UNIVERSIDAD DE GUANAJUATO

DIVISIÓN DE CIENCIAS ECONÓMICO ADMINISTRATIVAS

GESTION DE SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. CASO: UNIVERSIDAD DE GUANAJUATO

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MAESTRÍA EN ADMINISTRACIÓN

P R E S E N T A
VERÓNICA NOEMI MOSQUEDA RAMÍREZ

DIRECTOR DE TESIS:
DRA. LAURA ELENA ZARATE NEGRETE

CODIRECTOR:
DR. FRANCISCO JAVIER VELÁZQUEZ SAGAHÓN

GUANAJUATO, GTO., 2020

UNIVERSIDAD DE GUANAJUATO

DIVISIÓN DE CIENCIAS ECONÓMICO ADMINISTRATIVAS

GESTION DE SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. CASO: UNIVERSIDAD DE GUANAJUATO

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MAESTRÍA EN ADMINISTRACIÓN

P R E S E N T A
VERÓNICA NOEMI MOSQUEDA RAMÍREZ

DIRECTOR DE TESIS:
DRA. LAURA ELENA ZARATE NEGRETE

CODIRECTOR:
DR. FRANCISCO JAVIER VELÁZQUEZ SAGAHÓN

GUANAJUATO, GTO., 2020

AGRADECIMIENTOS

A LA UNIVERSIDAD DE GUANAJUATO

Por ser mi alma mater, y dar continuidad a mi desarrollo académico, profesional y humano.

"LA VERDAD OS HARÁ LIBRES"

A MI ASESORA LA DRA. LAURA ELENA ZARATE Y MI CODIRECTOR EL DR. FRANCISCO JAVIER VELAZQUEZ

Con profundo agradecimiento por el apoyo, la constante motivación, su conocimiento y guía que me brindaron que me oriento en la realización de este trabajo.

De todo corazón gracias.

A MIS PADRES

DAVID MOSQUEDA Y LOURDES RAMÍREZ

Por darme la vida y porque a través de su educación, su apoyo incondicional y amor me han guiado. Todo lo que hoy soy se lo debo a ellos.

Mi eterna gratitud.

A MI ESPOSO

MARCO A. CASTILLO

Por apoyarme día a día para alcanzar nuevas metas tanto profesionales como personales, creer en mi capacidad, brindándome tu comprensión, cariño y amor.

A MI HIJO

EMILIO CASTILLO

Agradezco tu amor y compresión, eres mi principal motivación.

A MIS HERMANOS

JESSICA, BRENDA Y EDUARDO

Por ser parte importante de una hermosa familia, son y han sido una gran compañía, hermano querido te dedico mi esfuerzo donde te encuentres.

AL COORDINADOR DE SEGURIDAD Y AMIGO

JORGE OMAR MARTINEZ

Te agradezco por tu desinteresada ayuda, por apoyarme siempre que lo necesité y por aportar considerablemente en mi proyecto. Te agradezco no solo por la ayuda brindada sino también por tu amistad mostrada.

A MIS AMIGOS

A todos aquellos que me dan su amistad incondicional y que han compartido conmigo varios momentos inolvidables, siempre serán parte importante de mi vida.

Gracias a la vida por este logro y a todas las personas que me apoyaron y creyeron en este proyecto.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Los constantes cambios en el mundo moderno, que están representados por un continuo desarrollo, una acelerada globalización, y la rápida evolución de la informática donde las computadoras y la conexión en red han cambiado la forma en que el ser humano percibe el mundo; con una pronunciada dependencia hacia un alto grado de información ha transformado fuertemente la cultura, que para casi todo el quehacer humano es necesario el utilizar la tecnología.

Por lo tanto, las computadoras y dispositivos móviles están involucrados de alguna manera en la mayoría de nuestras actividades diarias, como en los negocios de cualquier organización: empresas, instituciones educativas y áreas de gobierno, en las cuales sin el apoyo de estas herramientas ninguna de estas organizaciones sería capaz de manejar la impresionante cantidad de información que parece caracterizar a nuestra sociedad.

Sin embargo, siempre que interactuamos directa o indirectamente con tecnologías, dejamos rastros de datos que pueden utilizarse para generar información sobre nuestras vidas y actividades, se recopila una cantidad considerable y creciente de información sobre nosotros que se procesa, almacena, explora, comparte, comercializa y puede ser utilizada indebidamente tanto por individuos como por organizaciones públicas y privadas (Narain, Gupta y Ojha, 2014)

Independientemente de que sean organizaciones gubernamentales, privadas o públicas, la mayoría de ellas están aplicando actualmente una serie de medidas, políticas, procedimientos y directrices de seguridad para proteger a sus organizaciones. Esta concienciación se debió al hecho de que los incidentes de seguridad pueden llevar a consecuencias severamente adversas para las organizaciones, como pérdidas sustanciales a través de la pérdida directa de activos de información con impacto financiero.

