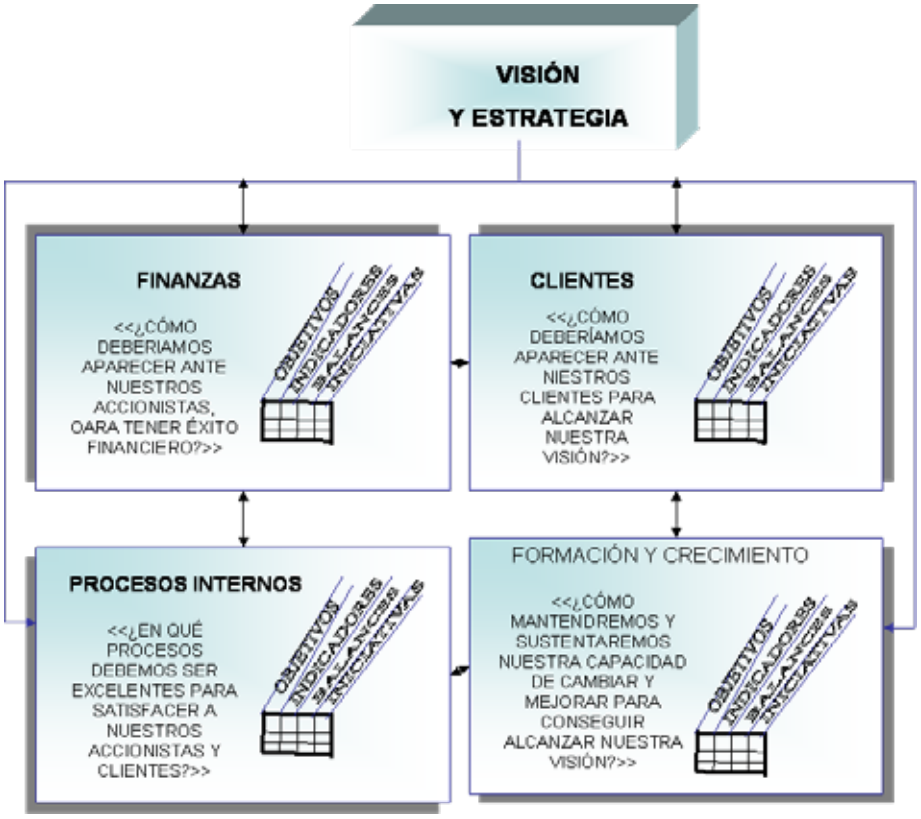


Gráfico 3: Perspectivas del Cuadro de Mando Integral o CMI «The Balanced Scorecard». Fuente: Cuadro de Mando Integral. Medición y gestión en la era de la información. (Elaborado según datos de Kaplan y Norton, 2000, p. 22). Adaptado por Briceño (2021).

Así, es pertinente, profundizar, en planteamientos propuestos por tan diversas tendencias, enfoques y teorías; para dimensionar sus reales posibilidades y factibles prospectivas, para ser implantada en el complejo ámbito de los cinco poderes públicos en la actual V república venezolana, de dilatada trayectoria en el mapa nacional e internacional, quien en su historiográfica existencia, en resguardo del Archivo de la Nación, reposan en Memorias y Cuentas de su historia de vida, ahora memoria tecnológica de generaciones actuales y por venir. A ese tenor, el gráfico 4 define la magnitud de lo que significa el CMI a una gerencia con criterio altamente efectivo, y que se adapta a una actualidad.

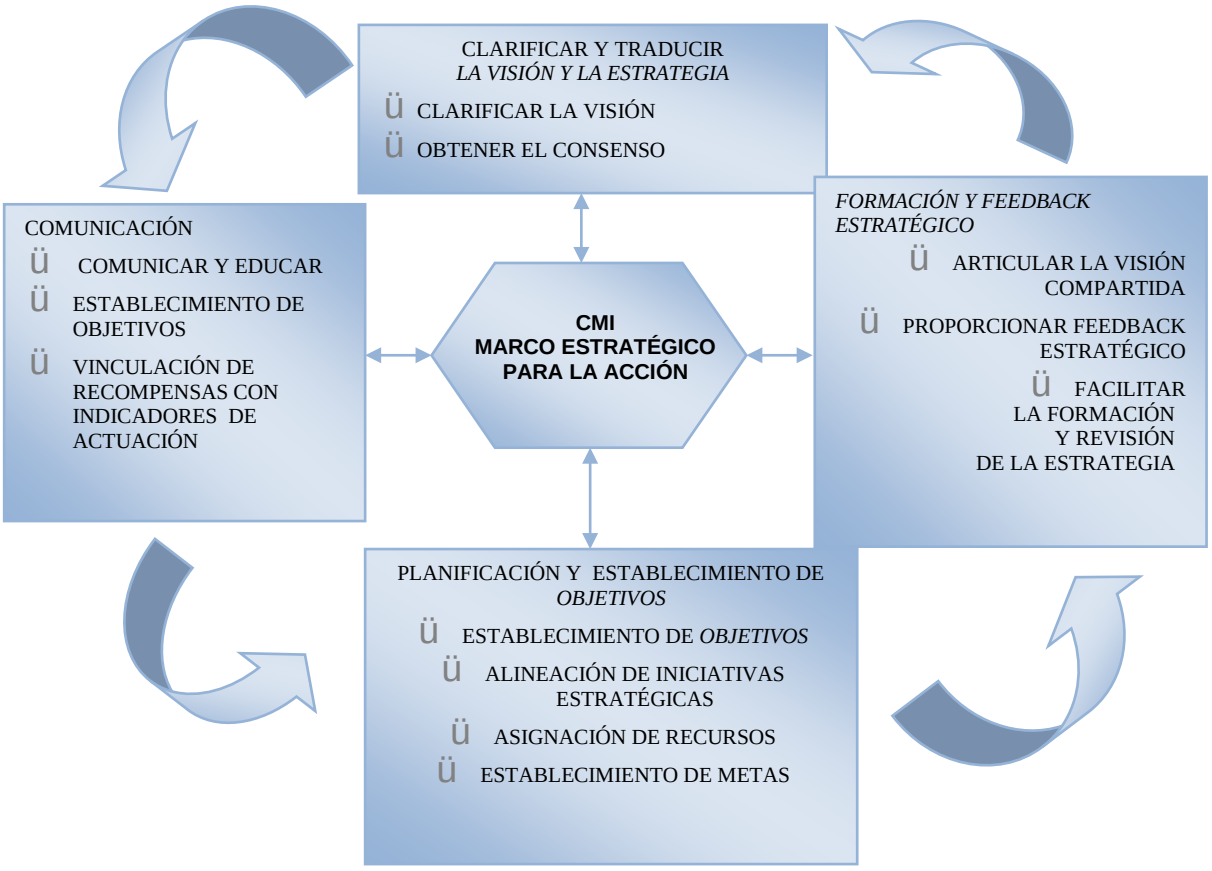


Gráfico 4: Cuadro de Mando Integral: Estructura o Marco Estratégico para la Gestión
Fuente: Sistémica medición y gestión organizacional en la era de la información. (Elaborado con base en datos de Kaplan y Norton, 2000, p. 24). Adaptado por Briceño (2021).

Para ampliar el enfoque del CMI, se asume el enfoque de Francés (2006), cuando en su obra: Estrategia para la empresa en América Latina; en el aparte que refiere al: "Árbol estratégico y Cuadro de Mando Integral" (Capítulo 4, pp. 101-122), describe la relación entre los diferentes niveles de estrategias presentes en una organización: empresa corporativa, de negocios y funcional del Cuadro de Mando Integral (Balanced Scorecard). En ese criterio, el citado autor, hace énfasis, que por definición, la estrategia corporativa se refiere a la organización en su conjunto y no de alguna de sus partes. Así, los componentes de esta estrategia es de diversificación, constituida por: estrategia de portafolio, estrategia horizontal y estrategia vertical. La estrategia de negocios, es en particular la Unidad de Negocio (UEN), y se define dentro del marco de la

estrategia institucional. La estrategia de negocios se refiere a la forma como puede competir una UEN con sus rivales. La estrategia competitiva es aplicable según sea el tipo de integración que posea la organización. Las estrategias funcionales, se aplican a cada función «cargo o puesto de trabajo» dentro de la UEN.

En la vinculación con Lineamientos Estratégicos con el CMI, Francés (op cit), indica la evolución teórica del CMI, como herramienta propuesta por Kaplan y Norton (op cit, en: 1996; 2000, 2001), y prolífica aceptación en empresas consultoras y en general en los medios gerenciales, para formular estrategias y evaluar el desempeño de la UEN. En su enfoque, presenta cuatro perspectivas, la de: accionistas, clientes, procesos internos y aprendizaje-crecimiento. Reseñando que en cada perspectiva: "… se establecen objetivos, variables o indicadores (measures), metas (targets) e iniciativas o proyectos de intervención (initiatives).". (p. 103).

Además, para ampliar la exégesis de su enfoque, Francés (op cit), indica que el CMI, adopta el nombre *Balanced Scorecard*, porque trata de establecer un balance entre variables de orientación externa, que per se, son cardinales para los accionistas y clientes; y en ese foro, de las variables de orientación interna, relevantes: a procesos de negocio, innovación, aprendizaje-crecimiento. A la par, el CMI busca balance entre medición de resultados, que reflejan el desempeño pasado y medición de variables-indicadores que determinan el desempeño futuro. También, comprende tanto variables cuantificables objetivas como variables de naturaleza subjetiva.

En criterio de Francés (op cit), el punto de partida para definir el CMI de una institución, lo constituye la visión que describe los logros a alcanzar en el largo plazo -habitualmente diez años-. Mientras que el destino estratégico (*strategic destination*) es un concepto del CMI, que representa objetivos temporales a ser alcanzado como logro en el mediano plazo -tres o cinco años-. De hecho, la visión se define a partir de los fines, valores y misión. Planteando

que los fines están relacionados con la perspectiva de los accionistas, mientras que la misión lo está con la de los clientes.

Desde esos referentes, con base en tradicionales teorías administrativas e innovadas tendencias, el desempeño laboral, en su pertinencia con el CMI vinculará otra serie de factores clave del entorno interno organizacional, al considerar cómo han evolucionado esas teorías y hasta dónde cada estructura de la organización interpreta lo que prescriben las taxativas normas jurídicas e institucionales endoexógenas, además de los aportes de las ciencias en su pluridisciplinaridad, y los incontenibles e inconmensurables adelantos de tecnologías emergentes, porque en su conjunción todos coadyuvan «o deberían» optimizar el ideario de desarrollo sustentable, sostenible perdurable para todas las organizaciones intelectual o en manufactura productiva, porque en representación de la sociedad venezolana el Estado suscribió en la 1ª Cumbre de la Tierra ONU-Rio-2002, y ponderada en Paris en 2016. De sí, la gestión es para que sin excepciones o exclusiones, todos los sectores de la vida pública nacional que per se, constituyen la sociedad, alcancen con satisfacción, prestigio, imagen y éxito sus metas, para bien común y beneficio de todos.

Planificación Estratégica Organizacional

Para Kabboul (S/f), planificar es:

> "... un proceso continuo y sistemático de tomar decisiones anticipadas sobre cursos de acción futura...". De allí que en su concepto: "... La Planificación Estratégica es el proceso continuo y dinámico de interpretación del entorno, evaluación de la naturaleza del negocio, con el propósito de definir objetivos y formular estrategias a largo plazo que permitan alcanzar la visión deseada..."; diferenciándola del Plan Estratégico, que es: "... el producto final que surge a raíz de todos los esfuerzos de planificación estratégica...". (p. 11).

De esta manera, si la planificación está dirigida al diseño e implantación de mejoras, y va más allá del mantenimiento preventivo que la administración

tiene estipulado dentro de su sistema productivo; es por lo cual, esas acciones se refieren a un proceso de reingeniería, que redimensiona tanto la recreación de aprendizajes existentes y su yuxtaposición con la normativa jurídica e institucional jerárquico del ordenamiento vigente, además primordialmente, establece los puntos de adquisición de habilidades tecnológicas a fin de garantizar los factores que inciden en la mediación y construcción de aprendizajes significativos de la acción productiva de la planeación, imprescindible al efectivo desempeño del talento humano.

Igualmente, Kabboul (op cit), define los niveles de planificación que se requiere en la serie de decisiones, se representan en la adaptación operacionalizada, según el mismo autor a continuación en el gráfico 5.

Gráfico 5: Niveles de Planificación. Fuente: Kabboul. (Guía de Planificación Estratégica, Mimeo S/f, p. 13). Adaptación: Briceño (2021).

Mientras que Páez (1994), Al respecto, expresa:

> "... Coexisten dos modelos de planificación: de un lado, la planificación normativa que fundamentalmente se implantó en el sector público, y del otro, los modelos de planificación

> estratégica que se implantaron en las grandes empresas del Estado…" (p. 51).

En sus aportes Molins (1991), indica el término planificación como: "...La gestión implica dirigir el funcionamiento y desarrollo de un sistema o conjunto de sistemas y por extensión, de una organización…". (p. 38). Otros reseñan: "*Dinámica de la Planificación*", donde los enfoques están en: "*Fases y/o Etapas*" a la "*Estrategia Organizacional*". Por lo pertinente a esquemas de planificación, del texto de compilación del citado autor, a saber:

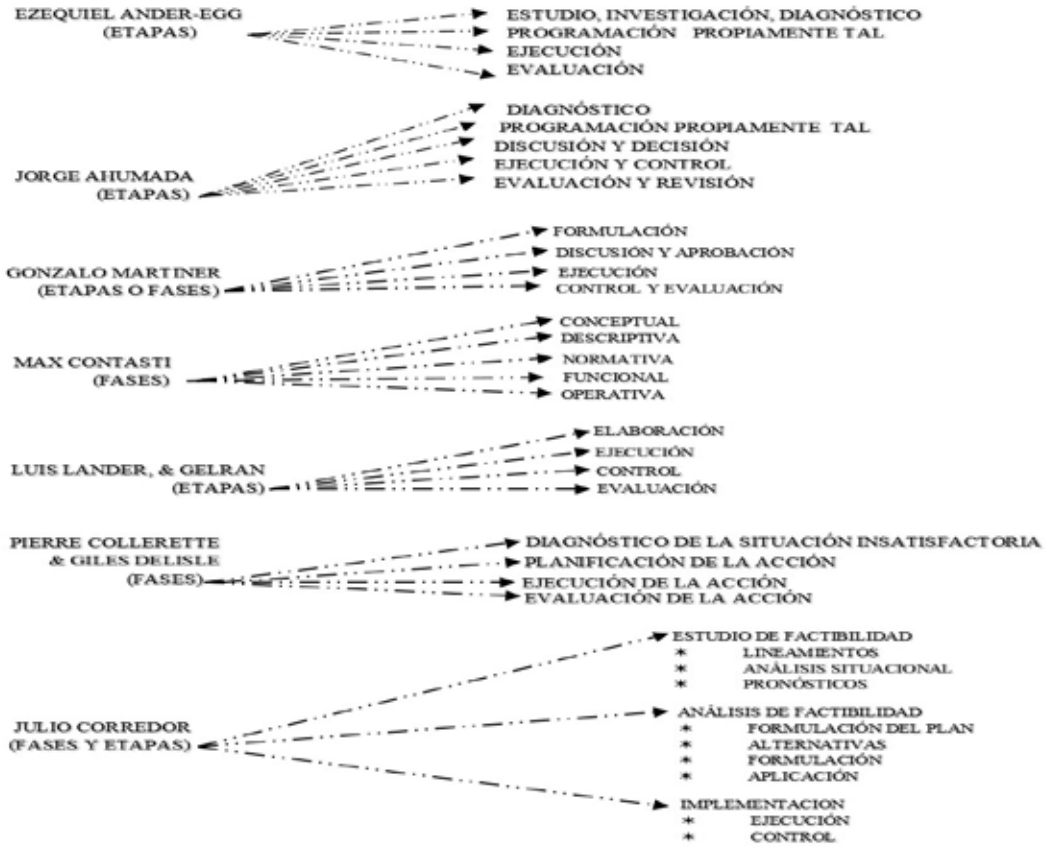


Gráfico 6 Esquemas de Planificación.
Fuente: (Molins, 1991 p. 42). Adaptación Briceño (2021)

Por su parte Steiner (1986), enuncia:

> "... la planificación estratégica formal se ha ido perfeccionando al grado que en la actualidad todas las compañías en el mundo cuentan con algún tipo de sistema, y

> un número cada vez mayor de empresas pequeñas está siguiendo este ejemplo". (p. 8).

Procesos de Gestión relevantes

Para Zacarías (1992), la producción ha de responder al trabajo intelectual, así plantea: "... planeando la labor antes de empezarla, esto es- estudiando: ¿Qué trabajo se hará, Como se hará, Dónde se realizará y cuándo se ejecutará?...", (p. 12). En esa preparación previa es aplicable al sistémico proceso la definición cuando expresa:

> ... La técnica de prever o imaginar de antemano cada paso de la larga serie de operaciones separadas, teniendo que efectuarse cada una con la máxima eficiencia, e indicar cada paso de manera que las disposiciones de rutina basten para que se realice en el lugar adecuado y momento oportuno... (p. 80).

Para fortalecer competencias del talento humano, el plan tiene como objeto expresar innovadora y sistemáticamente las opciones elegidas para asegurar su desarrollo; esto implica en primer lugar -una inversión económica- como expresa Lambin (1997), al referirse a la estructura del plan estratégico, indica: "... un plan estratégico es en definitiva, un plan financiero a mediano y largo plazo..." (p. 570). Así, es preciso considerar, componentes de esas innovaciones, a saber de su texto:

> *... una innovación puede descomponerse en tres elementos:*
> - Una ***necesidad*** a satisfacer, dicho de otro modo, una función o un conjunto de funciones a cumplir.
> - El ***concepto*** de un objeto o de una entidad idónea para satisfacer las necesidades, es decir; la idea nueva.
> - Unos ***ingredientes*** (inputs) que comprendan tanto un cuerpo de conocimientos preexistentes como de materiales o una tecnología disponible que permita hacer operativo ese concepto...

- … la gestión de innovación estratégica, va depender de **factores de riesgo**:
- **El riesgo de mercado**: grado de originalidad del concepto y su complejidad, que van a determinar la receptividad del mercado y el coste de transferencia para el usuario...
- **Riesgo tecnológico**: grado de innovación de la tecnología utilizada en relación con el concepto que va determinar la viabilidad técnica de la innovación...
- **El riesgo estratégico**: grado de novedad para la empresa, el grado de familiarización con el mercado y la tecnología... (p. 362).

De esta manera, la relevancia de un plan de mejoras, parte de la relación que se establece «en lo que se refiere a la Gestión Tecnológica» con enfoque en acciones para optimizar la productividad laboral del Servicio Público Educacional, a través de un plan estratégico en GST; así como también por el enfoque que en materia de calidad de producción exponen expertos y ONG's mundiales-nacionales, implica la continuidad y aplicabilidad temática, en los procesos sistemáticos que cualquier organización (especialmente en el caso-educativo).En este orden, el plan estratégico se concibe cimentado en factores clave a ser realizado por el ente planificador, como :

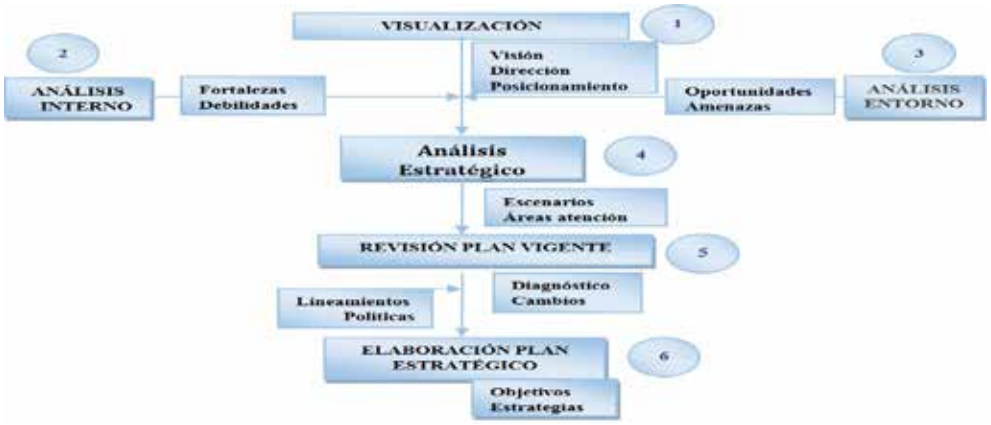


Gráfico 7 Flujograma de Proceso en Planificación Estratégica.
Fuente: Kabboul (op cit, p. 8). Adaptación Briceño (2021).

Otro elemento es lo que se refiere al desempeño de las actividades planificadas en Seguridad tecnológica, sea para evaluar el desempeño en su ejecutabilidad, o por las reducciones o la no ejecutabilidad por factores de

asignación presupuestaria, que como se indicó, dependen de la centralizada decisión de órganos y entes exógenos al campus universitario público, así lo usual es ajustarse, adaptándose -si fuera necesario-a no asumir medidas correctivas, y sí, diagnosticando, en qué medida las organizaciones universitarias vinculadas con la asignación de recursos por la Administración Pública nacional y centralista, sea que le consignen o no los aportes que plantean sus metas y que no se emprenden por sus ausencias para sostener u optimizar el desempeño de la requerida infraestructura, lo cual también tiene por objeto, obtener la especialización de las funciones y separación de poderes, coordinando y unificando actividades posibles, al sustentable de desarrollo de la cultura para todos en la complejidad del desempeño en Seguridad tecnológica, como universal mandato al derecho educativo.

Definiciones Clave en asuntos de Seguridad Tecnológica

Necesidades de seguridad en la tecnología

Según Villasmil F. (2006): la seguridad de tecnologías de la información en el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La información se encuentra de diversidad de formas y maneras o en diversos medios y no solo en los informáticos, no obstante, hay dos términos que podrían relacionarse, pero no entrar en confusión; tales conceptos son los de “seguridad de la información” y “seguridad informática”.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores.

Según Ferro (2020): “nadie a cargo de seguridad debe determinar quién y cuándo se puede tomar acciones apropiadas sobre un ítem en específico”. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización a organización. Independientemente, cualquier compañía con una red debe de tener una política de seguridad que se dirija a conveniencia y coordinación.

Políticas, Objetivos y puesta en marcha de Seguridad de la Información.

Las políticas de seguridad representan los documentos en donde se establecen las normas a seguir para realizar conexiones a la red inalámbrica de la empresa. Asimismo, las políticas de seguridad tendrán un alcance desde el punto de vista de seguridad de los datos que viajan a través de una WLAN, describiendo las responsabilidades y derechos de usuarios que operen y utilicen las redes inalámbricas de la empresa; estos documentos son el primer paso en la construcción de arquitecturas de seguridad efectivas y son considerados parte fundamental del esquema de seguridad efectivo.

El diseño de políticas de seguridad debe realizarse considerando que no disminuya la capacidad operativa de la organización. La existencia de políticas que impidan que usuarios cumplan sus tareas efectivamente, puede tener consecuencias indeseables ya que usuarios podrán encontrar formas de ignorarla y convertirla en algo inútil. Para que las políticas de seguridad de redes inalámbricas sean efectivas, los usuarios deben aceptarlas y estar

dispuestos a reforzarlas. En términos generales, se tiene que lograr que las políticas de seguridad cumplan con todos los servicios de seguridad: autenticación, confidencialidad, integridad, no repudiación, disponibilidad de los recursos a personas autorizadas y control de acceso.

Debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos entre los que se encuentran los siguientes:

- La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- La información: es el principal activo utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Por ejemplo, se puede tener el caso de España, país que posee una Ley Orgánica llamada “LOPD” cuya función es Protección de datos a personas naturales y en su normativa de desarrollo, protege ese tipo de datos estipulando medidas básicas y necesidades que impidan la pérdida de calidad de la información o su robo. También en ese país, ha establecido medidas tecnológicas de Seguridad dentro de su Esquema Nacional para permitir que los sistemas informáticos que prestan servicios a los ciudadanos cumplan con unos requerimientos de seguridad acordes al tipo de disponibilidad de los servicios que se prestan.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales

tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

Amenazas y sus tipos para las Redes Informática.

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tomadas en cuenta e incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo, mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad. Las amenazas pueden ser causadas por: Usuarios, Programas maliciosos, errores de programación, intrusos desde afuera o personal interno, siniestros o catástrofes y fallas eléctricas.

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella y con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo, el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas.

Generalmente las amenazas internas son por varias razones como:

- Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además, tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
- Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

El tipo de amenazas por el efecto, que causan a quien recibe los ataques podría clasificarse en:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
- Robo de dinero, estafas.

Finalmente, se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

- Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.

Los virus pueden destruir, de manera intencionada, los datos almacenados en un computador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

- Phishing.
- Ingeniería social.
- Denegación de servicio.
- Spoofing: de DNS, de IP, de DHCP, etc.

Los ataques están cambiando, si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

Tipos de Intrusos y ataques en la Redes Informáticas.

Existen diferentes tipos de ataques en Internet como virus, troyanos u otros, dichos ataques pueden ser contrarrestados o eliminados, pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como “el eslabón más débil”. Dicho ataque es capaz de conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de suplantación de identidad bajo un término que derivado del inglés “fishing “se transforma en

“phishing”, puede llegar a robar la contraseña de un usuario de una red social para un posterior acoso o fraude electrónico, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma (sin que deje de ser delito en ambos casos, al menos en países con legislación para el caso, como lo es España).

Análisis de Riesgos Informáticos.

Los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia de riesgos, se conocen como un proceso que comprende la identificación de activos informáticos, sus peligros y debilidades a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, o dicho de otra forma es analizar el riesgo informático.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

Elementos de un Análisis de Riesgo de una Matriz en las Redes.

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total, así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras.

La fórmula para determinar el riesgo total es:

RT (Riesgo Total) = Probabilidad x Impacto Promedio

A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el riesgo residual.

Análisis de Impacto en la Administración de Recursos.

El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver.

Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema.

Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor web público pueden poseer la característica de confidencialidad baja (ya que toda la información es pública) pero necesita alta disponibilidad e integridad, para poder ser confiable. En contraste, un sistema de planificación de recursos empresariales (ERP) es, habitualmente, un sistema que posee alto puntaje en las tres variables.

Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

Técnicas para Asegurar los Sistema Informáticos.

El activo más importante que se posee es la información y por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo. Cada tipo de ataque y cada sistema requiere

de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos).

A continuación, se enumeran una serie de medidas que se consideran básicas para asegurar un sistema tipo, si bien para necesidades específicas se requieren medidas extraordinarias y de mayor profundidad:

- Utilizar técnicas que cumplan con los criterios de seguridad al uso para todo el software que se implante en los sistemas, partiendo de estándares y de personal suficientemente formado y concienciado con la seguridad.
- Implantar medidas de seguridad físicas: sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.
- Codificar la información bajo los principios de la criptografía algebraica. Esto se debe realizar en todos aquellos trayectos por los que circule la información que se quiere proteger, no solo en aquellos más vulnerables. Por ejemplo, si los datos de una base muy confidencial se han protegido con dos niveles de firewall, se ha cifrado todo el trayecto entre los clientes y los servidores y entre los propios servidores, se utilizan certificados y sin embargo se dejan sin cifrar las impresiones enviadas a la impresora de red, tendríamos un punto de vulnerabilidad.
- Contraseñas difíciles de averiguar que, por ejemplo, no puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad. Las contraseñas, además, deben tener la suficiente complejidad como para que un atacante no pueda deducirla por medio de programas informáticos. El uso de

certificados digitales mejora la seguridad frente al simple uso de contraseñas.

- Vigilancia de red. Las redes transportan toda la información, por lo que además de ser el medio habitual de acceso de los atacantes, también son un buen lugar para obtener la información sin tener que acceder a las fuentes de la misma. Por la red no solo circula la información de ficheros informáticos como tal, también se transportan por ella: correo electrónico, conversaciones telefónicas de voz sobre IP, es decir a través de las redes (tecnologías IPV4 e IPV6), mensajería instantánea, navegación Internet, lecturas y escrituras a bases de datos, etc.
- Proteger la red es una de las principales tareas para evitar robo de información. Existen medidas que abarcan desde la seguridad física de los puntos de entrada hasta el control de equipos conectados, por ejemplo 802.1x. En el caso de redes inalámbricas la posibilidad de vulnerar la seguridad es mayor y deben adoptarse medidas adicionales.
- Redes perimetrales de seguridad o DMZ, permiten generar reglas de acceso fuertes entre los usuarios y servidores no públicos y los equipos publicados. De esta forma, las reglas más débiles solo permiten el acceso a ciertos equipos y nunca a los datos, que quedarán tras dos niveles de seguridad.
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos-antispyware, antivirus, llaves para protección de software, etc.
- Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

- Copias de seguridad e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.
- Controlar el acceso a la información por medio de permisos centralizados y mantenidos (conocida como técnica LDAP que significa activación por directorios de solo miembros para controlar los accesos a las redes para lo cual es preciso manejar un portal completo y complejo de servicios).
- Restringir el acceso mediante listas de control de acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro. y que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo, como se ha indicado más arriba, e incluso utilizando programa que ayuden a los usuarios a la gestión de la gran cantidad de contraseñas que tienen gestionar en los entornos actuales, conocidos habitualmente como gestores de identidad.

- Redundancia y descentralización.

Respaldo de Información en las Redes

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o *backups*. Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde el último *backup*). Es vital para las empresas elaborar un plan de *backup* en función del volumen de información generada y la cantidad de equipos críticos.

Hoy en día los sistemas de respaldo de información online, servicio de *backup* remoto, están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información derivando la necesidad del crecimiento de la copia de respaldo a proveedor del servicio.

Protección Contra Virus Informáticos.

Los virus son uno de los medios más tradicionales de ataque a los sistemas y a la información que sostienen. Para poder evitar su contagio se deben vigilar los equipos y los medios de acceso a ellos, principalmente la red.

Control del Software Instalado en los Equipos de Computación.

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la

procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Control de las Redes Informáticas.

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red solo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo *batch* puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

Protección Física de Acceso a las Redes

Independientemente de las medidas que se adopten para proteger los equipos de una red de área local y el software que reside en ellos, se deben tomar medidas que impidan que usuarios no autorizados puedan acceder. Las medidas habituales dependen del medio físico a proteger.

A continuación, en el siguiente punto se dará algunos de los métodos, sin entrar al tema de la protección de la red frente a ataques o intentos de intrusión desde redes externas, tales como Internet.

Redes Cableadas e Inalámbricas

Las rosetas de conexión de los edificios deben estar protegidas y vigiladas. Una medida básica es evitar tener puntos de red conectados a los equipos de hardware que “switchean” la red. Aun así siempre puede ser sustituido un equipo por otro no autorizado con lo que hacen falta medidas

adicionales: norma de acceso 802.1x, listas de control de acceso por MAC addresses, servidores de DHCP por asignación reservada, etc.

> Para las redes inalámbricas, Álvarez Y. (2006) expresa.
> "En este caso el control físico se hace más difícil, si bien se pueden tomar medidas de contención de la emisión electromagnética para circunscribirla a aquellos lugares que consideremos apropiados y seguros. Además se consideran medidas de calidad el uso del cifrado (WPA, WPA v.2, uso de certificados digitales, etc.), contraseñas compartidas y, también en este caso, los filtros de direcciones MAC, son varias de las medidas habituales que cuando se aplican conjuntamente aumentan la seguridad de forma considerable frente al uso de un único método."

La implantación de las redes inalámbricas está creciendo de forma sustancial gracias a la flexibilidad y movilidad que nos proporcionan este tipo de redes, también conocidas como "Wireless", siendo la mejor manera de proporcionar conectividad de datos sin necesidad de cablear; sin embargo, el grado de madurez conseguido no se corresponde con el nivel de seguridad aportado hasta el momento.

El funcionamiento de las redes inalámbricas se basa en el envío de información a través del aire y en forma de ondas de radio, pudiendo ser bastantes accesibles desde los límites externos de una organización, entre los cuales tenemos algunos de los grandes riesgos a los que se ven sometidas: Intercepción de datos, Inserción de usuarios y equipos de red no autorizados, Interrupción o negación del servicio reduciendo la calidad del servicio de WLAN.

Es por esta razón que la seguridad de la información de la empresa juega un papel significativo, sobre todo cuando las amenazas a que se ven expuestas las redes inalámbricas pueden afectar la información y la continuidad de las operaciones en las organizaciones.

Dado el planteamiento del problema y a la falta de seguridad en las redes que a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información, se hace necesario la identificación y corrección oportuna de las brechas de seguridad con riesgos significativos en la institución con relación a la red que dicha compañía implanta, así como el planteamiento de mecanismos y recomendaciones para fortalecer el esquema de seguridad.

2.3 BASES LEGALES

Desde la conceptuación de variables indagatorias de este estudio, está el hecho que lo normativo es materia del Derecho como disciplina las siguientes leyes:

Ley Orgánica de Telecomunicaciones:

Ley que da soporte jurídico desde el año 2011 (7 de febrero) por Gaceta Oficial No. 39.610 al área de las telecomunicaciones de la nación, servirá para regular la apertura de las telecomunicaciones en el país, reglamentando la transferencia de información entre los diferentes organismos, incluyendo las redes de datos (Redes de computadoras), a saber:

"Título I, Disposiciones Generales:

> **Artículo 4**.- Se entiende por telecomunicaciones toda transmisión emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos, u otros medios electromagnéticos afines, inventados o por inventarse. Los reglamentos que desarrollen esta Ley podrán reconocer de manera específica otros medios o modalidades que pudieran surgir en el ámbito de las telecomunicaciones y que se encuadren en los parámetros de esta Ley.

Título II, De los Derechos y Deberes de los Usuarios y Operadores.

Capítulo II, De los Derechos y Deberes de los Usuarios.

2. La privacidad e inviolabilidad de sus telecomunicaciones, salvo en aquellos casos expresamente autorizados por la Constitución o que, por su naturaleza tengan carácter público. “

Ley de Mensajes de Datos y Firmas Electrónicas:

Ley aprobada el 10-02-2001, en Gaceta Oficial No. 1.204 que apoya las transacciones a través de los formatos digitales, lo que permitirá desarrollar sobre bases legales, el comercio electrónico, la transferencia de datos entre organizaciones, el establecimiento de redes ínter empresariales, así como la comunicación efectiva entre organismos públicos y privados. Expresa:

“Capítulo I. Objeto y aplicabilidad del Decreto-Ley.

Artículo 1. El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y firmas electrónicas”

Ley Especial Contra Delitos Informáticos:

Este instrumento legal viene a fortalecer el auge de las comunicaciones y el desarrollo de las tecnologías de la información en Venezuela. En él se regula todo lo referente a sistemas informáticos y a los posibles delitos que se cometan haciendo uso de los mismos. Así, por ejemplo:

“Título I. Disposiciones Generales.

Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías

> de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley."

En esta ley el objetivo principal es proteger a los sistemas que utilizan tecnología de información, así como prevenir y sancionar los delitos cometidos contra el uso de esta tecnología, fue publicada según (gaceta oficial n° 37.3131 del 30 de octubre del 2001) en Venezuela actualmente se utiliza, para respaldar esta investigación y hacer ver con mayor claridad su importancia dentro de la realización de un reglamento de seguridad tecnológica en el área de la informática. Entre otros artículos de interés se encuentran:

> "**Artículo 6º** Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
> **Artículo 7º** Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.
> **Artículo 8º** Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.
> **Artículo 9º** Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí

> previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de uso restringido sobre personas o grupos de personas naturales o jurídicas.
> **Artículo 10º** Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos o dispositivos; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias."

Ley de Infogobierno

Esta ley promulgada por gaceta oficial No. 40.274 de fecha 17-11-2013, entro en vigencia y respalda los lineamientos a seguir en el uso de las tecnologías de la información a nivel nacional y a los órganos públicos y privados, además es de suma importancia ya que se toma en cuenta el aspecto social y al desarrollo integral de la nación. Dicha ley fue promulgada en el Palacio de Miraflores, en Caracas, a los diez días del mes de octubre de dos mil trece de conformidad con lo previsto en el artículo 213 de la Constitución de la República Bolivariana de Venezuela. Establece:

> "**Artículo 1**. Esta Ley tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación."
> **El artículo 5** Preveé las definiciones de términos como actuación electrónica, criptografía, infraestructuras críticas o estratégicas, seguridad de la información y se emplearan en este trabajo de grado según dicha ley. El artículo 55 versa

sobre la seguridad y las certificaciones electrónicas del software desarrollado al estado, los artículos 57 y 58 preeveen todo lo relacionado al uso de las técnicas matemáticas de criptografía y encriptamiento de códigos y claves, además de la protección de claves en los sistemas estratégicos del estado.

Los Estándares Normas ISO

la norma ISO 27001 (Organización Internacional para la Estandarización [ISO], 2013), contiene los diferentes objetivos de control y controles que las organizaciones deberían tener en cuenta para la planeación e implementación de su Sistema de Gestión de Seguridad de la Información, los cuales se describen con más detalle en la norma ISO 27002.

- **SO/IEC 27002.** Guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.
- **ISO/IEC 27003.** Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación.
- **ISO/IEC 27004.** Guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un Sistema de Gestión de Seguridad de la Información y de los objetivos de control y controles implementados de acuerdo al Anexo A de la norma ISO 27001
- **ISO/IEC 27005**. Esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerimiento que se deben tener en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.