Por lo cual, el presente trabajo surge al ver la importancia de la información y la necesidad de resguardarla de las posibles eventualidades que puedan surgir. Dentro de la literatura se define a la seguridad de la información (SI) como un conjunto de procesos,

procedimientos, personal y tecnología encargados de proteger los activos de información de una organización (Jourdan, Rainer, Marshall y Ford, 2010)

Ahora bien, este estudio está enfocado en las instituciones educativas públicas de nivel superior teniendo como caso de estudio la Universidad de Guanajuato enfocándonos en la gestión de seguridad de la información, cuyo objetivo es identificar los factores clave que impactan en la gestión de seguridad de la información dentro de la Universidad de Guanajuato, con base en una perspectiva de gestión estratégica para proponer pautas que propicien una gestión de seguridad de la información más eficaz.

Esta tesis delimitará su estudio en tiempo y en espacio, es decir, se toma como estudio la Dirección de Servicios y Tecnologías de la Información, ya que representa la cabeza estratégica de seguridad de la información dentro de la Universidad de Guanajuato, el presente es un estudio cualitativo, transversal de alcance descriptivo. La investigación no es experimental porque se realizó sin manipular intencionadamente las variables y sin asignar casualmente a los participantes, con una muestra no probabilística y usando como instrumento la entrevista guiada.

Se busca analizar y elevar la conciencia sobre las problemáticas en gestión de seguridad de la información que se tiene para establecer una seguridad de la información favorable para la Universidad de Guanajuato, ya que esto es algo implícito que está en el funcionamiento de cualquier organización. También se debe tomar en cuenta que se tiene que establecer una gestión de seguridad de la información que sea adecuada a la cultura organizacional y que a su vez esté conforme a las normativas.

Para la presente investigación fue necesario seleccionar las diferentes fuentes que han sido ejemplares por los aportes que hacen sobre el tema Seguridad de la información y la Gestión de seguridad de la información, en el que se retomó respaldos teóricos que ofrecen en este estudio precisiones conceptuales y una reflexión para portar en los trabajos de investigación. Por lo cual, esta investigación está estructurada de la siguiente manera:

En el Capítulo I se presenta el marco teórico sobre la seguridad de la información, se aborda a los principales estudiosos sobre el tema, su importancia organizacional y sus características principales, seguido de la gestión y características de esta.

El Capítulo II Marco Contextual presenta el estado actual de la seguridad de la información con el objetivo de dimensionar la importancia que tiene, desde un punto internacional hasta centrarse en el caso de estudio la Universidad de Guanajuato.

En el Capítulo III Metodología se desarrolla el proceso que tuvo esta investigación, se presentan los informantes clave y las técnicas e instrumentos utilizados para obtener la información necesaria para esta investigación y por último se destaca a la Hermenéutica-Analógica como una técnica de interpretación social destacada por Beuchoty, Velázquez y Nava.

En el Capítulo IV Resultados se narra todos los datos obtenidos a través de los informantes claves por medio de la técnica de la Hermenéutica-Analógica, en donde se detectan factores que intervienen en el desempeño de la Gestión de seguridad de la información dentro de la Universidad de Guanajuato.

Finalmente se cierra con las conclusiones de este trabajo de investigación y de análisis, se agregan algunas recomendaciones, así como futuras líneas de investigación que se deben tomar en cuenta para mejorar esta investigación.

Planteamiento del problema

Los incidentes de seguridad de la información hoy en día no sólo ocurren a las instituciones de los sectores productivos, financieros o gobiernos. Las instituciones educativas también son blancos de ataques, donde con mayor frecuencia se maneja información de carácter privado, relacionada con el control escolar, administrativo, financiero e incluso de las investigaciones de la institución, así como la información personal de alumnos, académicos y administrativos. Y aunque las instituciones educativas de nivel superior tienen a su cargo gran cantidad de información, desafortunadamente solo 4 de cada 10 Instituciones educativas de nivel superior tienen definida una política de seguridad de la información. De las 91 IES que tienen una política de seguridad establecida, un 35% está alineada a los objetivos institucionales, un 21% no incluye objetivos y un 5% indica que existen políticas que incluyen objetivos, pero no están alineados a los objetivos institucionales (ANUIES, 2017).

Objetivo general

Identificar los factores clave que impactan en la gestión de seguridad de la información dentro de la Universidad de Guanajuato, con base en una perspectiva de gestión estratégica para proponer pautas que propicien una gestión de seguridad de la información más eficaz.

Objetivos específicos

- Conocer los Factores Críticos de Éxito de la Gestión de Seguridad de la Información.
- Analizar e identificar los elementos clave de la gestión de seguridad de la información actualmente implementados en la Universidad de Guanajuato.
- Desarrollar estrategias para la gestión de seguridad de la información en la Universidad de Guanajuato.

Supuestos de investigación

- La alineación institucional contribuye a una mayor conciencia de los riesgos y controles de seguridad de la información.
- El soporte de los altos directivos influye en el desempeño de la gestión de seguridad de la información.

Justificación

Los datos arrojados por diferentes instituciones muestran una perspectiva de la importancia de la seguridad de la información en la actualidad y con base a esto se argumenta la presente investigación. Se tomaron en cuenta que la mayoría de las organizaciones han reemplazado sustancialmente la forma física de datos con formas electrónicas según lo permiten las redes de banda ancha actuales y las tecnologías de almacenamiento de información electrónica.

Los datos arrojados por diferentes instituciones muestran una perspectiva de la importancia de la seguridad de la información en la actualidad. El Informe de riesgo global del 2012 del Foro Económico Mundial, coloco los riesgos de ataques a sistemas informáticos o red entre los cinco principales que el mundo enfrentaría en la próxima década. Es difícil encontrar indicadores confiables del impacto financiero de los ataques en red en las organizaciones, sin embargo, con base a los datos del Ponemon Institute, el costo promedio del crimen de ataques cibernéticos para una muestra de 50 grandes empresas estadounidenses fue de US $ 5.9 millones por año, un incremento anual del 56%. Se sugiere que los riesgos a un sistema o red constituyen una amenaza significativa para las empresas, pero se necesita más información para permitir que las organizaciones evalúen el alcance del riesgo, ya que muchas siguen sin informarse (Foro económico mundial, 2012).

En México uno de los casos más notables, fue en el 2018 con la intrusión que afectó al Sistema de Pagos Electrónicos Interbancarios. El monto del dinero sustraído de los bancos se dice que fue entre los 400 a 800 millones de pesos (entre US$21 y US$42 millones). Este caso da ejemplo de cómo la alteración de la información puede verse reflejada de manera financiera (BBC Mundo, 2018).

Con base en dichos datos se sabe que la información es uno de los bienes más propenso a vulnerabilidades al mismo tiempo es uno de los recursos importantes dentro de la organización, por lo cual es necesario protegerla de amenazas internas y externas. Esta concienciación se debió al hecho de que los incidentes de seguridad pueden llevar a consecuencias severamente adversas para las organizaciones, como pérdidas sustanciales para la industria a través de la pérdida directa de activos de información e

impacto financiero, una pérdida en la reputación de la organización, la confianza del cliente y una pérdida de la productividad de los empleados o el riesgo de problemas legales.

CAPÍTULO 1. MARCO TEÓRICO

SEGURIDAD DE LA INFORMACIÓN

La era actual con su rápido avance tecnológico ha planteado nuevas amenazas a la información y a cada una de sus etapas en el ciclo de vida (generación de información, procesamiento, almacenamiento y distribución) en las organizaciones. Por lo tanto, actualmente los desafíos de seguridad de la información no es simplemente un problema técnico, los aspectos de gestión y comportamiento también son de importancia.

La disciplina de seguridad de la información ha madurado durante un período de tiempo con el entorno cambiante del uso de la información, la dependencia de las empresas con respecto a los sistemas de información y en consecuencia los diferentes escenarios de riesgo y/o amenaza.

La seguridad de la información ha sido definida desde múltiples perspectivas (Tabla 1), teniendo sus principios en 1990, durante este periodo se habla de una seguridad de la información con solo un enfoque técnico, orientado hacia el uso de contraseñas que aparecieron en 1980 para restringir a los usuarios entre computadoras.

Seguido de ello se presenta una definición que actualmente es dominante dentro de la literatura presentada por el Instituto Nacional de Estándares y Tecnología[1] (NIST, 2013) esta definición se basa en las siguientes tres propiedades:

- Confidencialidad: propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
- Integridad: propiedad de exactitud y exhaustividad.
- Disponibilidad: propiedad de ser accesible y utilizable a pedido de una entidad autorizada.

NIST es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia

[1] Traducido del inglés *National Institute of Standards and Technology*

industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

La Organización Internacional de Normalización (ISO) sigue los mismos principios presentados por el NIST, en ISO / 27002 (2016), define la seguridad de la información en los servicios en términos de confidencialidad, integridad, no repudio, identificación, autenticación y autorización. En el contexto de ISO la información puede tomar muchas formas, puede imprimirse o escribirse en papel, almacenarse electrónicamente, transmitirse por correo o por medios electrónicos, mostrarse en películas, transmitirse en conversación, etc. Existen otros autores como: Hong, Chi, Chao y Tang (2006), Whitman y Mattord (2009), Narain, Gupta y Ojha, (2014), que presentan definiciones en las que prevalecen estos tres aspectos: la confidencialidad, integridad y disponibilidad de la información.

Sin embargo, estas definiciones no incluyen los efectos humanos sobre la seguridad, por otro lado, actualmente también existen otras definiciones que permiten de manera más flexible términos explicativos de seguridad. Autores como: Ashenden (2008), Hagen, Albrechtsen, y Hovden, (2008), Herath y Rao (2009), Werlinger, Hawkey y Beznosov (2009) y Jourdan, Rainer, Marshall y Ford (2010), definen la seguridad de la información como un conjunto de procesos, procedimientos, personal y tecnología encargados de proteger los activos de información de una organización. Esta definición es más integral abarca todas las perspectivas y permite el estudio de los seres humanos, las organizaciones, la cultura, la ética, las políticas y la ley.

Tabla 1. *Conceptos seguridad de la información.*

Enfoque	Autores	Conceptos
Técnico	Posthumus y Von Solms, 2004	Disciplina multidimensional que ayuda a mitigar el riesgo de la información mediante la aplicación de una combinación adecuada de controles de seguridad.