- **ISO/IEC 27006.** Establece los requisitos relacionados en la norma ISO 27001 que deben cumplir las organizaciones para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27035.** Proporciona una guía sobre la gestión de incidentes de seguridad en la información

CAPÍTULO III

MARCO METODOLÓGICO

El marco metodológico de la investigación recoge fundamentalmente los pasos a seguir desde que se inicia el estudio hasta su culminación. La **metodología cuantitativa** según Martínez (1998), “es aquella que se dirige a recoger información objetivamente mesurable” (p. 63). Es de enfatizar que ese enfoque investigativo conceptualizado es el que prevalecerá en la presente investigación. Al respecto, parafraseando a Álvarez (1990), ha de señalarse que las técnicas cuantitativas de obtención de información requieren de apoyo matemático y permiten la cuantificación del resultado. Son utilizadas fundamentalmente para obtener datos primarios sobre todo de características, comportamientos y conocimientos. Otra característica importante en esta investigación fue el uso del procedimiento estadístico, como método deductivo predeterminado y estructurado enmarcado en el empirismo lógico positivista, el cual es el paradigma que rige este trabajo de grado.

Diseño, Tipo, Nivel y Modalidad de la Investigación

El Diseño de la presente investigación se planteó como una estrategia general que adopta la investigadora en su manera de asumir una problemática a resolver, lo cual se traduce en un esquema a seguir para efectuar los pasos de este estudio; siendo así en el presente trabajo de grado que se va a estudiar la viabilidad de soluciones técnicas institucionales al problema de la gestión de la seguridad tecnológica que existe en el IUTVAL y se asume un procedimiento bajo **enfoque cuantitativo** en su mirada ***NO EXPERIMENTAL*** la cual está

definida por Hernández, Fernández y Baptista (2006) como : “.. En un estudio no experimental no se construyó ninguna situación , sino que se observan situaciones ya existentes, no provocadas intencionalmente por el investigador..” (p.205).

La investigación no experimental es también conocida como investigación Ex Post Facto, término que proviene del latín y significa después de ocurridos los hechos. De acuerdo con Kerlinger (1983) la investigación Ex Post Facto es un tipo de “... investigación sistemática en la que el investigador no tiene control sobre las variables independientes porque ya ocurrieron los hechos o porque son intrínsecamente manipulables,” (p.269). En la investigación Ex Post Facto los cambios en la variable independiente ya ocurrieron y el investigador tiene que limitarse a la observación de situaciones ya existentes dada la incapacidad de influir sobre las variables y sus efectos (Hernández, Fernández y Baptista, 1991).

D´Ary, Jacobs y Razavieh (1982) consideran que la variación de las variables se logra no por manipulación directa sino por medio de la selección de las unidades de análisis en las que la variable estudiada tiene presencia, es por ello que se presenta al final del presente capitulo el cuadro de operacionalización de variables con sus dimensiones e indicadores como unidades de análisis para un posterior resultado descrito en el Capítulo IV del presente trabajo.

Los tipos de investigación, en palabras de Ávila se eligen de acuerdo al objetivo general y son siguiendo a Hurtado de Barrera (1996, 2007): exploratoria, descriptiva, analítica, comparativa, explicativa, predictiva, proyectiva, interactiva, confirmatoria y evaluativa. Es así como de acuerdo al objetivo general del presente trabajo, el cual es Construir un modelo de lineamientos estratégicos en seguridad tecnológica para la sustentabilidad de la gestión de Informática en el IUTVAL como institución formadora de capital social técnico; que se asume la actual indagación como una investigación de

tipo descriptiva, de manera que la búsqueda va dirigida a responder a las preguntas quién, qué, dónde, cuándo, cuántos (Borderleau, 1987). Las investigaciones descriptivas trabajan con uno o con varios eventos de estudio. En este tipo de investigación no se estudia relaciones causales entre los eventos ni se formulan hipótesis.

La **modalidad** de la presente investigación es un **proyecto factible**. Según el manual de la Universidad Pedagógica Libertador (2016), plantea que:

> "el proyecto factible, consiste en la investigación, elaboración y desarrollo de un modelo operativo viable para solucionar problemas, requerimientos y organizaciones o grupos sociales que pueden referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El proyecto debe tener el apoyo de una investigación de tipo documental y de campo o un diseño que incluya ambas modalidades" (p. 18).

Según Bavaresco (2006, p. 28) la **investigación de campo** se realiza en el propio sitio donde se encuentra el objeto de estudio. Ello permite el conocimiento más a fondo del problema por parte del investigador y puede manipular los datos con más seguridad.

Morales y otros (1999, p. 28), establece que en ese diseño de investigación el investigador se basa en métodos que permiten recoger datos en forma directa en la realidad donde se presentan, en el sitio de acontecimiento". Esta investigación es de campo debido a que se realiza en el IUTVAL la cual es una Institución Educativa de carácter público como Universidad y se acudió tanto a la Sede para recabar documentos, aplicar encuestas y observar in situ las dimensiones de acuerdo a los objetivos generales y específicos planteados en el primer capítulo del presente trabajo de grado.

Ahora bien en cuanto a su **profundidad o nivel es transversal** o transeccional ya que según Chávez Alizo (1994, p. 144) la investigación trasversal es el estudio que mide una vez la variable, se miden los criterios de uno o más grupos de unidades en un momento dado, sin pretender evaluar la

evolución de esas unidades. En este sentido Hernández, Fernández, Batista (2006, p. 208) la investigación trasversal recopila datos en un solo momento, en un tiempo único, su propósito es describir variables analizar su incidencia e interrelación en un momento dado.

Es trasversal puesto que la dimensión es temporal, o la cantidad de momentos en el tiempo en el cual se recolectan los datos, se hizo en un único momento y en un tiempo ideal. Se describen las variables y se analizaron en un momento dado, no se espera el desarrollo o la evolución de las variables de estudio.

Población y Muestra

En el ámbito del contexto/escenario del sector educativo universitario público que este trabajo amerita, contenido definido por Tamayo (2011), como: "… datos objetivos confrontados con la realidad.". (p. 172); realidad que para Arias (2012), requiere se obtenga desde lo accesible de la: "… población objetivo…", (p. 81), con base en la conceptuación que desde el problema, permite estructurar el registro informativo a través de objetivos, variables e indicadores, que en su operacionalización guían el constructo teórico y metódico en el planeamiento al proceso indagatorio.

Para efectos de la investigación se considerara una población constituida por nueve (9) individuos o sujetos tipo, intencionalmente escogidos por su carácter de representación dentro de la gerencia y gestión de funciones en el reseñado objeto estudio, ya que son los miembros del personal de la Dirección de Informática, de acuerdo a la estructura funcional del IUTVAL considerando que dicha estructura contempla 4 secciones: Redes, Soporte, Desarrollo, Plataforma educativa.

De esta manera la encuesta se aplicará, en la búsqueda de las opiniones de funcionarios públicos que poseen inherencia en la toma de decisiones en las diferentes funciones, vinculadas con procesos de Proyectos, Construcción, Adecuación, Mantenimiento y Servicios tecnológicos que todos pueden ser

afectados por la poca o mucha seguridad tecnológica de la que se disponga. De allí que la población asumida a la compilación de datos in situ, sean los funcionarios responsables de la distintiva estructura organizacional con atribuciones gerenciales en seguridad tecnológica en toda las Sede del IUTVAL, al ser asumida como Universidad Pública, Formadora de profesionales en carreras técnicas.

Desde el precedente enfoque de población, el criterio de muestra conceptuada para este estudio, es la consulta de campo o in situ, al optar por la muestra sustentada en foros estadísticos de tipo: *no-probabilístico*, (Ramírez, op cit, p. 106), asumiéndola como muestra: *intencional*, *finita*, *estratificada*, *heterogénea*, en encuesta con nueve (9) funcionarios administrativos, los cuales todos se deben involucrar con la gestión de seguridad tecnológica en su unidad natural de desempeño. Se seleccionó en consecuencia una muestra censal, definida por Ramírez (2006) como: "Aquella donde todas las unidades de investigación conforman el total de encuestados".

A ese propósito la indagación en campo, metodológicamente, en la nominación, delimitación y consulta con unidades de medida, reseñan la alternativa de: "… sujetos…" Manual UPEL p. 34; "… tipo…" Ramírez, op cit, p. 121; y, "… sujetos tipo…" Hernández, et al, op cit, p. 328. Por lo cual, el criterio de la muestra de población asumida como fuente primaria, competente para suministrar datos relevantes a la temática, es el reseñado descriptor sujeto tipo.

Por ende, la indagación en campo o in situ, será con los funcionarios responsables de la estructura organizacional denominada Dirección de Informática como garantes de la seguridad tecnológica en el IUTVAL, según descripción reseñada en el apartado contexto de la Institución objetivo del Capítulo II del presente Trabajo de Grado.

Instrumento y técnicas a la compilación de Datos

A los fines de sustentar el diagnóstico situacional del problema, como camino estratégico de enunciación de recomendaciones posibles, El tipo de instrumento que se seleccionó para recolectar los datos fue el cuestionario escrito, en la técnica encuesta por ser esta una de las técnicas que más se aplica para recoger y almacenar información en investigaciones descriptivas. Hayman (1996), define la encuesta: "...conjunto de técnicas de investigaciones mediante el cual los sujetos proporcionan información acerca de sí mismo en forma activa.". Con respecto al cuestionario escrito, Chávez (1994), los define como "... el conjunto de preguntas respecto a una o más variables de medir". (p.166).

En las ciencias sociales un cuestionario escrito de uso amplio por su escala psicométrica puede expresar actitudes, según Allport (1968) la actitud se establece como el vínculo existente entre el conocimiento adquirido de un individuo sobre un objeto y la acción que realizará en el presente y en el futuro en todas las situaciones en que corresponde; siendo así y teniendo a su predecesor Rensis Lickert (1932) quien público su método de evaluaciones sumarias al uso social o comúnmente denominada Escala de Lickert, se emplea dicha técnica de Lickert, para especificar el nivel de acuerdo o desacuerdo con una declaración (elemento, ítem o reactivo o pregunta).

Siguiendo ese modelo para esta investigación, el Instrumento fue diseñado en escalamiento tipo Likert, consistente en el planteamiento de trece (13) ítems, contentivos de "juicios o afirmaciones" que buscan "la reacción" del informante consultado. (Hernández, et al, op cit, p. 369). A ese tenor, cada ítem es contentivo de cinco (5) opciones a la selección de una «a cada opción se le asigna un numeral para calcular la confiabilidad del instrumento», según la alternativa: Muy De Acuerdo (5-**MDA**), De Acuerdo (4-**DA**), NI de acuerdo NI en desacuerdo (3-**NINI**), En Desacuerdo (2-**ED**), Muy En Desacuerdo (1-**MED**).

Se puede apreciar el instrumento en el Anexo A

Validez del Instrumento

La Validez es definida por Stefano, V. (2000):

> "Se refiere al grado en que un instrumento realmente mide la variable que pretende medir. Para determinar esta característica pueden tenerse en cuenta diferentes tipos de evidencias relacionadas con el contenido, el criterio y el constructor, entre otras; el investigador debe seleccionar el tipo o los tipos de validación que más le convengan, previa documentación en las fuentes de metodología…La validez de contenido se determina antes de la aplicación del instrumento sometiendo el mismo al juicio de expertos (profesionales relacionados con la temática que se investiga), se requiere un número impar de expertos, mínimo tres (3). Una vez se obtenga la evaluación de los expertos, se procede a contrastar las opiniones con respecto a cada ítem; se aceptará como válido el criterio de la mayoría y se deberán modificar aquellos ítems en donde el criterio que predomine sea el de mejorar o cambiar algún aspecto de los mismos". (p.51).

Para Hernández (et al, op cit), la: "Validez, se refiere al grado en que un instrumento mide la variable que pretende medir". (p 349). En cuanto a la validez del sondeo de opinión con sujetos tipo, con anuencia tutorial, se obtiene el juicio de expertos en: Gerencia Educacional, Administración y Metodología de Investigación; a los cuales, para obtener la pertinente Certificación, se les suministró la matriz de ponderación, la cual fue debidamente suministrada y se evidencia en el Anexo B.

Confiabilidad del Instrumento

La confiabilidad del instrumento se refiere al grado que su aplicación repetida al mismo objeto estudio produce iguales resultados. En esos parámetros, para determinar la confiabilidad del instrumento de compilación de datos se utilizará el cálculo del Coeficiente de la Ecuación Alfa de Cronbach,

porque requiere de una única administración de la encuesta y produce valores que oscilan entre 0 y 1. Su ventaja reside en que no es necesario dividir en dos mitades los ítems del guión, sólo se aplica a «investigación transversal o transeccional: un sólo momento a un mismo efecto», y de sus resultas se calcula el coeficiente *a*. (Hernández et al, op cit, p. 354).

Se asume su estadígrafo, para el cálculo. De allí que la Ecuación, es transcrita a continuación:

Por ello, detalle de cálculos realizados con Microsoft Excel ®, se indican con los resultados obtenidos de la Confiabilidad

procesamiento, que consiste en tabular estadísticamente datos obtenidos, para en gráficos porcentuales y cuadros de frecuencia, presentar resultados, analizándolos e interpretándolos como resultados obtenidos en campo dentro de su conjunción con la analogía o no de teorías o tendencias obtenidas desde la estrategia referencial señalada en el marco teórico.

Etapas de la Investigación

La UPEL (2016) establece las siguientes etapas de investigación para un proyecto factible: “diagnóstico, planteamiento y fundamentación teórica; procedimiento metodológico, actividades y recursos necesarios para su ejecución; análisis y conclusiones sobre la viabilidad y realización del proyecto” (p.21).

Etapa 1: Diagnóstico:

En el capítulo I, se diagnosticó el problema describiendo la problemática observada, la cual originó la necesidad de reformular estrategias

Etapa 2: Fundamentación Teórica:

En el capítulo II, se mostraron los antecedentes relacionados a la investigación, lo cual permitió orientar y aportar conclusiones valiosas para la investigación. Asimismo, se realizó un arqueo de las teorías relacionadas con la variable de estudio, deduciendo a través de ellas, las dimensiones e indicadores medidos en el estudio.

Etapa 3: Procedimiento metodológico:

A través de esta etapa, se determinó el tipo, diseño y modalidad de investigación; se estableció la población y la muestra a estudiar; posteriormente se diseñó un instrumento validado por expertos, el cual consta de 12 ítems que midieron las dimensiones y los indicadores establecidos en la operacionalización de variables. El instrumento fue aplicado a una muestra censal de 9 profesionales universitarios en el ejercicio de funciones en el área administrativa de informática del IUTVAL.

Etapa 4: Determinación de los factores motivantes y factores de mantenimiento:

Se recopiló la data obtenida con el instrumento, se analizó contrastándose con la teoría presentada en la revisión teórica. Dichos resultados y análisis, permitieron saber lo que incide en la cultura de gestión en seguridad tecnológica del personal bajo estudio, lo cual finalmente permitió deducir los lineamientos estratégicos como modelo de gestión posible para aplicar en el IUTVAL.

Etapa 5: Análisis y Selección de Estrategias:

La fase anterior, de acuerdo al análisis realizado y los datos obtenidos mediante el instrumento aplicado, generó la propuesta, traducida en un modelo de estrategias para la Departamento de Tecnología de Sistemas e Información del IUTVAL en materia de seguridad tecnológica.

Operacionalización de Variables de la Investigación

Por su parte, Tamayo (op cit), indica: "… el término *variable*, en su significado más general, se utiliza para designar cualquier característica de la realidad que pueda ser determinada por la observación y que pueda mostrar diferentes valores de una unidad de observación a otra.". (p. 163). Así, en la consulta referencial, como de campo o in situ, en el propósito de buscar, acceder, obtener, procesar e interpretar datos.

Según Hurtado (2007): El proceso que permite precisar los indicios y las dimensiones o sinergias de los eventos se llama operacionalización.: "se realiza cuando el investigador desea hacer un abordaje focalizado de la investigación, cuando ya tiene un concepto específico del evento y su intención es construir un instrumento estructurado". En este caso, el instrumento permitirá captar sólo aquellos aspectos del evento que estén previamente definidos y contemplados en los indicios. Obsérvese el siguiente cuadro al respecto de la presente investigación:

.

Cuadro 1.Operacionalización de variables en la investigación.

Objetivo específico	Variable	Dimensión	Indicadores	Ítem
Identificar la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como conformadora de capital social en el D.T.S.I. del IUTVAL	*Normativa*	Leyes del estado y reglamentos internos	Ejecución de procesos	1
	Sustentabilidad	Perdurabilidad de los espacios y servicios de seguridad tecnológica	Satisfacción	2
			Participación	3
			Corresponsabilidad	4
Describir en el marco de la cultura gerencial, la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios en el D.T.S.I. del IUTVAL.	*Toma de Decisiones*	Programabilidad y técnicas de solución de problemas para Seguridad tecnológica.	Supervisión Control	5 6
			Políticas estándares	7
Determinar las tendencias de la praxis de GST en el D.T.S.I. para la seguridad tecnológica, considerando la cultura gerencial y el rol educativo de la organización IUTVAL.	*Ámbito teórico/práctico científico - tecnológico*	Racionalidad, técnicas teóricas y aplicadas en materia de seguridad tecnológica.	Formación	8 9
			Comunicación	10
			Uso de tecnologías	11
Enunciar un conjunto de lineamientos bajo modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL como organización educativa.	*Requerimientos de estrategias novedosas*	Verificación de la necesidad socio-tecnológica favorable	Carencia de modelo gestión estratégica en seguridad tecnológica	12

Fuente: Autora, 2021.

CAPÍTULO IV

RESULTADOS

Procesamiento, Presentación, Análisis, Interpretación

Los resultados se fundamentan en la Estadística Descriptiva o deductiva, según lo citado entre otros, por Hernández, Fernández, Baptista (2006, p. 496), a la par de Govinden (2005, p. 3), cuando como se indicó, plantean que esa modalidad estadígrafa, viabiliza definir datos, valores y puntuaciones obtenidas en la estrategia en campo o in situ.

Se requirió el procesamiento de los datos a través de la tabulación automatizada utilizando la ayuda informática de la herramienta de productividad denominada Excel, para diagramar los valores obtenidos en gráficos porcentuales circulares previa construcción de los histogramas de frecuencias (cuadros de datos). El análisis e interpretación cuantitativa, de los resultados, como en todo proyecto factible solo se obtiene a partir de una estricta comparación fáctica de los datos que ya están allí, dado que esta investigación es no experimental, para ser representados y explicados a partir de un componente teórico acorde a la variable que se esté representando con su indicador.

Se destaca también, el escalamiento tipo Likert de la encuesta aplicada, que consiste en el planteamiento de: "… juicios o afirmaciones que buscan la reacción…", del sujeto consultado. (Hernández, et al, op cit, p. 369). El formato consto de 12 preguntas para respuestas en las alternativas: Muy De Acuerdo = **MDA 5**, De Acuerdo = **DA 4**, Ni de acuerdo Ni en desacuerdo = **NINI 3**, En Desacuerdo = **ED 2**, Muy En Desacuerdo = **MED 1**.