	Hong, 2006	Métodos técnicos y procesos de gestión en los recursos de información.
	Instituto Nacional de Estándares y Tecnología, 2013	Confidencialidad, integridad y disponibilidad.
	ISACA, 2016	La seguridad de la información se ocupa de la información, independientemente de su formato, abarca documentos en papel, propiedad digital e intelectual en la mente de las personas y comunicaciones verbales o visuales.
Visión integral	Ashenden, 2008	Seguridad de la Información tiene como objetivo ofrecer beneficios reales de negocio ahora tanto por la protección y, sin embargo, facilitar el intercambio controlado de la información y la gestión de los riesgos asociados a través de un entorno cambiante amenaza.
	Hagen *et al*., 2008	Con el fin de minimizar la complejidad de las medidas de seguridad de la organización estudiados en este trabajo, las medidas se clasifican en cuatro grupos principales: la política de seguridad; procedimientos y control; herramientas no tecnológicas y métodos y la creación de conciencia individual y organizacional y mantenimiento.
	Herath y Rao, 2009	Seguridad eficaz información de la organización depende de los tres componentes, a saber: personas, procesos y tecnología.
	Werlinger *et a*l., 2009	Elementos tecnológicos humanos, organizativos, y la interacción podría explicar cómo los diferentes factores que conducen a las fuentes de las

	brechas de seguridad y vulnerabilidades dentro de las organizaciones.
Jourdan *et al*., 2010	Conjunto de procesos, procedimientos, personal y tecnología encargados de proteger los activos de información de una organización.
Craigen et al., 2014	Considera la seguridad de la información como la recopilación y configuración de recursos, procesos y estructuras empresariales contra ataques maliciosos.

Fuente: Autoría propia.

Después de conocer la definición integral de seguridad de la información es importante mencionar la diferencia que existe entre términos que en ocasiones se suelen utilizar como sinónimos a pesar de que difieren. Es importante tener en cuenta que existe una diferencia entre la seguridad de la información, la seguridad de la tecnología de la información y ciberseguridad.

La seguridad cibernética (ciberseguridad), a pesar de que a menudo se usa como un término análogo para la seguridad de la información, difiere de esta. En la seguridad cibernética la información y las tecnologías de la información son causas de vulnerabilidad, ya que los activos que trata la ciberseguridad pueden ser información o infraestructura de información y comunicación. La característica más determinante de la seguridad cibernética es el hecho de que todos los activos deben protegerse de las vulnerabilidades que existen como resultado del uso de las tecnologías de información y comunicación (TIC) que forman la base del ciberespacio. De hecho, dichos activos incluyen absolutamente a cualquier persona o cosa que pueda alcanzarse a través del ciberespacio.

Entonces el término de seguridad cibernética si se relaciona con la seguridad de la información, pero no es un sinónimo con el termino seguridad de la información.

En el caso de la seguridad de las TIC, los activos que deben protegerse son la infraestructura de tecnología de la información. La seguridad de la información, por otro lado, extiende esta definición de los activos a proteger para incluir todos los aspectos de la información en sí. Por lo tanto, incluye la protección de los activos de TIC, y va más allá de la tecnología para incluir información que no se almacena o comunica directamente mediante el uso de las TIC.

Marcos de Referencia de Seguridad de la Información

En casi todas las áreas del conocimiento se requieren estándares que permitan establecer bases y criterios para la excelencia y el campo de la seguridad de la información no es la excepción (Solano, 2016). Al adoptar una guía autorizada, las organizaciones pueden demostrar su compromiso con las prácticas comerciales seguras; las organizaciones pueden solicitar una certificación, acreditación o una clasificación de madurez de seguridad que acredite su cumplimiento de un conjunto de reglas y prácticas.

Existen razones que están detrás del desarrollo de estándares y juegan un papel crucial en la mejora de los enfoques de seguridad de la información; Tsohou, Kokolakis, Lambrinoudakis y Gritzalis, (2010), mencionan los siguientes beneficios de la estandarización:

- Facilitación de una mejor comunicación entre humanos y organizaciones.
- Mejorar la eficiencia y eficacia de los procesos clave.
- Facilitar la integración de sistemas e interoperabilidad.
- Dar derecho a varios productos o métodos, que deben compararse significativamente.
- Proporcionar un medio para que los usuarios evalúen nuevos productos o servicios.
- Estructurar el método para desplegar nuevas tecnologías o modelos de negocio.
- Simplificar entornos complejos.
- Promover el crecimiento económico.

Los marcos de referencia de la seguridad de la información requieren una interpretación cuidadosa para los entornos organizacionales actuales, ya que en la primera lectura parecen estar sesgados hacia grandes centros de computación. No obstante, proporcionan una importante declaración autorizada para la alta gerencia y extensas listas de verificación de medidas de seguridad. Se recomienda a los administradores de seguridad que elaboren

directrices locales, basándose en una interpretación informada de los estándares, adaptados a la organización y luego presenten un informe inicial para la alta gerencia. Dicho informe debe detallar en qué medida el nivel organizativo de la gestión de la seguridad de la información es o no compatible con las directrices.

Entonces, la cantidad de seguridad requerida por una organización (los requisitos de seguridad) normalmente provienen de tres fuentes (BS 7799-1, 1999).

- El primero se deriva de la evaluación de los riesgos para la organización.
- El segundo es el de los requisitos legales, legales reglamentarios y contractuales que debe cumplir la organización; y
- En tercer lugar, el conjunto particular de principios, objetivos y requisitos para el procesamiento de la información que una organización ha desarrollado para respaldar sus operaciones (Humphreys, 1998).