Procesamiento y Resultados del Instrumento

Objetivo 1:

Identificar la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como coformadora de capital social en el D.T.S.I. del IUTVAL

Dimensión: Leyes de Estado y Reglamentos Internos

Pregunta 1. La normativa jurídica nacional que rige la gestión de seguridad tecnológica facilita la aplicación de soluciones para gerenciar las instalaciones y servicios tecnológicos en IUTVAL.

Cuadro 2. Normativa y facilidades de aplicar soluciones en Gestión de Seguridad Tecnológica. (GST)

OPCIÓN	FRECUENCIA	%
MUY DE ACUERDO = **MDA**		
DE ACUERDO = **DA**	3	33
NI DE ACUERDO NI EN DESACUERDO = **NINI**		
EN DESACUERDO = **ED**	4	45
MUY EN DESACUERDO = **MED**	2	22

Nota. Elaborado con base en datos de consulta obtenidos en el ítem 1.

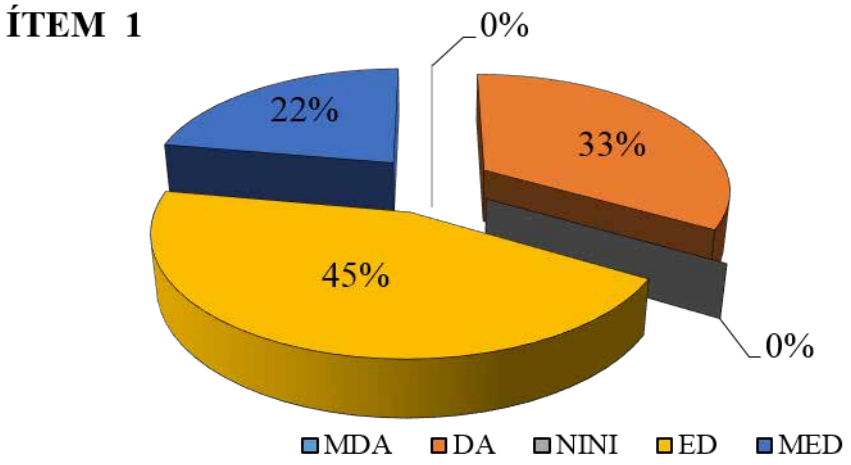


Gráfico 8 Normativa y facilidades de aplicar soluciones en GST
Fuente: Autora (2021).

Análisis Cuantitativo del Procesamiento de Datos Pregunta 1

En resultados obtenidos de la entrevista con nueve funcionarios que se desempeñan en la gerencia de la Sede de Informática en el IUTVAL, el 33% en la opción De Acuerdo apoyó la afirmación; el 45% En Desacuerdo y 22% Muy En Desacuerdo, quiere decir que el 67 % no apoyó el juicio del ítem 1.

Interpretación de Resultados Pregunta 1

Este ítem está vinculado con el indicador Ejecución de procesos y la variable Normativa, donde el 67%, de los funcionarios no apoya el juicio consultado en el ítem 1. Lo cual significa que la Normativa Jurídica no facilita la adecuada gestión para la aplicación de soluciones en las instalaciones y servicios tecnológicos en el IUTVAL.

Ahora el deber ser del enfoque de gerencia, parafraseando a Matteo (2014) para la sustentabilidad de una gestión en su concepción, incorpora a la Responsabilidad Social Organizacional, como un agente dinamizador –ejecutivo-operativo- tanto interno como externo, de la gestión organizacional enmarcada en el desarrollo sustentable que permea una facilidad en la ejecución de las labores al recurso humano o capital social de la institución y su entorno.

Dimensión: Perdurabilidad de los Espacios y Servicios de seguridad tecnológica.

Pregunta 2. La sustentabilidad de las instalaciones y servicios tecnológicos seguros en el IUTVAL se evidencia fundamentalmente en la normativa interna.

Cuadro 3. Evidencias de la sustentabilidad de las instalaciones IUTVAL

OPCIÓN	FRECUENCIA	%
MDA	1	11
DA	1	11
NINI		
ED	5	56
MED	2	22

Nota. Elaborado con base en datos de consulta obtenidos en el ítem 2.

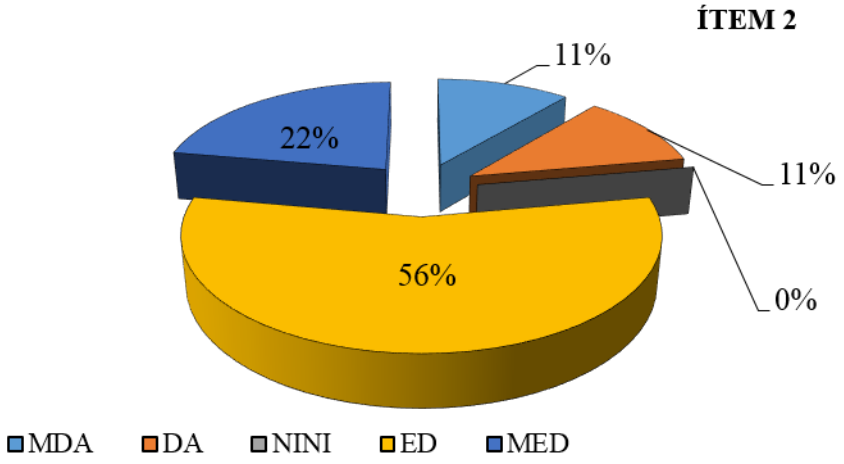


Gráfico 9 Evidencias de la sustentabilidad de las instalaciones IUTVAL.
Fuente: Autora (2021).

Análisis Cuantitativo del Procesamiento de Datos Pregunta 2

Resultados obtenidos de la encuesta con nueve funcionarios que se desempeñan en la gerencia de la Sede de Informática en el IUTVAL, el 11 % en la opción Muy De Acuerdo, el 11% en la opción De Acuerdo apoyó la afirmación; el 0% en la opción NI en acuerdo NI en desacuerdo, en el 56% En Desacuerdo y 22% Muy En Desacuerdo, no apoyó el juicio del ítem 2, con lo cual no se satisface la sustentabilidad de los espacios donde debe funcionar las soluciones de seguridad tecnológica en el IUTVAL.

Interpretación de Resultados Pregunta 2

Para la Variable Sustentabilidad y el indicador Satisfacción, al haber una mayoría de 78 % que no apoyó el juicio del ítem 2, se establece con ese resultado que no se satisface la sustentabilidad de las instalaciones y servicios para GST en el IUTVAL.

Pregunta 3. Las normas jurídicas e institucionales para la gestión de seguridad tecnológica permiten la participación protagónica de toda la comunidad universitaria para el cuido de las instalaciones y servicios tecnológicos.

Cuadro 4. Participación Protagónica de la comunidad según normas de GST.

OPCIÓN	FRECUENCIA	%
MDA	1	11
DA	2	22
NINI		
ED	3	34
MED	3	33

Nota. Elaborado con base en datos obtenidos en el ítem 3.

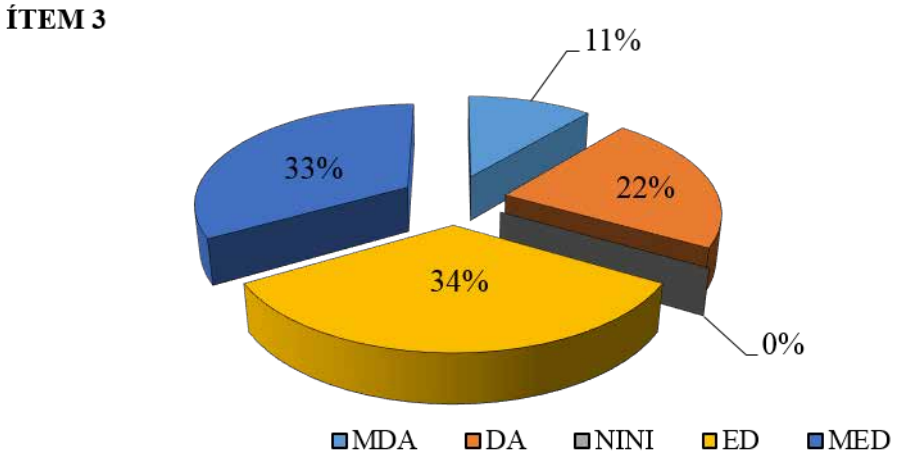


Gráfico 10 Participación Protagónica de la comunidad según normas de GST.
Fuente: Autora (2021).

Análisis Cuantitativo del Procesamiento de Datos Pregunta 3

Se lee de la gráfica que el 11% Muy De Acuerdo y el 22% De Acuerdo apoyó el juicio; el 34% En Desacuerdo y el 33% Muy En Desacuerdo; es decir el sector que no apoyó la afirmación del ítem 3 fue un total de 63% , o sea más de la mitad de los encuestados.

Interpretación de Resultados Pregunta 3

Considerando la Variable Sustentabilidad y el indicador Participación, al haber una mayoría de 67 % que no apoyó el juicio del ítem 3, se establece con ello que no se satisface de acuerdo a las normas jurídicas e institucionales para la gestión de GST en cuanto a la participación protagónica de toda la

comunidad universitaria en los espacios para la gestión de seguridad tecnológica en el IUTVAL.

Pregunta 4. En el ordenamiento jurídico interno que debe aplicar el gerente de la Dirección de informática para GST, se posibilitan acciones de corresponsabilidad social para bien común del IUTVAL en servicios tecnológicos del área de seguridad.

Cuadro 5. Posibilidad de corresponsabilidad social: acciones y bien común IUTVAL.

OPCIÓN	FRECUENCIA	%
MDA		
DA	2	22
NINI	1	11
ED	4	45
MED	2	22

Nota. Elaborado con base en datos obtenidos en el ítem 4.

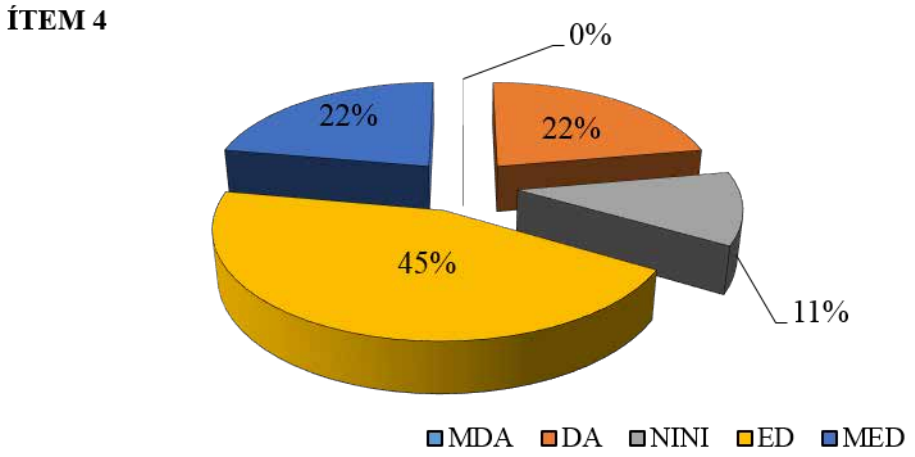


Gráfico 11. Posibilidad de corresponsabilidad social: acciones y bien Común IUTVAL.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 4

A partir de la gráfica 14, se establece que el 22%, en la opción De Acuerdo apoyó la afirmación; el 11% se ubicó NI de acuerdo NI en desacuerdo; y no apoyó el juicio del ítem 4 el 67%, que resulta de la suma del 45% En Desacuerdo y 22% Muy En Desacuerdo.

Interpretación de Resultados Pregunta 4

Como se indicó en el ítem 1, correlacionándolo ahora con la respuestas del ítem 4 el valor social, como principio constitucional y deberes de las personas en Responsabilidad Social, Corresponsabilidad, Participación; es símil con la LOE-2009 «que a 2016, no ha cumplido con las Disposiciones Transitorias (DT), 2ª y 3ª», de sí al estudiante por ejemplarizar a cualquier miembro de la comunidad, lo preceptúa en Arts.13, y en los Arts.17-23, a: "Corresponsables de la Educación", para el cuidado de sus instalaciones, equipos y ayuda a gestión de seguridad tecnológica, por ejemplo en la previsión de eventos inseguros para la intranet del Instituto, este actor – como podría sucederle a cualquier otro - no lo hace porque por ejemplo sin saber puede estar usando un pen drive con virus informático.

Este ítem está vinculado con el indicador Corresponsabilidad y la variable Sustentabilidad, donde el 67%, de los funcionarios de la Dirección de Informática no apoya el juicio consultado en el ítem 4, es decir no se cumple con la corresponsabilidad.

Cerrando lo relativo a la variable sustentabilidad en sus tres indicadores (satisfacción, participación y corresponsabilidad) el deber ser es encontrar que el enfoque de gerencia para la sustentabilidad de la gestión tecnológica en materia de seguridad, considere en su esencia, un marco de actuación ético y de responsabilidad social, en un sentido de corresponsabilidad, solidaridad y convicción, como vías para iniciar el tránsito hacia el uso de políticas, normas y lineamientos estratégicos en toda la institución.

Objetivo 2:

Describir en el marco de la cultura gerencial, la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios en el D.T.S.I. del IUTVAL.

Dimensión: Programabilidad y técnicas de solución de problemas para Seguridad tecnológica.

Pregunta 5. En el IUTVAL la gerencia (Dpto. DTSI) en GST, es una estructura Organizacional que puede decidir/establecer la supervisión de personas en la institución para garantizar el control, fiscalización e inspección de la universidad.

Cuadro 6. Supervisión Gerencial en GST en el IUTVAL: Decisión y Control.

OPCIÓN	FRECUENCIA	%
MDA	2	22
DA	1	11
NINI	1	11
ED	4	45
MED	1	11

Nota. Elaborado con base en datos obtenidos en el ítem 5.

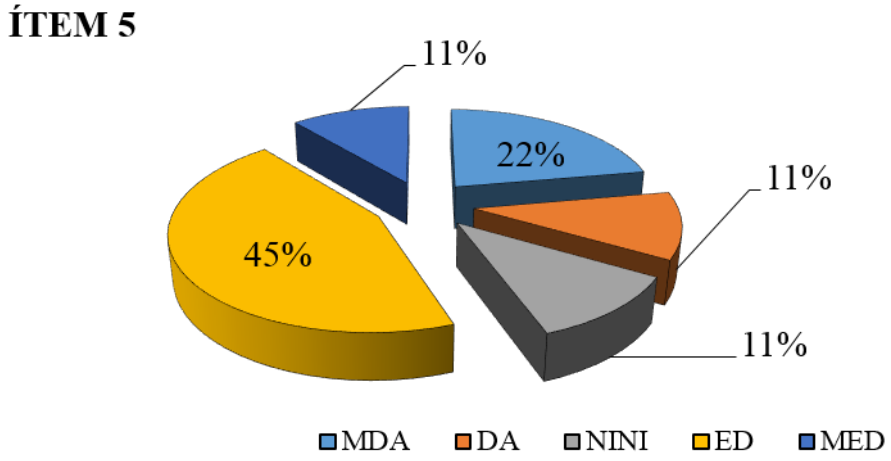


Gráfico 12. Supervisión Gerencial en GST en el IUTVAL: Decisión y Control.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 5

La opción Muy De Acuerdo con 22% y De Acuerdo 11% apoyó el juicio, para un total de 33%; el 11 % se ubicó en la opción NI de acuerdo Ni en desacuerdo; y el 56% que resulta de la suma de: el 45% En Desacuerdo y 11%

Muy En Desacuerdo, no apoyó la afirmación consultada en el planteamiento del ítem 5.

Interpretación de Resultados Pregunta 5

El 56 % de los gerentes de GST, considera que son una estructura organizacional que NO pueden decidir de forma autónoma la supervisión por parte de personas e instituciones por ejemplo externas (asesorías, contratos, otros) para garantizar el control, fiscalización e inspección de la universidad de una manera ad hoc, o sea acompañados de otros expertos externos y estar actualizados.

La variable toma de decisiones en cuanto a su indicador supervisión debería programarse según Matteo (2014) para la organización siendo esta “un sistema de producción –de bienes/servicios-, pero también es una comunidad moral, es una cuestión de principios y convicciones para valorar lo que está en juego para la existencia misma de la organización y su entorno”.

El deber ser en toda estructura organizacional es tener bien claro bajo quien estará la supervisión técnica específica tanto de trabajos realizados, como el uso por parte de la comunidad universitaria de todas las instalaciones tecnológicas (laboratorios, intranet), esta es una parte prioritaria en la toma de decisiones, referentes al cuadrante de GST. El 56%, no apoyó la afirmación consultada en el planteamiento del ítem 5.

Pregunta 6. Se cumple con divulgar resultados del planeamiento operativo, su registro y estadísticas al desempeño institucional de la GST, exigidos en las normativas de estado para el sector universitario a fin de divulgas las acciones de gestión de seguridad tecnológica en la organización.

Para visibilizar este resultado a continuación está el cuadro 7 y su representación con análisis del gráfico 13.

Cuadro 7.Divulgación de resultados: registro de estadísticas y desempeño en GST en el IUTVAL.

OPCIÓN	FRECUENCIA	%
MDA	1	11
DA	1	11
NINI		
ED	5	56
MED	2	22

Nota. Elaborado con base en datos obtenidos en el ítem 6.

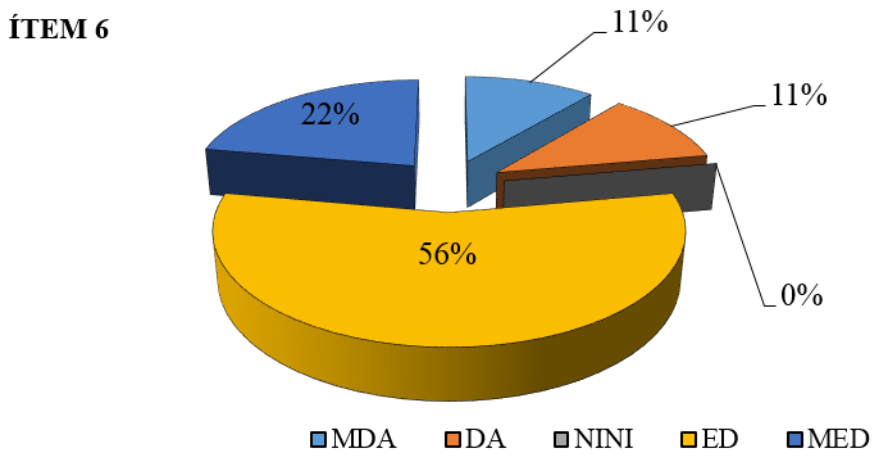


Gráfico 13. Divulgación de resultados: registro de estadísticas y desempeño en GST en el IUTVAL.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 6

A partir del gráfico No. 16; El 11% Muy De Acuerdo, el 11% De Acuerdo, solo el porcentaje 22 % apoyó la afirmación; y el 78% que resulta de sumar: el 56% En Desacuerdo y 22% MED, no apoyó el juicio planteado en el ítem 6.