Una vez que se hayan determinado los requisitos de seguridad, se debe identificar el conjunto de controles de seguridad más efectivo para proporcionar ese nivel de seguridad. Como se vio en la primera de estas tres fuentes, el análisis de riesgos todavía puede desempeñar un papel en la obtención de información, pero como un componente secundario de los requisitos de seguridad.

Dichos análisis de riesgo de seguridad involucran documentación del escenario de seguridad organizacional actual y es probable que esta sea una tarea importante cuando se realice en la primera ocasión. El principal problema es que a lo mejor la tarea sea igualmente exigente en cualquier ocasión futura; si las auditorías de seguridad que verifican la conformidad con los estándares o los requisitos externos impuestos se convierten en eventos regulares, entonces, se requiere una cuidadosa reflexión sobre la manera en que el administrador de seguridad registra la escena local.

En los últimos años, han surgido estándares internacionales en seguridad de la información, como Bs 7799, ISO 27000, COBIT, ITIL, entre otros, los cuales son usados de acuerdo con las necesidades dentro de la organización.

> Según las iniciativas internacionales más importantes y más ampliamente aceptadas para el desarrollo y el funcionamiento de un sistema de gestión de seguridad de la información es ISO 27000, ITIL y COBIT, las más relevantes en aspectos como información, seguridad, gestión, así como la gobernanza de la nube y departamentos de gestión de riesgos, legales, auditoría, cumplimiento, privacidad, continuidad del negocio, control de calidad, instalaciones, recursos humanos y seguridad de TIC´s e información[2] (Stoll, 2014).

El código de prácticas de la British Standards Institution para la gestión de la seguridad de la información BS 7799 se anuncia como el primero en su clase en el año de 1995 dentro de los estándares de seguridad de la información. BS 7799 describió un conjunto de controles de seguridad recomendados como buenas prácticas corporativas. Se destacaron diez controles de administración clave en la norma, que constituyen los requisitos mínimos para cualquier organización (BS 7799, 1999). Éstas son:

1. Documento de política de seguridad de la información, indicando los objetivos de seguridad de la información.
2. Asignación de responsabilidades de seguridad de la información. Un método sugerido Posthumus y Von Solms, 2004 implica nombrar a la información "propietarios", "custodios" y "usuarios".
3. Programas de educación y capacitación en seguridad de la información para todo el personal.
4. Informe de incidentes de seguridad, asegurando formalmente que todos los empleados estén al tanto de los procedimientos.
5. Controles de virus implementados para detectar y prevenir virus.
6. La planificación de la continuidad comercial, la identificación de riesgos para las operaciones comerciales y el desarrollo de planes para garantizar que los procesos comerciales críticos continúen ejecutándose en caso de desastre.
7. Control de la copia del software propietario para garantizar que solo se use el software desarrollado por o con licencia de la empresa.

[2] Traducido del inglés.

8. La protección de los registros de la organización para protegerlos de la pérdida, destrucción y falsificación.
9. Protección de datos: regístrese en el registrador de protección de datos y asegúrese de que la información se use solo para fines comerciales genuinos.
10. El cumplimiento de la política de seguridad debe supervisarse periódicamente en toda la organización y todos los elementos de la gestión de la seguridad de la información se analizan periódicamente.

Estos diez controles han sido base para el resto de los estándares establecidos dentro del campo de la seguridad de la información.

Los Objetivos de Control para la Información y Tecnología Relacionada (COBIT) se ha implementado en muchos países desde su introducción en 1996. COBIT es un marco desarrollado por la asociación de auditoría y control de sistemas de información (ISACAF), una organización independiente de profesionales de gobierno de TIC's. El propósito del marco COBIT es proporcionar a la administración un modelo de gobierno de TIC que les ayude a controlar y administrar la información y la tecnología relacionada (IT *Governance Institute*, 2000). El marco explica cómo los procesos de TIC entregan la información que la empresa necesita para lograr sus objetivos. Esta entrega se controla a través de 34 objetivos de control de alto nivel, uno para cada proceso de tecnologías de información (TI).

> El marco identifica cuáles de los siete criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad), así como cuáles de los recursos de TIC (personas, aplicaciones, tecnología, instalaciones y datos) son importantes para los procesos de TIC para apoyar plenamente los objetivos de negocio[3] (Hussain y Sidiqqui, 2005).

La Organización Internacional de Normalización (ISO) 27000 proporciona un marco de seguridad de la información muy robusto para cualquier industria. Basado en el estándar 17799 de la *British Standards Institution*, a menudo se lo conoce como la versión de seguridad de la información del estándar de calidad ISO 9000. ISO 27000 se descompone

[3] Traducido del inglés.

aún más en varios estándares de acuerdo con el contenido. Por ejemplo, ISO 27000 proporciona una descripción de la norma, ISO 27001 describe como gestionar la seguridad de la información e ISO 27002 es un complemento de ISO 27001 de buenas prácticas.