Interpretación de Resultados Pregunta 6

Este ítem está vinculado con el indicador Supervisión y la variable Toma de decisiones. El 78% no apoyó la afirmación planteada en el ítem 6.; con lo cual No se aplican técnicas de programabilidad para la supervisión en relación a

los registros que se deberían llevar en sistemas y otros archivos. Teorías y tendencias gerenciales, y en la Constitución Nacional (CN, Art. 7), establece sobre la memoria tecnológica (documentos o archivos institucionales: registrados, asegurados, mantenidos, divulgados en contextos endo - exógenos), son preceptos de la Constitución Nacional (1999): Arts. 28, 57, 58, 60, 108, 143.

Pregunta 7. La gerencia estratégica de desempeño integral en GST, NO SE FUNDAMENTA en las políticas estándares ISO de GST para la toma de decisión

Cuadro 8. Gerencia estratégica de desempeño integral en GST, sustentada en políticas estándares ISO.

OPCIÓN	FRECUENCIA	%
MDA	3	34
DA	2	22
NINI	1	11
ED	3	33
MED		

Nota. Elaborado con base en datos obtenidos en el ítem 7.

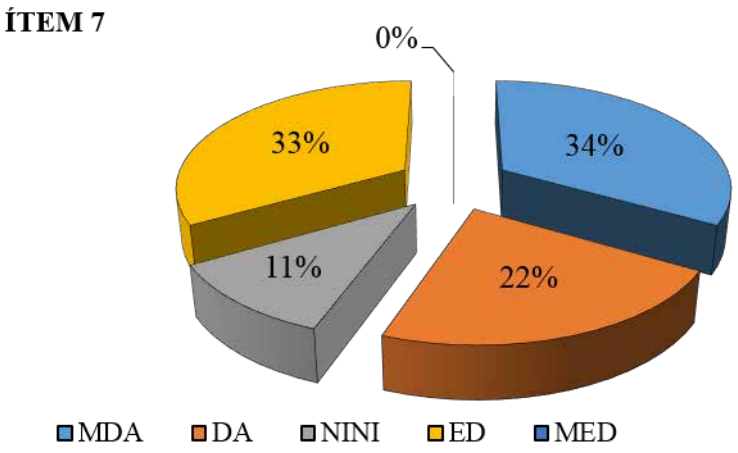


Gráfico 14. Gerencia estratégica de desempeño integral en GST, sustentada en políticas estándares ISO.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 7

Desde los datos se totaliza que El 56% apoyó la afirmación, considerando que el 34% Muy De Acuerdo sumado al 22% De Acuerdo; el 11% se ubicó NI de acuerdo NI en desacuerdo; y el 33%, En Desacuerdo, no apoyó el juicio consultado en el ítem 7. Es decir que No fundamentan sus políticas en estándares.

Interpretación de Resultados Pregunta 7

La sustentabilidad de un modelo de gestión se basa en el estándar o normativa ISO/IEC JTC 1/SC 27, organización técnica que ha establecido una familia de Estándares Internacionales para la Gestión de Seguridad de la Información (ISMS). La familia incluye obligaciones sobre requerimientos de gestión del riesgo, métrica, medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. Dichos principios se esgrimieron en el capítulo 2 de este trabajo de grado y deben ser incorporados en la propuesta.

Objetivo 3:

Determinar las tendencias de la praxis de GST en el D.T.S.I. para la seguridad tecnológica, considerando la cultura gerencial y el rol educativo de la organización IUTVAL.

Dimensión: Racionalidad técnica y teórica

Pregunta 8. La formulación de planes de GST en el IUTVAL está sustentada en tendencias gerenciales, garantizando el desarrollo de gestión con alcance de Validación (Planeación vs Ejecución).

Cuadro 9. Formulación de planes en GST con tendencias al desarrollo de gestión y Validación (Planeación vs Ejecución).

OPCIÓN	FRECUENCIA	%
MDA	1	11
DA	3	34
NINI	1	11
ED	2	22
MED	2	22

Nota. Elaborado con base en datos obtenidos en el ítem 8.

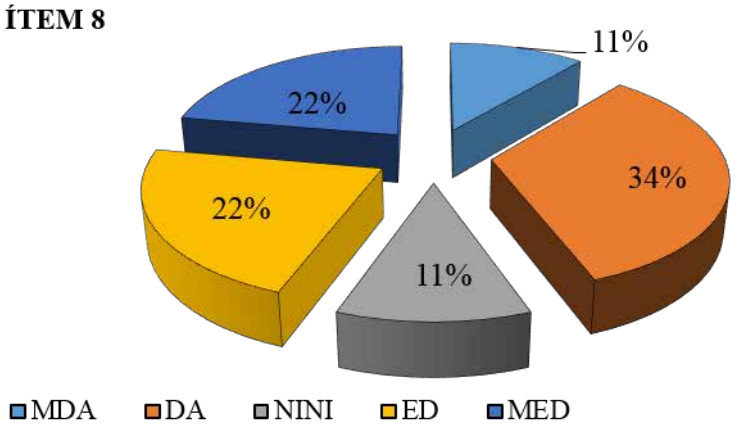


Gráfico 15. Formulación de planes en GST con tendencias al desarrollo de gestión y Validación (Planeación vs Ejecución).
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 8

Se estableció a partir del cuadro No. 9 que el 45% de los encuestados apoyó la afirmación estando el 11% Muy De Acuerdo y el 34% De Acuerdo; el 11% se ubicó NI de acuerdo NI en desacuerdo; y el 44% de los encuestados no apoyo el juicio del ítem 8 porque el 22% estuvo En Desacuerdo y el restante 22% Muy En Desacuerdo.

Interpretación de Resultados Pregunta 8

A pesar de no ser la mayoría absoluta, el 44 % de los funcionarios consideró que le falta formación en su área tecnológica, siendo el indicador acá a precisar la formación en la variable ámbito teórico-científico-tecnológico; no obstante, un 45 % considera que SI ejerce una Planeación Vs Evaluación de acuerdo a sus conocimientos teóricos. La cuestión a resolver entonces para una propuesta que logre homogeneizar el grupo de funcionarios y sobre todo a los indecisos (11%) estaría en cómo lograr la formación tanto de la gestión estratégica de las Unidades, por ejemplo soporte técnico y redes con software, como de todo el talento humano vinculado con el uso y disfrute de

instalaciones, esencialmente en procesos de GST, para satisfacer los intereses de los diferentes grupos que conforman la compleja estructura organizacional del IUTVAL.

Pregunta 9. La gerencia de GST, esta empoderada de parámetros normativos y tendencias de última generación de las ciencias administrativas gerenciales, para implementar supuestos teóricos en gestión estratégica considerando estructura, organización y seguridad tecnológica.

Cuadro 10. Empoderamiento de supuestos teóricos en gestión estratégica considerando estructura, organización y seguridad tecnológica.

OPCIÓN	FRECUENCIA	%
MDA		
DA	2	25
NINI		
ED	4	50
MED	3	25

Nota. Elaborado con base en datos obtenidos en el ítem 9.

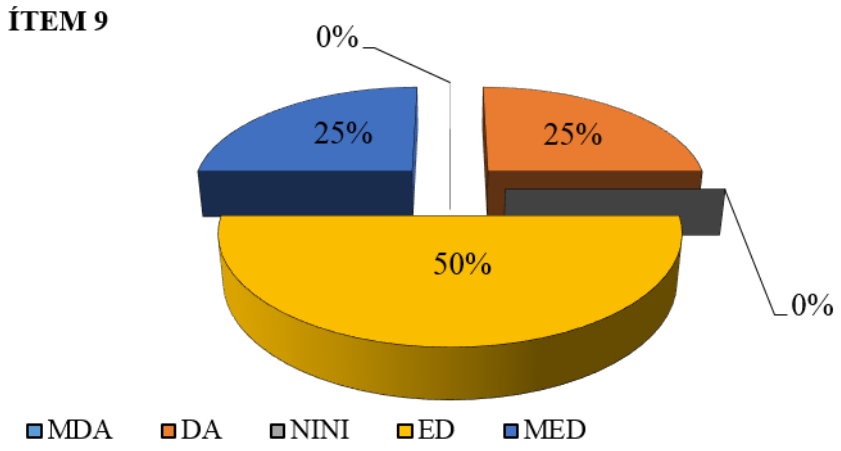


Gráfico 16. Empoderamiento de supuestos teóricos en gestión estratégica considerando estructura, organización y seguridad tecnológica.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 9

El 25% encuestado estuvo De Acuerdo es decir apoyó la afirmación; y el 75% de los funcionarios encuestados no apoyó la consulta del ítem 9, cifra que se obtiene de la suma del 50% En Desacuerdo y 25% Muy En Desacuerdo.

Interpretación de Resultados Pregunta 9

Al respecto de la triada de gestión: organización (cultura), estructura (gerencia) y seguridad (tecnológica) ocurre que los funcionarios no se auto consideran empoderados de las recientes tendencias en teorías, eso significa que adolecen de formación idónea para afrontar los problemas de seguridad tecnológica que se pueden presentar como pishing, hacking, bloqueos en sistema o equipos, lo que constata que se cumple en este respecto el principio de mala gestión de J. Etkin, (2011) considera que: "Los directivos no analizan en profundidad o resuelven con una mirada egoísta la problemática, entre principios y estrategias, entre ejercicio del poder y la sustentabilidad social de la organización". Para la propuesta a fin de dar respuesta en términos de formación en materia de seguridad tecnológica es una exigibilidad operativa institucional interna para una mejora en la logística estructural y organizativa.

Pregunta 10. El hecho gerencial en GST, como gestión técnica clave se registra en las memorias tecnológicas institucionales.

Cuadro 11. Registro en memorias tecnológicas institucionales de la gestión en GST.

OPCIÓN	FRECUENCIA	%
MDA	1	11
DA	2	22
NINI	2	22
ED	3	34
MED	1	11

Nota. Elaborado con base en datos obtenidos en el ítem 10.

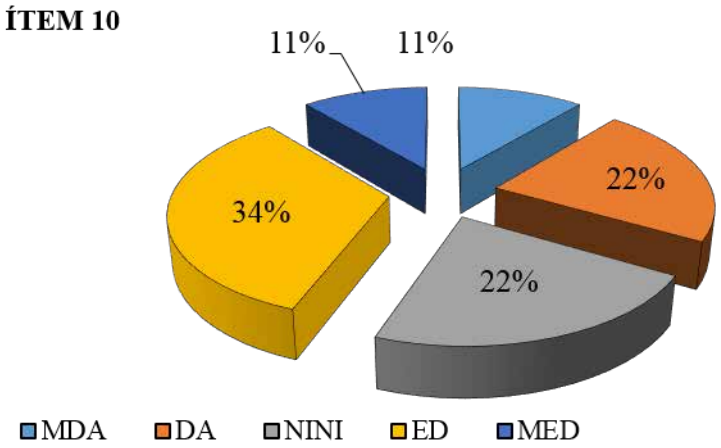


Gráfico 17. Registro en memorias tecnológicas institucionales de la gestión en GST.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 10

El 33% apoyo la afirmación con el 11% Muy De Acuerdo y 22% De Acuerdo; el 22% se ubicó en NI de acuerdo NI en desacuerdo; y el 45%, resultado de sumar 34% En Desacuerdo y 11% Muy En Desacuerdo, no apoyó la afirmación consultada en el ítem 10.

Interpretación de Resultados Pregunta 10

Este ítem está vinculado con el indicador Comunicación. El 45% de los entrevistados no apoyó la afirmación consultada en el planteamiento del ítem 10. Habermas (2002), planteó en la Acción Comunicativa, el asumir la comunicación a profundidad de entendimiento. Dicho principio de actuación debe incorporarse en un modelo de Gestión, cualquiera que sea el carácter del modelo, es por ello que se amerita de una técnica protocolar para que de manera estratégica operativa y forma inmediata se entienda el problema y se pase a derivar la solución o la acción a ejecutar de acuerdo al tipo del problema o su grado de dificultad, empleando la escalabilidad de procesos en la información y comunicación.

Pregunta 11. Las herramientas científico – tecnológica en información, comunicación, hardware/software, sistemas, redes se replantean y se solicitan a lo interno de la gerencia estratégica en base a sustentar las funciones garantes de la GST, pero no se adquieren.

Cuadro 12. Tendencias de lo científico – tecnológico hardware/software sustentado en las funciones garantes de GST.

OPCIÓN	FRECUENCIA	%
MDA	4	45
DA	2	22
NINI		
ED	3	33
MED		

Nota. Elaborado con base en datos obtenidos en el ítem 11.

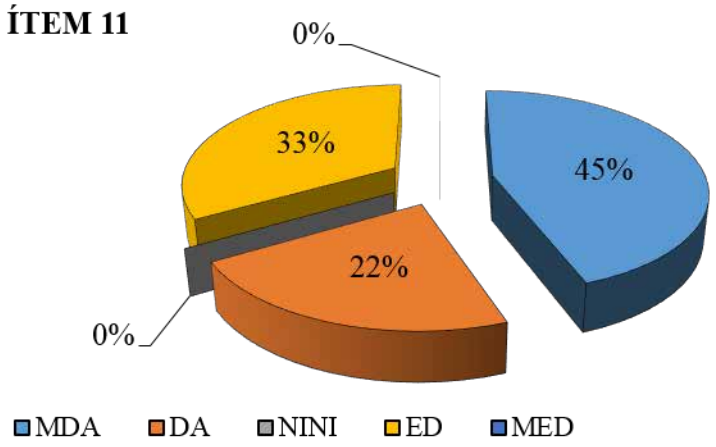


Gráfico 18. Tendencias de lo científico – tecnológico hardware/software sustentado en las funciones garantes de GST.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 11

El 67% apoyo la afirmación del ítem 11; resultado de la suma de 45% en la opción Muy De Acuerdo, y el 22% en la opción De Acuerdo; la opción NI en acuerdo NI en desacuerdo 0%, el 33% En Desacuerdo y 0% Muy En Desacuerdo.

Interpretación de Resultados Pregunta 11

Este ítem está relacionado con el indicador uso de tecnologías y la variable Ámbito teórico científico – tecnológico. El 67% apoyó la afirmación planteada a su consulta en el ítem 11. Es decir que la opinión técnica de los expertos del departamento de Sistemas e información se ignora a la hora de suplir tecnología.

Para la propuesta debería existir una relación entre la evolución y cambio por reposición de plataformas en el IUTVAL producto de la adaptación de nuevas tecnologías de hardware y/o software, como herramientas para afrontar nuevas realidades del entorno, lo cual facilitará cambios en su cultura tecnológica.

Objetivo 4:

Enunciar un conjunto de lineamientos bajo modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL como organización educativa.

Dimensión: Verificación de la necesidad socio tecnológica favorable

Pregunta 12. Se cuenta en IUTVAL con líneas estratégicas para la acción de seguridad, uso o disfrute de los bienes y espacios universitarios en materia de GST.

Cuadro 13. Existencia de líneas estratégicas para la seguridad en GST.

OPCIÓN	*F*	%
MDA	3	33
DA	1	11
NINI		
ED	4	45
MED	1	11

Nota. Elaborado con base en datos obtenidos en el ítem 12.

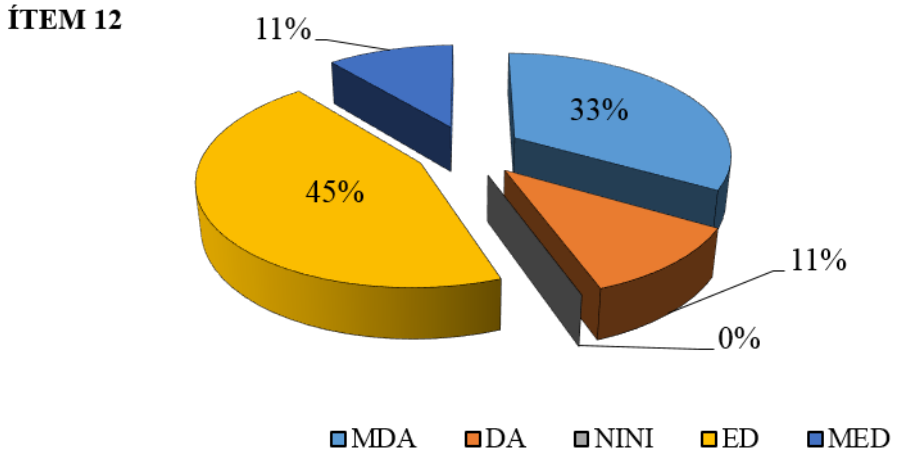


Gráfico 19. Existencia de líneas estratégicas para la seguridad, uso o disfrute de los bienes y espacios universitarios en GST.
Fuente: Autora (2021)

Análisis Cuantitativo del Procesamiento de Datos Pregunta 12

El 44% encuestado que representa la suma de 11% Muy de Acuerdo y el 33% De acuerdo Apoyó la afirmación; y el 56% de los gerentes encuestados no apoyo la consulta del ítem 12, cifra que se obtiene de la suma 45% En Desacuerdo y 11% Muy En Desacuerdo.

Interpretación de Resultados Pregunta 12

El primer paso de una empresa u organización que intenta ser responsable y no solo utilitaria, que enfrenta una realidad que no ha creado y no tiene en claro cómo enfocar, es “salir de la gerencia o dirección por resultados”, y avanzar en el sentido de la Gerencia Sustentable, fundamentada en la ética y la responsabilidad social de las competencias para la que fue creada esa estructura organizativa.

Para Amartya Sen (2000): “la racionalidad económica se abre a la racionalidad ética como fundamento de la nueva economía.” Es por eso que se necesita implementar con urgencia un modelo nuevo de gestión de seguridad tecnológica que realce la triada de gestión: organización (cultura), estructura (gerencia) y seguridad (tecnológica).

CAPÍTULO V

PROPUESTA

Modelo De Gesti n De Seguridad Tecnológica

La gnosis que sustenta las líneas de gestión que se declaran en este capítulo se esgrimen debido a que toda organización en materia de seguridad tecnológica de auto generarse la habilidad y capacidades para resguardar su información y asegurarla de ataques externos o internos a los que está expuesto el mundo digital bien sea por causas de usuarios inexperto (impericia) o por causa de situación creada (exprofesa).

A partir del diagnóstico se estableció la eminente necesidad de un modelo especifico en materia de Gestión de Seguridad Tecnológica para la Información (GSTI) en el IUTVAL, el cual de acuerdo con la información aportada por sus funcionarios que laboran en el Departamento de Sistemas e Información debe contener la posibilidad de

- Plantearse acorde a la normativa del marco tecnológico e institucional
- Mantener seguridad física y ambiental con controles presenciales y virtuales de acceso a la información.
- Facilitar la participación de los funcionarios responsables directos (Dpto. de S.I.) y de la comunidad universitaria (usuarios)
- Contemplar procedimientos que permitan la solución de los eventos de vulnerabilidad que se presenten, indicando la posible técnica de solución
- Mantener comunicación permanente haciendo que fluyan las líneas de mando, considerando los controles, registro y documentaciones de los incidentes.

Tener como guía la aplicación de estándares ISO/207 (01/ et all) que coadyuve a la normalización e implementación de nuevos recursos tecnológicos.