Como se ha mencionado la Norma ISO 27001, está orientada a los requisitos para implementar un SGSI, tiene su origen en la norma BS 7799-2: 2002. La norma ISO 27001 es un documento que se divide en ocho partes:

- Objeto y campo de aplicación: En esta parte se explica el objetivo y campo de aplicación de la norma.
- Normas para consulta: Se hacen referencias a otras normas relacionadas.
- Términos y definiciones: Presenta una breve descripción de términos y definiciones para entender mejor la norma.
- Sistema de gestión de la seguridad de la información: Presenta una descripción acerca de los aspectos relevantes para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
- Responsabilidad de la dirección: se describe la importancia de la responsabilidad y la participación de la Dirección, la gestión de los recursos, la formación y capacitación.
- Auditorías internas del SGSI: se explica cómo llevar a cabo un auditor.
- Revisión del SGSI por la dirección: se describe el proceso para revisar los resultados del SGSI, por parte de la Dirección.
- Mejora del SGSI: aspectos de mejora continua, detección de áreas de oportunidad del SGSI.

El Sistema de Gestión de Seguridad de la Información (SGSI) es el concepto central sobre el que se construye ISO 27001, aunque este concepto no solo está presente en esta normativa. Se dice que un sistema de gestión de seguridad de la información es, como su nombre lo indica, un conjunto de políticas relacionadas con la gestión de la seguridad de la información (ISO 27001). El idioma surge principalmente de ISO 27001; el concepto clave de SGSI es que una organización diseñe, implemente y mantenga un conjunto coherente de procesos y sistemas para gestionar de manera efectiva la accesibilidad de la información, asegurando así

la confidencialidad, integridad y disponibilidad de los activos de información y minimizando los riesgos de seguridad de la información.

La biblioteca de infraestructura de tecnologías de la información (ITIL) representa la base de muchos estándares y es la metodología más utilizada para la implementación y administración de servicios de TI independientemente del tipo de organización (Taylor, Lloyd y Rudd, 2011). ITIL fue desarrollado por la Agencia Central de Telecomunicaciones por Computadora (ahora llamada Oficina de Comercio Gubernamental) en el Reino Unido en la década de 1980. ITIL se considera un marco de buenas prácticas de gestión de servicios de tecnologías de la información que cubre todas las actividades de las organizaciones de servicios de TI. ITIL V3 se introdujo en el 2007 y se revisó en el 2011; consta de 5 fases con 26 procesos de TI y 4 funciones de TI (Van, 2007). A continuación, se muestran las fases del ciclo de vida de ITIL:

- Estrategia de servicio
- Diseño de servicio
- Transición de servicio
- Operación de servicio
- Servicio de mejoramiento continuo.

Las herramientas de software ITIL están basadas en módulos; más comúnmente, un módulo por proceso. ITIL brinda información sobre cómo ofrecer los servicios de TI, cómo alinear la TI con la estrategia de las organizaciones y cómo diseñar un buen servicio de TI.

Es importante mencionar que Vermeulen y Von Solms (2002), indican que para la implementación efectiva de la seguridad de la información existen diferentes fases comenzando por el compromiso de la alta dirección, posteriormente los estándares de seguridad de la información pueden ser fundamentales para proporcionar a las organizaciones un enfoque de gestión de seguridad de la información, así como para proporcionar la base de un enfoque coherente para la seguridad de la información.

Gestión de la Seguridad de la Información

Primeramente, la gestión eficaz de la seguridad de la información requiere que los recursos de seguridad se implementen en múltiples frentes, incluida la prevención de ataques, la reducción de la vulnerabilidad y la disuasión de amenazas; además de alinear la seguridad de TI con la seguridad de la institución y garantizar que la seguridad de la información se administre de manera efectiva en todas las actividades de servicio y gestión de servicios. Entonces

> la gestión de la seguridad de la información es el proceso de administración de las personas, las políticas y programas con el objetivo de asegurar la continuidad de las operaciones mientras mantiene la alineación estratégica con la misión de la organización[4] (Cazemier, Overbeek, y Peters, 2000).

Fue en el año de 1995, cuando las normas de gestión de seguridad de la información fueron publicadas por primera vez por el *British Standard Institution* donde se estableció el estándar BS 7799-1, dentro del cual se habla de: Gestión de la seguridad de la información - Parte I: Código de práctica para la gestión SI, con este surgió un marco de gestión más completo para la SI. Dentro de este se define la gestión de SI como los mecanismos que protegen el almacenamiento de la información permitiendo la implementación de la seguridad de la información (*British Standards Institution*, 1995).

Pero los contenidos de gestión de seguridad de la información varían según los diferentes investigadores e instituciones. La gestión de seguridad de la información se ha definido desde diferentes perspectivas a nivel de organización: como un componente integrado en la empresa gobierno (Johnston y Hale, 2009; Póstumo y Von Solms, 2004; Tsohou, Karyda y Kokolakis 2015; Von Solms y Von Solms, 2006), como una forma de gestión de riesgos (Chang, Chen y Chen 2011; Dhillon y Backhouse, 2001; Webb, Maynard, Ahmad y Shanks, 2014), y como un ciclo de vida de la toma de decisiones de fases múltiples dinámicas (Ma, Schmidt y Pearson, 2009., Nazaret y Choi, 2015; Nyanchama, 2005; Pipkin, 2000). Tudor

[4] Traducido del inglés.

(2001), expresa que hay cinco componentes para cualquier arquitectura de gestión de seguridad de la información:

- Organización e infraestructura de seguridad.
- Política de seguridad, normas y procedimientos.
- Líneas de base de seguridad y evaluaciones de riesgo.
- Programas de concientización y capacitación en seguridad; y finalmente
- Cumplimiento.

Dichos componentes deben ser conocidos y aplicados por toda la institución, para que estos puedan lograr el objetivo planteado.

Uno de los principales participantes en la gestión de la seguridad son los gerentes de seguridad de la información teniendo una variedad de funciones, que incluyen planificación de seguridad, formación de políticas, administración del personal, gestión de riesgos, selección de tecnologías de seguridad, evaluación de amenazas, implementación de contramedidas, monitoreo de desempeño y mantenimiento. La selección de contramedidas a las amenazas de seguridad sigue siendo uno de los problemas inevitables que requieren atención continua. Los gerentes pueden optar por contrarrestar una amplia variedad de amenazas a la seguridad que están presentes con varias estrategias que incluyen detección, disuasión, reducción de la vulnerabilidad, educación y capacitación.

Luego, es importante considerar los aspectos organizacionales de la seguridad de la información, ya que la gestión de la seguridad de la información efectiva requiere que cierto personal se dedique a su implementación. Entonces, el último elemento de la etapa de preparación es formular una visión y estrategia de seguridad.

Políticas de Seguridad de la Información

Simultáneamente también se habla de políticas de seguridad para el manejo de la gestión de seguridad en las organizaciones; se define que una política de seguridad de la información es un documento de orientación para delimitar un comportamiento aceptable en los empleados cuando utilizan los activos de información de una organización (Höne y Eloff, 2002). Dicha

política proporciona a la administración de la seguridad de la información un vehículo importante para establecer prácticas de seguridad de la información en una organización (Von Solms y Von Solms, 2004). En consecuencia, una política de seguridad de la información es un componente importante en los dos procesos de dirigir y controlar una organización que se encuentran en muchos marcos de gestión de seguridad de la información (Von Solms, 2011).

Kabay (1996) señaló que el establecimiento de una política de seguridad de la información debería incluir cinco procedimientos, que son:

- Evaluar y persuadir a la alta dirección.
- Analizar los requisitos de seguridad de la información.
- Formar y redactar una política.
- Implementar la política; y
- Mantener esta política.

El ciclo de vida de la política de seguridad de la información propuesto por (Gupta, 2001) abordó cuatro partes:

- Evaluación de políticas.
- Evaluación de riesgos.
- Desarrollo de políticas y definición de requisitos.
- Revisión de tendencias y gestión de operaciones.

Durante este proceso de diseño, los gerentes de seguridad de la información se basan principalmente en los requisitos de seguridad de la información obtenidos y en los estándares de seguridad internacionales, para regular el comportamiento de seguridad de los empleados y prevenir el mal uso de los sistemas de información (Baker y Wallace, 2007).

Se han desarrollado sugerencias para marcos de procesos para sistematizar el trabajo con el diseño de políticas de seguridad de la información. Por ejemplo, Wood (1995) proporcionó pautas para el proceso de diseño de políticas de seguridad de la información, argumentando que las diferentes audiencias a menudo requieren políticas personalizadas: "uno debe comprender las necesidades especiales de una organización antes de intentar generar

directivas de gestión escritas específicas". Beautement (2016), comparte lo anteriormente definido por Wood (1995), al encontrar que las poblaciones de empleados en una organización no son homogéneas, lo que significa que una política puede traducirse en diferentes comportamientos de seguridad.

Una política de seguridad de la información debe basarse en los riesgos relevantes (es decir, debe ser relevante para los empleados), coincidir con el idioma de la audiencia, estar actualizada y tener una estructura clara. Höne y Eloff (2002) también incluyeron un conjunto de características generales, que se centran en el aspecto comunicativo del contenido: una política de seguridad de la información debe ser breve y fácil de leer, reflejar la cultura organizacional y tener una apariencia visual relevante para los empleados, estar al día y ser realista.

Stahl (2012), adoptó un enfoque lingüístico para evaluar la calidad comunicativa de las políticas de seguridad de la información. Ofrecieron seis recomendaciones basadas en un análisis crítico del discurso de 25 políticas de seguridad de la información de alto nivel en el sector sanitario del Reino Unido.

- Primero, las políticas de seguridad de la información se deben escribir utilizando un lenguaje y una terminología que sea accesible para los usuarios.
- En segundo lugar, argumentaron que una organización debería " proporcionar un conjunto separado de directrices orientadas a los empleados, si éstas ayudan a comunicar de manera efectiva el subconjunto de problemas que son aplicables a todos los empleados".
- Además, como tercera recomendación, declararon que las políticas deberían ser relevantes para los empleados y abordar "los problemas que son importantes para los usuarios".
- Sus recomendaciones cuarta y quinta son "el contenido sustantivo de las políticas a temas de importancia general para toda la fuerza laboral" y "sobre el contenido técnico para audiencias especializadas a los apéndices claramente referenciados o documentos de políticas separados".

- Finalmente, en la sexta recomendación, una política debe "dar consejos específicos y prácticos y pautas prácticas", que también es una forma de demostrar la relevancia de la política.