- Fundamentar sus acciones administrativas y políticas tecnológicas en teorías gerenciales actualizadas.
- Respetar y mejorar la formación técnica de los funcionarios expertos.

Con todas esas expectativas el conjunto de lineamientos que se presentan a continuación persiguen una intencionalidad subyacente la cual es favorecer la sustentabilidad de la cultura gerencial tecnológica en la Universidad, resumiendo un conjunto de primacias posibles como nuevos lineamientos estratégicos, que le permitan al IUTVAL como organización educativa y formadora de capital social, tener en cuenta a Drucker (1995) quien plantea que el factor tecnoambiental es un reto que "consistirá en lograr la dignidad social de los trabajadores de servicios. Siendo así que las organizaciones con mayor capacidad de cambio se rediseñan en corto tiempo.

Factibilidad de la Propuesta de Lineamientos estratégicos

Un estudio de factibilidad, es una herramienta analítica que se emplea con la finalidad de conocer, si un proyecto con ciertas características y bajo ciertas condiciones, puede realizarse convenientemente para obtener un beneficio. Dicho esto se explica el análisis realizado para dar posibilidad de implantación del modelo de gestión GSTI-IUTVAL.

Factibilidad técnico –operativa:

Lo resaltante de este estudio en un proyecto, es el diseño de la función de producción que mejor utilice los recursos disponibles para obtener el producto deseado. Aunado a esto, se incluyen las técnicas e instrumentos necesarios para

ese fin y especialmente para poder medir el grado de adecuación de esa función de producción a un predeterminado conjunto de criterio.

En el caso de IUTVAL la factibilidad técnico operativa de esta propuesta viene dado porque ya se cuenta en la estructura organizativa con el Departamento de Sistemas e Información y las Unidades que lo conforman, así que ello viabiliza la puesta en marcha de este modelo operativo de acciones estratégicas basadas en la confiabilidad operacional, entonces se da su viabilidad porque de ponerse en marcha sería en un contexto operacional específico de la Institución IUTVAL.

Los límites de diseño, siendo este un modelo sistémico vendrá dado por los criterios de calidad de la filosofía de trabajo de la organización, es decir atendiendo la visión y misión del IUTVAL; pero además los establecidos por el Dpto. De S.I. en cuanto a disponibilidad, integridad y disponibilidad de la información.

Factibilidad Económica:

Un proceso implica el uso de los recursos de una organización, para obtener algo de valor. Ningún producto puede fabricarse y ningún servicio puede suministrarse sin un proceso, y ningún proceso puede existir sin un producto o servicio (Krajewski, 2000). Con lo antes expuesto, puede afirmarse que tanto la generación de un producto o la prestación de un servicio es sinónimo de producción.

En virtud de que esta propuesta lo que pretende es un cambio en la forma de vivenciar la gestión de seguridad de la información, se indagó que la universidad cuenta con sus propios mecanismos como lo son los proyectos de actualización del personal a través de las solicitudes de requerimientos específicos que le plantean los niveles gerenciales a la Dirección de recursos humanos para formar a su personal. Por otra parte el IUTVAL cuenta con un parque tecnológico instalado, para lo cual está obligado por ley de estado (infogobierno) a la utilización de software libre de distribución gratuita (sin

adquisición de licencias) y es el Ministerio del Poder Popular para Educación Universitaria , a través de la Oficina de Planificación del Sector Universitario –OPSU- el ente que facilita el recurso para adquisición o sustitución de equipos (ejemplo: servidores, salas de informática).

Factibilidad legal:

En el sentido legal se argumenta que en el país rigen deberes de participación, corresponsabilidad, responsabilidad social en el Subsistema Educación Universitaria, al cumplir estos u otros principios que desde las condiciones biosocioambientales de las infraestructuras ad hoc, son concordantes a lo preceptuado en la Constitución (CRBV,1999) bajo los Art. 3, 7, 102 a 111, u otros, ya que por demás son taxativos eventos del desempeño gerencial–laboral–personal–social del universal contexto vinculado con el todo y las partes del contexto de gestión universitaria.

Así mismo se deben cumplir todas las normativas vigentes que le aplican a la Institución de acuerdo a la Ley de Universidades, así como del Ministerio del Poder para la Educación Universitaria Ciencia y Tecnología y Oficina de Planificación del Sector Universitario, Ley del ejercicio de la Ingeniería, normas ISO.

Principios básicos de los lineamientos propuestos

Visión:

Posibilitar a la organización que se integren triada de gestión: organización (cultura), estructura (gerencia) y seguridad (tecnológica) como factores del capital social de la organización educativa IUTVAL.

Misión:

Ejecución de habilidades que involucren las dimensiones: Políticas, Estrategias, Operatividad e Implementación, en la organización educativa IUTVAL.

Objetivo:

Plantear las líneas de acción y procesos a seguir en materia de seguridad tecnológica en el IUTVAL.

Como llevar a cabo la Ejecución de las líneas de acción del modelo (PLAN):

Los indicadores de desempeño en mantenimiento son obtenidos a partir de las perspectivas del Balanceo de Indicadores o del Control de Mando Integral y aplicados desde las divisiones hasta los empleados. Los objetivos del modelo son relacionados con los factores claves de éxito (misión y visión) y el resultado será los indicadores claves de desempeño para mantenimiento que contribuirán a guiar la puesta en marcha del modelo.

Los indicadores deben ser formulados para los diferentes niveles jerárquicos de la estructura organizacional. Para cada nivel, los indicadores tienen determinados propósitos para usuarios específicos. Los usuarios al más alto nivel gerencial se refieren al rendimiento administrativo global, mientras que los que están en los niveles funcionales tienen que ver con la condición física de los activos.

Uno de los más grandes desafíos que tendrá resuelto la gerencia consiste en la entrega de la traducción de la visión en acciones y actividades de apoyo. Es importante que ya se delineó la forma como se va a realizar este paso de la teoría a la práctica o de la visión a la acción que implica un equilibrio entre la mejora del ambiente actual y futuro.

Entre las mejores prácticas de carácter mundial avaladas por el Autor Amendola (2016), en materia de Gestión de Seguridad, es como sigue:

Gráfico 20. Elementos estratégicos operativos basados en el Balanceo de Indicadores. Adaptación: Autora (2021).
Fuente: Amendola (2004,2014).

El indiscutible poderío de los sistemas balanceados de indicadores da cuenta de ello cuando se torna en gestión a un sistema de indicadores. A medida que se aplique en el IUTVAL dentro de sus estructuras la metodología de los Sistemas Balanceados de Indicadores, se percatará que puede utilizarse para: clarificar la estrategia y conseguir el consenso sobre ella, comunicar la estrategia a toda la organización, alinear los objetivos generados con los del resto de la estructura por departamentos, con la estrategia, vincular los objetivos a largo plazo y los presupuestos anuales del mantenimiento de la seguridad, identificar y alinear las iniciativas estratégicas, realizar revisiones periódicas y sistemáticas, y obtener información de retorno (evaluación) para la estrategia y mejorarla.

Acciones estratégicas organizacionales propuestas:

Aplicar una metodología orientadora de estrategias, de acuerdo a los principios gerenciales esbozados en capítulo 2 de este trabajo de grado, incluye como un principio a seguir al Balanced Scorecard (Sistema de Balanceo de Indicadores), implica un enfoque de 4 fases, es por ello que las dimensiones tácticas establecidas por la autora de este objeto de estudio, son:

1.- Evaluación situacional:

Al plantearse un problema de seguridad tecnológica, el Dpto. de S.I. deberá detenerse a considerar los síntomas percibidos, necesidades, tipos de fallos, tipos de equipos, ingresos, costes, toma de decisiones una herramienta pragmática para construir un sistema de intervenciones

La técnica de elaboración del diagrama causa-efecto es bastante sencilla:

1) En la cabeza del pescado escribimos el efecto o síntoma que pretendemos analizar. La espina central del pescado, agrupará las causas que según nuestro análisis producen dicho efecto.

2) Las diferentes categorías en que podemos agrupar las causas conforman las espinas que se desprenden de la horizontal principal. Escribimos el nombre de la categoría en el extremo de cada nueva línea.

3) Cada causa concreta que vayamos encontrando (simplemente mediante la reflexión o mediante sesiones conjuntas de brainstorming) las vamos añadiendo en la categoría bajo las que consideramos que mejor encaja

A continuación, podrá apreciarse en la gráfica un ejemplo:

Gráfico 21. Diagrama de Ishikawa. Adaptación: Autora (2021).
Fuente: Alzola, R (2013).

2.- Diseño de rutas:

Este paso consiste en la aplicación de diseño de metodologías que se adapten a la planificación de la decisión, según Duffuaa (2002), la planeación en el contexto del sostenimiento de tareas se refiere al proceso mediante el cual se determinan y preparan todos los elementos requeridos para efectuar una metodología antes de iniciar el trabajo.

Se presenta un modelo de hoja para la planeación:

Cuadro 14. Formato Planeación.

Hoja de: _____		Llenada por: _____		**Fecha:** _____		
Equipo Responsable: _____		Aprobación: _____		**Prioridad: Emergencia** (), urgente (), Normal ( ), Programado ( ), Aplazable ( )		
Núm.	Fecha de Terminación	Orden de Trabajo #	Unidad	Descripción del Trabajo	Oficios	Tiempo estimado

Fuente: Duffuaa (2002)

El objeto de la sencillez del formato es evitar un inmenso papeleo y que al mismo tiempo existan registros y controles para los procesos de solución que se emprenden en la organización.

3.- Priorización de iniciativas de solución

Los equipos inteligentes necesitan "campos de entrenamiento" o de práctica conjunta para desarrollar sus aptitudes colectivas de aprendizaje en estos indicadores:

Aprendizaje en equipo: Es el proceso de alinearse y desarrollar la capacidad de un equipo para crear los resultados que sus miembros realmente desean. Se construye sobre la visión compartida y el dominio personal. Es preciso dominar el dialogo y las discusiones productivas.

Modelos mentales complementarios: La necesidad de una acción innovadora y coordinada, donde cada miembro permanece consciente de los demás y actúa de manera que complementa los actos de los otros

Dominio personal: Establecimiento de los conocimientos de cada individuo para las funciones que debe desempeñar

Visión sistémica compartida: Colectivamente podemos ser más agudos e inteligentes que en forma individual. El cociente intelectual del equipo es potencialmente superior al de los individuos.

4.- Definición de proyectos:

Los proyectos deben ser puestos en marcha, considerando muy de cerca los indicadores de gestión que se hayan descrito en el exigido Plan Operativo Anual, que es una norma institucional.

Acciones estratégicas tecnológicas propuestas:

Las estrategias para la acción, son precisamente el prepárese para iniciar un camino, hay que considerar dar respuesta a consideraciones que desde

siempre han estado sobre la mesa de la gestión en tecnologías de información (TI o IT), por ejemplo ¿Cómo puedo hacer las auditorías? ¿Con qué periodicidad? ¿Dónde van a estar almacenados los datos? ¿Tengo acceso o no a las instalaciones? ¿Tienen los proveedores una certificación? Una estrategia es, precisamente, prepararnos para iniciar un camino que dignifique las políticas como estrategias

Políticas de seguridad tecnológica y lineamientos técnicos por adaptar:

Para utilizar el medio estratégico de una cierta acción no militar y asociarla a una tarea de combate, la seguridad informática debe ser asumida como: "el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante". En el aspecto de seguridad, esta abarca el software y el hardware pero además la información contenida en ambos. De sí que se apliquen los lineamientos estratégicos siguientes:

Eficiencia, eficacia y efectividad:

Lockheed y Hanushek (1994) señalan que "...un sistema eficiente obtiene más productos con un determinado conjunto de recursos, insumos o logra niveles comparables de productos con menos insumos, manteniendo a lo demás igual".

En el análisis actual de la tecnología, la más acabada formulación del concepto de eficiencia, y su cercano de eficacia, se debe a Miguel Ángel Quintanilla (Quintanilla & Lawler, 2000). Partiendo desde la definición de un sistema técnico como un dispositivo complejo compuesto por entidades físicas y agentes humanos aprovechando todos los recursos disponibles, técnicamente se es eficiente para producir un bien determinado. En consecuencia los sistemas deben permitir facilitar el trabajo y lograr las metas con anticipación, siendo así hay dos términos: virtualización de servidores y trabajo remoto.

Para debilitar las amenazas omnipresentes, la institución debe adoptar la naturaleza distribuida de Internet, usando la virtualización de servidores lo cual es usar el mismo número de equipos que se tienen pero mediante la aplicación de otro software se puede crear una máquina virtual (VM) para emular un host físico (punto de inicio y fin de transferencia de datos), o sea se creará un nuevo entorno de sistema operativo independiente que es, lógicamente (pero físicamente no está), aislado del servidor host. Al ofrecer varias máquinas virtuales a la vez, este enfoque permite que varios sistemas operativos corran simultáneamente en una única máquina física para utilizar su escala y flexibilidad a su favor cuando implementan una defensa para asegurar el buen funcionamiento. Al detectarse algún problema de tiempo real ocasionado por un agente externo o interno , se activará la seguridad que se logró al añadir una capa de defensa distribuida a nivel global que es escalable, o sea actualizable desde lugares remotos – vía internet sin entrar a las instalaciones físicas o un sistema redundante ubicado en otro espacio físico que pueda interconectarse mediante el protocolo IP con el principal - esa táctica en orden de magnitud es superior a cualquier defensa centralizada.

Confidencialidad

No todos los procesos y las órdenes estarán accesibles para todos los actores sociales de la empresa, por tanto, existirán unas jerarquías en el manejo de los sistemas e información.

Integridad

La integridad en materia de tecnologías, es la relación entre la veracidad, resguardo de la data y su seguridad para que la misma no se corrompa; se coloca un listado de consideraciones para la integridad que deben ser siempre revisados:

Antivirus configurados: hay que tener el software antivirus certificado y además las actualizaciones de su denominada definición o huella para los nuevos virus y que siempre sea efectivo.

Sistemas operativos con versiones actualizadas, bajo licencias libres, ello significa que la empresa adapta cada versión a su necesidad. Verificarlas tanto en los servidores como en los equipos independientes o itinerantes (laptop).

Las redes: La institución exige el uso del correo digital como solución de comunicación , mensajería o el acceso a web; no obstante la comunicación debe restringirse a través de un diseño de red que salvaguarde a lo interno de la organización, mediante una configuración adecuadas de los equipos de telecomunicaciones que conforman dicha red y que resuelven el protocolo interno DHCP/IP esos equipos como enrutadores, switches y equipos de servicios de red (DNS) deben localizarse tanto en un lugar con las especificaciones técnicas electrónicas como seguros y no al aire libre.

Aplicaciones y acceso a las aplicaciones: Esto implica la administración mediante definición de mecanismos de acceso y autenticación efectiva de los usuarios con la autorización para registrar, modificar y consultar datos en una aplicación. Una técnica adecuada es el Protocolo compacto de acceso a direcciones (LDAP) el cual le asigna a través de atributos característicos a cada usuario unos identificadores que permiten validarlo a través de un nombre distintivo a manera de código y que permite intercambiar niveles de información tanto segura y en por tipos de importancia da o no acceso a ciertos espacios de los portales y/o sistemas de la compañía.

Prácticas de salvaguarda: No es solo colocar las normas de seguridad, sino evaluarlas progresivamente y verificar su efectividad, que se detecten y corrijan errores que de alguna manera hayan permitido incidentes de seguridad.

Otras: La clasificación de la información, las protecciones físicas de los activos de información, los planes de continuidad y el cifrado de la información (encriptamiento matemático mediante fórmulas de conversión de los significados de la información que la empaca y desempaca cuando se necesite. También ser atentos a las Auditorias de sistemas y servicios.

Disponibilidad:

La disponibilidad es un concepto tecnológico que tiene que ver con la posibilidad de acceder la información y el tiempo en que los servicios han estado en alta sin fallos, dando la respuestas esperadas, La accesibilidad a su vez está relacionada con los servicios externos e internos en que han sido fiables, o sea que han arrojado data y funciones certeras o verdaderas ; y todo ello está directamente proporcionado por la calidad del mantenimiento de los sistemas (respaldos, borrado de información o archivos en desuso, auditorias basados en archivos autograbables). La innovación para la empresa poseer celdas de información segura en la nube, fundamentada en conexión satelital a través del satélite Miranda, para evitar las limitaciones percibidas en las soluciones perimetrales e internas tradicionales. El deber ser es proponer mejoras en la infraestructura tecnológica y en los servicios automatizados.

Conformidad

Para dar orientación a que se cumplen las estrategias se diseñaron unas normativas que se colocan en el apéndice Anexo D (pág. 123) de los anexos de este trabajo.

Acciones estratégicas de gestión de seguridad propuestas (NORMAS ISO):

Luego de identificar, estimar y cuantificar los riesgos, se deben determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, para enfrentarlos de la manera más eficaz, se centró en el respeto a la norma ISO que en la cláusula 4.2.1 (g) de la norma plantea de manera muy precisa que se deben seleccionar objetivos de control y controles apropiados del estándar ISO 27001:2005:

(a) Aplicar controles apropiados.

(b)Aceptar riesgos consistente y objetivamente.

(c) Evitar los riesgos.

(d) Transferir los riesgos, y la selección se debe justificar sobre la base de las conclusiones del análisis y evaluación de los riesgos.

En general, aquellos riesgos cuya tasación esté estimada como de baja frecuencia, se puede asumir el riesgo y tratarlo más tarde. Por el contrario, los que se estiman de alta frecuencia o tasación ALTA es donde se debe tomar medidas. De las opciones propuestas por la norma se decidió tomar las 2 primeras, por lo que en este caso serán controlados o asumidos. En consecuencia, se deben proponer controles para gestionar los riesgos calificados como tasación ALTA.

Estos controles se toman de la ISO/IEC 27002:2005; sin embargo, la norma aclara que los controles propuestos no son exclusivos y podrían adoptarse otros tipos de controles.

Para efectos de ejemplificar, se han tomado en consideración lo planteado a continuación se muestra en el cuadro Nº 15 los controles a implantar para el tratamiento de los riesgos, en aquellos activos donde la tasación resultó Alta.

Cuadro 15. Controles para el tratamiento de los riesgos.

Activos	Tasación de Activos			Total	Amenazas	PO	Vulnerabilidad	PEV	VA	PO	Total	Controles Propuestos	Clausula
	Confidencialidad	Integridad	Disponibilidad										
Servidor	A	A	A	A	Plagio	M	Acceso no autorizado	A	A	A	A	7.1.3 Uso aceptable de los activos	Gestión de activos
					Respaldo	B	Falta de control de respaldo	A				8.2.3 Proceso Disciplinario	Seguridad ligada a los recursos humanos
					Alteración	M	Desconocimiento	B				11.1.1 Política de control de acceso	Control de Acceso
					Privacidad	A	Acceso no autorizado	M					
Pc`s de Informática	A	A	A	A	Falta de seguridad	M	Control de acceso	A	A	A	A	9.1.2Control físico de ingreso, 9.1.3 Seguridad en las oficinas, 9.2.1 Ubicación y protección del equipo	Seguridad física y ambiental
					Fallos técnicos,	A	Energía eléctrica	A				10.1.2 Gestión de Cambios, 10.10.1 Registro	Gestión de comunicaciones y operaciones

												de auditoría, 10.10.5 Registro de fallas	
					Errores de usuario,	M	Falta de políticas	A				11.5.3 Sistema de gestión de contraseñas	Control de Acceso
					Falta de seguridad	A	Acceso no autorizado	B				11.1.1 Política de control de A.	Control de Acceso

CONCLUSIONES Y RECOMENDACIONES

En el objetivo 1 de los resultados que se obtuvieron hasta ese punto se estableció del análisis de las preguntas 1 a 4, que quedando identificada en el IUTVAL de qué forma se vincula el ámbito jurídico de Gestión de Seguridad Tecnológica (GST) y su sustentabilidad como coformadora de capital social, tanto desde lo legal jurídico como desde la perdurabilidad de los espacios y servicios tecnológicos en lo referente a seguridad tecnológica. Más de un 63% aproximadamente de los encuestados en las cuatro primeras respuestas coincidió en que no hay normativas para la ejecución de procesos que satisfagan ni permitan la participación con corresponsabilidad en los espacios y servicios de seguridad tecnológica.

En lo relativo al Objetivo 2, se determinó que la cultura gerencial de los responsables en GST se manifiesta en cuanto a la actitud que ellos tienen para la toma de decisiones, fundamentada en principios y convicciones para valorar lo que está en juego para la existencia misma de la organización y su entorno; en consecuencia, lo que resultó para Supervisión y control de la seguridad tecnológica, partiendo de las respuestas a los ítems 5 y 6 fue que piensan que los mecanismos que poseen para el ejercicio de la inspección es rígido porque el enfoque de la organización es muy directivo y estructuralista apegado al liderazgo normativo, lo cual da poca flexibilidad para maniobrar ante los riesgos, es por ello que en la propuesta se incorporaron acciones basadas en el Cuadro de Mando Integral.

El objetivo tercero , que se refirió en sus dimensiones a la formación, comunicación y uso de tecnologías, estuvo relacionado con el ámbito teórico-práctico y la racionalidad técnica y teórica al ejercicio o praxis para la GST en el IUTVAL , pudiendo señalar A modo de cierre del análisis que se satisfizo el cumplimiento del objetivo 3, se logró explicar las tendencias en la praxis

tecnológica que se presenta en el IUTVAL para la gestión de GST, al englobar los indicadores Formación, Comunicación y Uso de Tecnologías para la variable Ámbito teórico – científico tecnológico en la dimensión Racionalidad técnica – teórica que se practica en el campo organizacional, como un funcionamiento bajo "la Resiliencia" considerándose esta como la capacidad de recuperación de las organizaciones ante un evento no esperado; como un detonante de acciones de previsión, o como parte principal de un proceso estratégico. En esencia, consiste en la capacidad de un sistema para absorber los cambios, que se vislumbran comouna serie de crisis repentinas (López, 2009; Smith y Graetz, 2011), y aún conservar su funcionalidad esencial (Walker y otros., 2006) –citados en C. Medina, (2012)-

Para el objetivo 4 lo que se diagnosticó fue la verificación de la necesidad de un diseño totalmente novedoso como propuesta de modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL.

Como recomendación se deja que uno de los más grandes desafíos que tendrá que afrontar la gerencia consiste en traducir la visión en acciones y actividades de apoyo. Es importante identificar y delinear la forma como se va a realizar este paso de la teoría a la práctica o de la visión a la acción que implica un equilibrio entre la mejora del ambiente actual y futuro; por lo cual pertinentemente esta investigación presentó la Propuesta con su factibilidad como aporte del presente trabajo de grado, el cual fue un proyecto factible que culminó con el planteamiento del modelo de gestión en seguridad tecnológica. Por tanto, se cumplió el objetivo general planteado en el presente trabajo de grado.

Los gerentes deben considerar al personal que enviaran a posteriori a un conjunto de talleres en formación y actualización de las metodologías y técnicas de gestión para asumir los lineamientos estratégicos que planteó la propuesta.

REFERENCIAS BIBLIOGRÁFICAS

Alzola, R. (2013). *Como y para que hacer un diagrama de Ishikawa*. Disponible en: http://marcaladiferencia.com/como-y-para-que-hacer-un-diagrama-de-ishikawa/ Consulta: 30-07-2016.

Amaro L., J. (2016). Seguridad en Internet. Paakat: Revista de Tecnología y Sociedad ISSN: 2007-3607 Universidad de Guadalajara Sistema de Universidad Virtual México. Recuperado el 28 de Agosto de 2019 de, http://www.redalyc.org/pdf/4990/499054323006.pdf

Amendola, L. (2004). *Organización y gestión del mantenimiento "mantenimiento como negocio: Balanced Scorecard*". 3ª Edición. Editorial PMM.

Amendola, L. (2014). *Modelos de Mantenimiento Confiable*. 1ª edición, Editorial PMM.

Amendola, L. (2016). *Modelos mixtos de confiabilidad*. 1ª Edición. Editorial PMM.

Arias, F. (2012). El Proyecto de Investigación. Introducción a la metodología científica. (6ª Ed.). Caracas. Episteme C. A.

Baas, S. (1997). Participatory Institutional Development. Conferencia sobre Agricultura sostenible y control de la arena realizada en el área del Desierto de Gansu. Estados Unidos: Organización de las. Naciones Unidas para la agricultura y la alimentación (FAO).

Bavaresco, Aura M (2006). *Proceso Metodológico en la Investigación: Cómo hacer un Diseño de Investigación*. (5ª Ed.). Editorial EDILUZ. Maracaibo-Venezuela.

Chávez Alizo, Nilda (1994). Introducción a la investigación educativa. (1ª Ed.). Editorial Coordinación del Estado Zulia. Maracaibo-Venezuela.

Constitución. (1999). Gaceta Oficial de la República de Venezuela, Nº 36.860. Diciembre 30, 1999. [2ª Versión Gaceta Oficial Nº 5.453, del 24-03-2000. Enmienda Nº 1, Gaceta Oficial Nº 5908 (E), del 19-02-2009].

D´Ary, L., Jacobs, Ch. y Razavieh, A. (1982). Introducción a la Investigación Pedagógica (2ª Edición). México: Interamericana.

Decreto N° 6.217, Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública (2008). Gaceta Oficial de la República Bolivariana de Venezuela, N° 5.890 (E). Julio 31 de 2008. [Reforma por Ley Habilitante]

Decreto Nº 8.938 (2012). Decreto con rango, valor y fuerza de Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras. Gaceta Oficial de la República Bolivariana de Venezuela. Nº 6.076 (E). Mayo 07 de 2012. [Reforma por Ley Habilitante. DLOTTT: Vigencia Mayo de 2013].

Decreto-Ley Orgánica de Planificación. (2001). Gaceta Oficial de la República de Venezuela Nº 5.554. Noviembre 13 de 2001. (Ley Habilitante 2001).

Drucker, peter. (1995). *Managing in a Time of Great Change*. Edit. Harpers Collins, USA.

Economía Digital (13 febrero 2017). Los diez mayores ataques informáticos de 2016. *Economía Digital*. https://www.economiadigital.es/tecnologia/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

Ferro Veiga, José Manuel. (2020). *Asesor/Gestor en seguridad privada integral: Curso superior en dirección de seguridad privada*. Caracas. Ediciones IESA.

Francés, A. (2006). *Estrategia y Planes para la Empresa con el Cuadro de Mando Integral.* México. Ediciones Pearson Educación.

González y Bellino (1995). *Modelo de Gestión de Recursos Humanos*. Tesis de Maestría, Universidad Metropolitana, Caracas.

Govinden, L. P. (2005). Introducción a la Estadística. (2ª Ed.). Bogotá. McGraw Hill Interamericana S. A.

Hernández S., R., Fernández, C., y Baptista, P. (1991). *Metodología de la Investigación.* (1ª Ed.). México. McGraw-Hill Interamericana S. A.

Hernández S., R., Fernández, C., y Baptista, P. (2006). *Metodología de la Investigación.* (4ª Ed.). México. McGraw-Hill Interamericana S. A.

Hurtado de Barrera, J. (2000). Metodología de la Investigación Holística. (3ª Ed.). Caracas. SYPAL. IUTC.

Kabboul, O. (S/f). Guía de Planificación Estratégica. (Mimeo sin datos editoriales).

Kaplan R. y Norton D. (2000). *El Cuadro de Mando Integral.* (*The Balanced Scorecard.* Traducción. 2ª Ed.). España. Gestión 2000.

Kerlinger, F. (1983). *Investigación del comportamiento. Técnicas y metodología*. (2ª Ed.). Editorial interamericana. Mexico.

Krajewski, L. y Ritzman, L. (2000). *Administración de operaciones. Estrategia y análisis*. (5ª ed.). México: Pearson Educación de México, S.A.

Lambin, J-J. (1997). *Marketing Estratégico*. 3ª Ed. Colombia. McGraw Hill.

Ley del Estatuto de la Función Pública. (2002). Gaceta Oficial de la República Bolivariana de Venezuela, N° 37.482. Julio 11, 2002.

Ley de Infogobierno. (2003). Gaceta Oficial de la República Bolivariana de Venezuela, No. 40.274, Noviembre 17, 2003.

Ley de Mensajes de Datos y Firmas Electrónicas (2001).Gaceta Oficial de la República Bolivariana de Venezuela, No. 1.024, Febrero 10, 2001.

Ley Especial Contra Delitos Informáticos (2001).Gaceta Oficial de la República Bolivariana de Venezuela, No. 37.3131, Octubre 30, 2001

Ley Orgánica de Telecomunicaciones (2011). Gaceta Oficial de la República Bolivariana de Venezuela No. 39.610; Febrero 7 de 2011

Ley Orgánica de Ciencia, Tecnología e Innovación (2014). Gaceta Oficial de la República Bolivariana de Venezuela No. 6.151; Noviembre 13 de 2014

Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (2005). Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.236. Julio 26, 2005. [Derogó la LOPCYMAT de 1986].

López, José Luis. (Anfitrión). (24 de febrero de 2020). Experto en seguridad informática: «Lo que es gratis no lo es: el valor somos nosotros» [Episodio de audio podcast]. En 970Universal. https://970universal.com/2020/02/24/experto-en-seguridad-informatica-no-estamos-en-una-burbuja-cuando-usamos-la-red/

Matteo, C. (2014). *Enfoque Teórico de Gerencia para la Sustentabilidad a partir de la relación Organización-Sociedad*. Trabajo de Tesis Doctoral presentado ante la Universidad Central de Venezuela para optar al grado de Doctora en Gerencia. Caracas. Venezuela.

Molins *Pera, M.* (1991). *Dinámica de la Planificación.* Disponible en: http://www.virtual.unal.edu.co/cursos/capitulos/ lecciones/leccion3.html.

Organización Internacional para la Estandarización. (2008). ISO 9001:2008. Sistemas de Gestión de la Calidad – Requisitos. (4ª Ed. 11-15-2008). PDF. Disponible en: www.iso.org. Consulta: 2015, Junio 14.

Organización Internacional para la Estandarización. (2013). ISO 27001. Sistemas de Gestión de Seguridad de la Información – Requisitos. (2ª Ed. 25-09-2013). PDF. Disponible en: https://www.iso.org/isoiec-27001-information-security.html. Consulta: 2018, Enero 30.

Páez, J. (1994). *Revisión de enfoques, énfasis y etapas de la planificación en Venezuela*. Disponible: http://www.virtual.edu/cursos/leccione3.html. Consulta: 2015, Abril 20.

Pagnotta, S., (2016). La Universidad de Virginia fue víctima de un phishing que robó datos tributaries. Recuperado el 28 de Agosto de 2019 de, https://www.welivesecurity.com/la-es/2016/01/25/universidad-de-virginia-victima-phishing/

Ramírez, T. (2006). Como Hacer un Proyecto de Investigación. (Nueva Ed.) Caracas. PANAPO.

Rovira, M. (2014). Use el managing apreciativo para afinar su cultura gerencial. Disponible en: http://www.elfinancierocr.com/gerencia/liderazgo/Gerencia-direccion_estrategica-liderazgo-managing_apreciativo-Manuel_Rovira_0_620937902.html. Consulta: 2016, Enero 28. (Adaptación Riera Chang, 2015).

Sabino, C. (2002). *El Proceso de Investigación*. (Nueva Edición Actualizada). Caracas. PANAPO.

Schein, Edgar (1992). *Cultura Organizacional y Liderazgo.* Barcelona, Edit. Plaza y Janes.

Steiner G. (1986). *Planificación Estratégica. Lo Que Todo Director Debe Saber*. (5ª Impresión). México. CECSA.

Susanto, H., Nabil Almunawar, M., y Chee Tuan, Y. (2017). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical / Computer Sciences, 23-29.

Tamayo y Tamayo, M. (2011). El Proceso de la Investigación Científica. (5ª Ed.). México. LIMUSA.

Universidad Pedagógica Experimental Libertador. Vicerrectorado de Investigación y Postgrado. (2016). *Manual de Trabajo de Grado de Especialización y Maestría y Tesis Doctórales.* 5ª Edición. Caracas. FEDUPEL. Autor.

Villasmil F. (2006). Análisis de los riesgos de seguridad informática, para las pequeñas y medianas empresas (PYME`S) usando el estándar ISO-17999, para la definición de políticas de seguridad que protejan sus sistemas de información. Universidad Centrooccidental "Lisandro Alvarado".Barquisimeto-Venezuela.

Zacarías Rodríguez, P. (1992). El Rol de la Planificación. Disponible en: http://www.fao.org/docrep/field/.htm. Consulta: 2015, marzo 18.

ANEXO A

INSTRUMENTO: CUESTIONARIO

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

CUESTIONARIO

El presente instrumento tiene la finalidad de obtener datos provenientes de la opinión del personal funcionarios adscritos al Departamento de Tecnología de Sistemas e Información (Dpto. DTSI) del Instituto Universitario de Tecnología- Valencia IUTVAL.

Los datos suministrados en este instrumento son de carácter estrictamente confidenciales, en consecuencia, puede expresar su opinión con absoluta libertad. De la veracidad con la cual responda el cuestionario dependerá la validez y confiabilidad de los resultados.

Instrucciones

1. Lea todas las preguntas antes de comenzar a responder. Si no entiende alguna pregunta, pida explicación a la persona que le entregó el cuestionario.

2. Suministre de manera clara y sencilla la información solicitada en cada una de las preguntas.

3. Siéntase libre de expresar su opinión personal acerca de los temas abordados.

4. Escriba con letra de molde o imprenta

5. No existen respuestas erradas, todas son válidas. Su aporte es muy valioso para el de mejoramiento de nuestros procesos administrativos.

GRACIAS POR SU VALIOSA COLABORACIÓN.

CUESTIONARIO

Instrucciones: Lea detenidamente cada ítem y responda ***marcando una X*** en la casilla según su apreciación directa como Gerente. MDA= Muy de Acuerdo, DA=De acuerdo, NINI = Ni en Acuerdo Ni en Desacuerdo, ED= En desacuerdo, MED= Muy en desacuerdo.

Ámbitos: Normativo, jurídico, científico – tecnológico, gerencial e institucional de la infraestructura operativa universitaria en instalaciones, para cumplir la labor de la Gestión de Seguridad Tecnológica (GST) para beneficio de todos.

	MDA	DA	NINI	ED	MED
1. La normativa jurídica nacional que rige la gestión de seguridad tecnológica facilita la aplicación de soluciones para gerenciar las instalaciones y servicios tecnológicos en IUTVAL.					
2. La sustentabilidad de las instalaciones y servicios tecnológicos seguros en el IUTVAL se evidencia fundamentalmente en la normativa interna.					
3. Las normas jurídicas e institucionales para la gestión de seguridad tecnológica permiten la participación protagónica de toda la comunidad universitaria para el cuido de las instalaciones y servicios tecnológicos.					
4. En el ordenamiento jurídico interno que debe aplicar el gerente de la Dirección de informática para GST, se posibilitan acciones de corresponsabilidad social para bien común del IUTVAL en servicios tecnológicos del área de seguridad.					
5. En el IUTVAL la gerencia (Dpto. DTSI) en GST, es una estructura Organizacional que puede decidir/establecer la supervisión de personas en la institución para garantizar el control, fiscalización e inspección de la universidad.					
6. Se cumple con divulgar resultados del planeamiento operativo, su registro y estadísticas al desempeño institucional de la GST, exigidos en las normativas de estado para el sector universitario a fin de divulgar las acciones de GST en la organización.					
7. La gerencia estratégica de desempeño integral en GST, NO SE FUNDAMENTA en las políticas estándares ISO de GST para la toma de decisión.					

	MDA	DA	NINI	ED	MED
8. La formulación de planes de GST en el IUTVAL está sustentada en tendencias gerenciales, garantizando el desarrollo de gestión con alcance de Validación (Planeación vs Ejecución).					
9. La gerencia de GST, esta empoderada de parámetros normativos y tendencias de última generación de las ciencias administrativas gerenciales, para implementar supuestos teóricos en gestión estratégica considerando estructura, organización y seguridad tecnológica					
10. El hecho gerencial en GST, como gestión técnica clave se registra en las memorias tecnológicas institucionales.					
11. Las herramientas científico – tecnológica en información, comunicación, hardware/software, sistemas, redes se replantean y se solicitan a lo interno de la gerencia estratégica en base a sustentar las funciones garantes de la GST, pero no se adquieren.					
12. Se cuenta en IUTVAL con líneas estratégicas para la acción de seguridad, uso o disfrute de los bienes y espacios universitarios en materia de GST.					

GRACIAS POR SU VALIOSA COLABORACIÓN.

ANEXO B

FORMATO DE VALIDACI N INSTRUMENTO

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGÍA DE LA INFORMACIÓN

Estimado especialista:

Me dirijo a usted en la oportunidad de solicitar su valiosa colaboración en el sentido de participar en el proceso de validación de un cuestionario, el cual tiene como finalidad recopilar información relacionada al estudio titulado **"MODELO DE GESTIÓN GERENCIAL DE LA SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA EN LA ORGANIZACIÓN**. **Caso: Instituto Universitario de Tecnología de Valencia".**

Con base en su destacada trayectoria y comprobada calificación profesional en su campo, se le ha considerado para emitir juicio en relación a este instrumento de investigación, a tal efecto se anexa información relativa a la investigación, el cuestionario y su respectivo instrumento de validación.

Agradecido de la colaboración prestada, me despido de usted.

Atentamente:

Ing. Jennyfer Briceño

INFORMACIÓN DE LA INVESTIGACIÓN

Título de la Investigación

MODELO DE GESTIÓN GERENCIAL DE LA SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA EN LA ORGANIZACIÓN
Caso: Instituto Universitario de Tecnología de Valencia

Objetivos de la Investigación

Objetivo General

Proponer un Modelo de Gestión estratégico para la Seguridad de la información y Tecnología favorable a la sustentabilidad de la cultura gerencial en la organización educativa IUTVAL como coformadora de capital social.

Objetivos Específicos

1. Identificar la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como coformadora de capital social en el Departamento de Tecnología de Sistemas e Información del IUTVAL.

2. Describir en el marco de la cultura gerencial, la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios en el Departamento de Tecnología de Sistemas e Información del IUTVAL.

3. Determinar las tendencias de la praxis de GST en el Departamento de Tecnología de Sistemas e Información para la seguridad tecnológica, considerando la cultura gerencial y el rol educativo de la organización IUTVAL.

4. Enunciar un conjunto de lineamientos bajo modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL como organización educativa.

Población y Muestra

Población de 9 funcionarios adscritos al Departamento de Tecnología de Sistemas e Información del IUTVAL y muestra censal de los mismos 9 profesionales universitarios en el ejercicio de funciones en el área administrativa de informática del IUTVAL.

Técnicas e Instrumentos de Recolección de Datos

Como técnica de recolección de datos se utilizará la encuesta, la cual será implementada mediante un cuestionario tipo Lickert buscando obtener datos acerca de los siguientes aspectos:

1. Relación entre las Leyes del estado y procedimientos internos, facilidades de su aplicación
2. Perdurabilidad de los espacios y servicios de GST.
3. Programabilidad de planes y técnicas de solución de problemas de GST.
4. Direccionalidad y coherencia en los lineamientos de gestión y gerencia de GST.
5. Racionalidad entre el dominio de la teoría y el uso de las tecnologías (hardware y software)
6. Verificación de las necesidades de formular la propuesta sobre los lineamientos estratégicos de GST.

Operacionalización de Variables

Objetivo específico	Variable	Dimensión	Indicadores	Ítem
Identificar la vinculación entre el ámbito jurídico de la gestión en seguridad tecnológica y su sustentabilidad gerencial como coformadora de capital social en el D.T.S.I. del IUTVAL	*Normativa*	Leyes del estado y reglamentos internos	Ejecución de procesos	1
	Sustentabilidad	Perdurabilidad de los espacios y servicios de seguridad tecnológica	Satisfacción	2
			Participación	3
			Corresponsabilidad	4
Describir en el marco de la cultura gerencial, la actitud que tienen los responsables de seguridad tecnológica en el IUTVAL, considerando la calidad de las instalaciones, dotación oportuna, tecnología instalada y servicios en el D.T.S.I. del IUTVAL.	*Toma de Decisiones*	Programa-bilidad y técnicas de solución de problemas para Seguridad tecnológica.	Supervisión Control	5 6
			Políticas estándares	7
Determinar las tendencias de la praxis de GST en el D.T.S.I. para la seguridad tecnológica, considerando la cultura gerencial y el rol educativo de la organización IUTVAL.	*Ámbito teórico/práctico científico - tecnológico*	Racionalidad, técnicas teóricas y aplicadas en materia de seguridad tecnológica.	Formación	8 9
			Comunicación	10
			Uso de tecnologías	11
Enunciar un conjunto de lineamientos bajo modelo estratégico de gestión en seguridad tecnológica favorable al IUTVAL como organización educativa.	*Requerimientos de estrategias novedosas*	Verificación de la necesidad socio-tecnológica favorable	Carencia de modelo gestión estratégica en seguridad tecnológica	12

Fuente: Autora (Briceño, 2021)

PLANILLA DE EVALUACIÓN DEL INSTRUMENTO

Nombres y Apellidos del Evaluador: Henry José Gil Guzmán
Cédula de Identidad: 6.442.559 **Teléfono(s):** 0424-4693138
Formación Académica: MSc. en Educación Superior
Áreas de experiencia laboral: Docente Universitario
Institución: Instituto Universitario de Tecnología de Valencia
Cargo Actual: Docente Universitario
Tiempo: 18 años
Instrucciones: De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
Suficiencia: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente
	4. Alto nivel	Los ítems son suficientes
Claridad: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
Relevancia: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

¿Hay alguna modificación sugerida a la redacción de alguna pregunta? ¿Cuál? No hay ninguna modificación

¿Hay alguna dimensión que es parte del estudio y no fue evaluada? ¿Cuál? El instrumento abarca todas las dimensiones

Instrumento de investigación a evaluar: Cuestionario.

Puntaje individual Promedio puntaje

Dimensión	Indicadores	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observaciones
Leyes del estado y reglamentos internos	Ejecución de procesos	1	4	4	4	4	
Perdurabilidad de los espacios y servicios de seguridad tecnológica	Satisfacción	2	4	4	4	4	
	Participación	3	4	4	4	4	
	Corresponsabilidad	4	4	4	4	4	
Programabilidad y técnicas de solución de problemas para Seguridad tecnológica	Supervisión	5	4	4	4	4	
		6	4	4	4	4	
	Liderazgo	7	4	4	4	4	
Racionalidad, técnicas teóricas y aplicadas en materia de seguridad tecnológica	Formación	8	4	4	4	4	
		9	4	4	4	4	
	Comunicación	10	4	4	4	4	
	Uso de tecnologías	11	4	4	4	4	
Verificación de la necesidad socio-tecnológica favorable	Carencia de gestión estratégica	12	4	4	4	4	

6442.559

15/08/2021

Firma del Evaluador **Cédula** **Fecha**

PLANILLA DE EVALUACIÓN DEL INSTRUMENTO

Nombres y Apellidos del Evaluador: Yerlin Yamileth Colmenares Guanipa
Cédula de Identidad: 14.304.178 **Teléfono(s):** 0412-7400308
Formación Académica: MSc. en Tecnología Educativa
Áreas de experiencia laboral: Docente Universitario
Institución: Instituto Universitario de Tecnología de Valencia
Cargo Actual: Docente Universitario
Tiempo: 16 años
Instrucciones: De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
Suficiencia: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente
	4. Alto nivel	Los ítems son suficientes
Claridad: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
Relevancia: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

¿Hay alguna modificación sugerida a la redacción de alguna pregunta? ¿Cuál? No hay ninguna modificación

¿Hay alguna dimensión que es parte del estudio y no fue evaluada? ¿Cuál? El instrumento abarca todas las dimensiones

Instrumento de investigación a evaluar: Cuestionario.

Puntaje individual Promedio puntaje

Dimensión	Indicadores	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observaciones
Leyes del estado y reglamentos internos	Ejecución de procesos	1	4	4	4	4	
Perdurabilidad de los espacios y servicios de seguridad tecnológica	Satisfacción	2	4	4	4	4	
	Participación	3	4	4	4	4	
	Corresponsabilidad	4	4	4	4	4	
Programabilidad y técnicas de solución de problemas para Seguridad tecnológica	Supervisión	5	4	4	4	4	
		6	4	4	4	4	
	Liderazgo	7	4	4	4	4	
Racionalidad, técnicas teóricas y aplicadas en materia de seguridad tecnológica	Formación	8	4	4	4	4	
		9	4	4	4	4	
	Comunicación	10	4	4	4	4	
	Uso de tecnologías	11	4	4	4	4	
Verificación de la necesidad socio-tecnológica favorable	Carencia de gestión estratégica	12	4	4	4	4	

Firma del Evaluador **Cédula** **Fecha**

14304178. 21/08/2021

PLANILLA DE EVALUACIÓN DEL INSTRUMENTO

Nombres y Apellidos del Evaluador: Winston Rafael Magdaniel
Cédula de Identidad: 13.049.115 **Teléfono(s):** 0426-272.88.67
Formación Académica: MSc. en Ciencias de la Educación
Áreas de experiencia laboral: Docente
Institución: Instituto Liceo Josefina Espinoza
Cargo Actual: Docente y Coordinador Área de Idiomas
Tiempo: 15 años
Instrucciones: De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
Suficiencia: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente
	4. Alto nivel	Los ítems son suficientes
Claridad: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
Relevancia: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

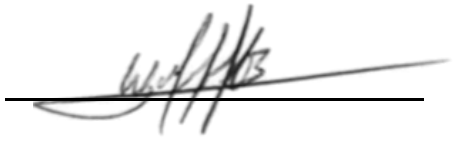
¿Hay alguna modificación sugerida a la redacción de alguna pregunta? ¿Cuál? No hay ninguna modificación

¿Hay alguna dimensión que es parte del estudio y no fue evaluada? ¿Cuál? El instrumento abarca todas las dimensiones

Instrumento de investigación a evaluar: Cuestionario.

Puntaje individual Promedio puntaje

Dimensión	Indicadores	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observaciones
Leyes del estado y reglamentos internos	Ejecución de procesos	1	4	4	4	4	
Perdurabilidad de los espacios y servicios de seguridad tecnológica	Satisfacción	2	4	4	4	4	
	Participación	3	4	4	4	4	
	Corresponsabilidad	4	4	4	4	4	
Programabilidad y técnicas de solución de problemas para Seguridad tecnológica	Supervisión	5	4	4	4	4	
		6	4	4	4	4	
	Liderazgo	7	4	4	4	4	
Racionalidad, técnicas teóricas y aplicadas en materia de seguridad tecnológica	Formación	8	4	4	4	4	
		9	4	4	4	4	
	Comunicación	10	4	4	4	4	
	Uso de tecnologías	11	4	4	4	4	
Verificación de la necesidad socio-tecnológica favorable	Carencia de gestión estratégica	12	4	4	4	4	



23/08/2021

13 049.115

Firma del Evaluador **Cédula** **Fecha**

ANEXO C

CONFIABILIDAD DEL INSTRUMENTO

CONFIABILIDAD

	Items												
Sujetos	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**total**
1	1	3	2	2	2	2	3	1	2	3	2	5	28
2	3	1	4	4	5	2	5	2	2	5	5	2	40
3	2	1	2	2	2	2	4	4	1	3	4	5	32
4	3	2	5	4	5	4	4	4	2	4	5	4	46
5	3	3	1	2	1	1	2	3	1	4	4	5	30
6	2	2	4	2	4	5	5	4	4	2	5	2	41
7	2	2	2	3	3	2	5	2	2	1	2	2	28
8	2	3	1	1	2	1	2	5	4	2	5	2	30
9	1	2	1	1	2	2	2	1	1	2	2	1	18
Promedio	2,111	2,111	2,444	2,333	2,889	2,333	3,556	2,889	2,111	2,889	3,778	3,111	32,556
Varianza	0,611	0,611	2,278	1,250	2,111	1,750	1,778	2,111	1,361	1,611	1,944	2,611	20,028
TOTAL	20	21	25	25	31	27	39	34	28	36	45	40	371
Desviacion Estandar	0,781736	0,781736	1,5092309	1,118034	1,4529663	1,3228757	1,3333333	1,4529663	1,1666667	1,2692955	1,3944334	1,6158933	15,199167

ALPHA=0,95

Numero de Items = 12

Numero de Items - 1 grado de libertad = 11

Sumatoria de Varianza Items individuales (St^2) = 20,03

Opciones de respuestas de los Items: Muy De Acuerdo=5, De Acuerdo=4, Ni de Acuerdo Ni en Descuerdo=3, En Desacuerdo=2, Muy En Desacuerdo=1

ANEXO D
POLÍTICAS DE SEGURIDAD

POLÍTICAS DE SEGURIDAD INFORMÁTICA			
MÓDULO	**PROPÓSITO**	**ALCANCE**	**NORMAS**
GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN	Normar el registro, gestión y control de los activos fijos y bienes de propiedad del Departamento de Tecnología de Sistemas de Información	Estandarizar el proceso para el manejo de los activos fijos y bienes el registro informáticos y documentos en que conste la historia de cada bien, su destinación y uso; e identificar y designar al personal que recibe el bien para el desempeño de sus funciones.	a) Todos los aspectos que no se encuentren normados de forma expresa en este documento deben ser complementados o suplidos por las disposiciones del Consejo Directivo. b) El personal que incumpliere sus obligaciones o contraviniere las disposiciones de esta Política, así como las leyes y normativa conexa, debe incurrir en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho. c) El Consejo Directivo debe contratar pólizas de seguro de los activos para protegerlos contra diferentes riesgos que pudieran ocurrir; se actualizarán periódicamente, a fin de que las coberturas mantengan su vigencia. d) El DTSI de la Institución establecerá una codificación adecuada que permita una fácil identificación, organización y protección de los activos. Todos los activos llevarán etiquetas impresas con el número de Bienes Nacionales correspondiente en una parte visible, permitiendo su fácil identificación. e) Es responsabilidad del DTSI mantener registros actualizados, individualizados, numerados, debidamente organizados y archivados, para que sirvan de base para el control, localización e identificación de los equipos informáticos, hardware, software y medios de comunicación. f) Es responsabilidad de cada Jefatura Académica y/o Administrativa, garantizar el uso adecuado de los activos informáticos, a fin de determina si las condiciones de custodia son adecuados y no se encuentran en riesgo. g) El DTSI debe tener un inventario de lo siguiente: · Procesos estratégicos y de apoyo para la institución. · Las normas y reglamentos que son la razón de ser de la institución. · Los archivos generados por el personal tanto de manera física como digital, esto dependerá de las funciones que realiza la institución. · Archivos del desarrollo, soporte de los nuevos y anteriores sistemas informáticos.

POLÍTICAS DE SEGURIDAD INFORMÁTICA			
MÓDULO	**PROPÓSITO**	**ALCANCE**	**NORMAS**
SEGURIDAD EN RELACIÓN A RECURSOS HUMANOS	Establecer las normas para la gestión de la seguridad del personal del IUTVAL	El presente documento es de aplicación para todo el personal del IUTVAL.	a) El personal del IUTVAL, debe declarar el entendimiento y compromiso de las normas del presente documento, a través del conocimiento y aceptación del acuerdo de Confidencialidad de la Información, y los mecanismos que se establezcan para la contratación y selección de personal. De igual manera, el personal externo autorizado manifiesta su compromiso de cumplimiento de las normas de seguridad de la información, a través de los respectivos contratos, convenios, u otros instrumentos que defina el Consejo Directivo para este efecto. b) Es responsabilidad de Recursos Humanos verificar la documentación presentada por los candidatos, previa contratación, además de: · Verificar antecedentes de los posibles candidatos a ser empleados, proveedores o contratistas que vayan a tener alguna relación con la institución. · Validar que el nuevo personal firme el acuerdo de confidencialidad y de no – divulgación de la información de la institución, antes de cualquier acceso a la información. · Indicar las funciones y responsabilidades a desarrollar formalmente, por parte del nuevo personal contratado. · Notificar al Oficial de Seguridad de la Información para la activación de los accesos a los servicios o recursos tecnológicos, facilitados por la institución. c) Las jefaturas deben asignar al personal a su cargo, los perfiles y roles de acceso a la información que corresponda a través de las aplicaciones informáticas institucionales, así como los servicios y recursos tecnológicos necesarios para el cumplimiento de sus funciones y responsabilidades. d) Es responsabilidad de las jefaturas concientizar, socializar y capacitar de forma periódica sobre las normas seguridad de la información que deben tomar en cuenta en el desarrollo de sus funciones en la institución, y de las responsabilidades. e) La Jefatura en conjunto con Recursos Humanos consideraran las sanciones que se le aplicará al personal que por algún motivo, cometió alguna irregularidad o no cumplimiento a las disposiciones emitidas en el presente documento, el mismo que debe considerar la gravedad del evento así como el impacto al negocio. f) Al término de la relación laboral de un servidor, la respectiva Jefatura debe asegurar la entrega y recepción de la información de la empresa a cargo del personal saliente, y debe mantenerla bajo su custodia hasta que concluyan los plazos de retención respectivos. Se debe confirmar la devolución de los activos de la institución, incluida la información física o digital, el retiro de los derechos de acceso a los sistemas informáticos, servicios y recursos tecnológicos. g) El DTSI, conjuntamente con cada la Jefatura son responsables de la seguridad de la información física o digital, y deben promover procesos de comunicación y concienciación al personal del IUTAL, respecto a los riesgos, responsabilidad y compromiso en el cuidado de la información de la empresa. h) El personal que por motivo de desvinculación del IUTVAL está en la obligación de este trasmitir toda la información y el conocimiento sobre su cargo al nuevo personal o a su jefatura inmediata.

POLÍTICAS DE SEGURIDAD INFORMÁTICA			
MÓDULO	**PROPÓSITO**	**ALCANCE**	**NORMAS**
GESTIÓN DE COMUNICACIONES Y OPERACIONES	Establecer las normas que regulen la Gestión de las Comunicaciones y Operaciones, con el propósito de proteger la Información almacenada en los computadores dentro de la infraestructura tecnológica del IUTVAL y minimizar la exposición ante las amenazas	El cumplimiento de las normas de este documento es obligatorio para todo el personal del IUTVAL.	a) El DTSI debe implementar los mecanismos y controles necesarios para garantizar la disponibilidad de los servicios y recursos tecnológicos que posee la institución. b) Es responsabilidad del DTSI el respaldo de la información que la jefatura inmediata considere pertinente en un período no mayor a 180 días y su restauración de la información y los sistemas que manejan la empresa. c) La elaboración de los instructivos para el manejo de errores, inconvenientes o problemas que pueden presentarse en la infraestructura tecnológica de la institución, así también como el reinicio y recuperación de los sistemas informáticos en caso de fallas es de responsabilidad del DTSI.

POLÍTICAS DE SEGURIDAD INFORMÁTICA			
MÓDULO	**PROPÓSITO**	**ALCANCE**	**NORMAS**
CONTROL DE ACCESOS	Regular el proceso de administración y control de accesos lógicos para usuarios finales, alineado a las mejores prácticas de seguridad de la información, a fin de mitigar los riesgos de accesos y uso indebido de los mismos.	El presente documento contempla los procedimientos que forman parte del proceso de administración y control de accesos lógicos para usuarios finales del IUTVAL	a) Para los accesos a la red de datos y a la infraestructura tecnológica del IUTVAL, se debe establecer mecanismos de autenticación que garanticen la identificación del personal de la y/o personal externo debidamente autorizado, al igual que de los computadores de escritorio y/o portátiles y equipos periféricos de la infraestructura tecnológica de la empresa. b) El control de accesos lógicos se basara en la creación de usuarios específicos y únicos asignados a los funcionarios que requieran acceso a los sistemas informáticos, así como a la infraestructura tecnológica. c) Para los casos que de no cumplir con lo indicado en el ítem anterior, se creará cuentas genéricas; las mismas que deben estar asignado a un personal responsable. d) El uso de contraseñas, cuentas individuales y/o genéricas es intransferible; para el caso de cuentas genéricas estas deben ser asignadas y registradas a una persona de la institución responsable de la misma. e) Cuando un usuario finalice su relación laboral y/o contractual con la institución, el DTSI debe proceder a la deshabilitación inmediata y definitiva del usuario de red, aplicaciones informáticas, servicios y recursos tecnológicos, así como la revocatoria de los respectivos perfiles, roles, y privilegios que tenía autorizado.