El desarrollo de una política de seguridad de la información implica más que la mera formulación y aplicación de políticas y a menos que las organizaciones reconozcan explícitamente los diversos pasos requeridos en el desarrollo de una política de seguridad, corren el riesgo de desarrollar una política mal pensada, incompleta, redundante e irrelevante, y que no será totalmente compatible con los usuarios (Fredrik Karlsson, Karin Hedström, Göran Goldkuhl, 2017).

En resumen, una política de seguridad de la información que sea de alta calidad comunicativa puede ser una herramienta práctica y útil para la gestión de la seguridad de la información y una herramienta para los empleados.

Factores Críticos de Éxito

El concepto de éxito organizacional cambia a través del tiempo, dependiendo de las exigencias del medio ambiente, y necesidades internas que se impongan para el logro de los objetivos de supervivencia, rentabilidad y crecimiento. Así, alcanzar el éxito exige a la organización prestar atención de manera armónica y simultánea a múltiples peticiones formuladas por un entorno cada vez más complejo, cambiante y orientado a la información y por una organización cada vez más dinámica donde se pongan a funcionar nuevos conceptos y relaciones a fin de poder dar respuesta a tal complejidad externa.

La única manera de mantener el equilibrio armónico que tal reto exige es identificando aquellos eventos, condiciones, variables, áreas, circunstancias o actividades coyunturales en las cuales los resultados satisfactorios aseguren un desempeño exitoso para la organización. Este es el aporte que la metodología de gestión por factores críticos de éxito hace a la gerencia moderna (Villegas,1995).

El método de gestión por factores críticos de éxito apareció sugerido en la literatura administrativa en los inicios de 1960 por Ronald (1960) y a pesar de su importancia para la gestión competitiva, permaneció relativamente inexplorado hasta marzo de 1979 cuando el

equipo para investigación en sistemas de información del Massachussets *Institute of Technology* lo retomó como herramienta aplicable a la definición de requerimientos de información de un sistema de información gerencial (Rockart, 1979).

A partir de allí la literatura administrativa retoma el concepto de factores críticos de éxito precisándolo y aplicándolo no sólo a la definición de requerimientos de información sino también:

- A la valoración de empresas.
- Al proceso de Benchmarking.
- A la formulación de estrategias de Desarrollo Corporativo.
- Al apoyo del análisis ambiental.
- A la formulación de la estrategia del negocio en las fases de análisis de recursos y de elección de la estrategia.
- Como soporte al sistema de retroalimentación durante la ejecución de la estrategia.
- Como base para la comunicación de las prioridades gerenciales.
- Como herramienta para la evaluación de desempeño individual en el sistema de incentivos y recompensas.
- Para el diseño de sistemas de control.
- Al proceso de reingeniería y a la reflexión prospectiva.

Distintos autores hacen énfasis en distintos niveles del sistema económico razón por la cual las definiciones varían en grado de generalidad y externalidad a la organización, lo que no necesariamente las hace contradictorias entre sí sino complementarias. Las siguientes definiciones de factores críticos han sido ordenadas de lo general y externo (ambiente macroeconómico y competitivo) a lo particular e interno (actividades críticas que deben desarrollar los individuos clave para que se alcance el éxito de la organización):

> Los factores críticos de éxito son factores internos o externos a la empresa que deben ser identificados y reconocidos porque soportan o amenazan el logro de los objetivos de la empresa e incluso su existencia. Requieren de atención especial para evitar

> sorpresas desagradables o la pérdida de oportunidades. Pueden ser internos o externos, positivos o negativos en su impacto[5] (Ferguson, 1982).

Características, condiciones o variables que cuando están debidamente soportadas, conservadas o gerenciadas tienen un impacto significativo en el éxito de una empresa que compite en una industria específica. Afectan directamente a la rentabilidad, cambian y no siempre son predecibles (Leidecker, 1984).

> Los factores críticos de éxito son variables que la gerencia puede influenciar a través de sus decisiones y que pueden afectar significativamente la posición competitiva global de las firmas en una industria. Estos factores usualmente cambian de industria a industria y dentro de una industria específica se derivan de la interacción de las características económicas y tecnológicas del sector en cuestión y de las armas con las cuales los competidores al interior han construido su propia estrategia[6] (Hofel, 1978).

Condiciones internas o externas claves para que la estrategia de la empresa sea exitosa. Por ejemplo: aceptación de usuarios, movimientos de los competidores, recursos humanos o financieros (Eccles, 1993).

> Factores importantes al éxito estratégico. Dichos factores deben ser supervisados para asegurar la ejecución exitosa del programa estratégico de la empresa. También se usan para guiar y motivar a los empleados clave a actuar de manera que hagan una contribución óptima a la estrategia. Deben reflejar el éxito de la estrategia elegida, representar los elementos básicos de dicha estrategia, motivar y alinear a los gerentes y ser muy específicos y cuantificables (Jenster, 1987).

Eventos, condiciones, circunstancias o actividades en las cuales resultados satisfactorios asegurarán un desempeño competitivo para la organización (Eccles, 1993).

[5] Traducido del inglés.
[6] Traducido del inglés.

Los factores críticos de éxito se definen como el número limitado de áreas en las que los resultados, si son satisfactorios, garantizarán un desempeño competitivo exitoso para el individuo, departamento u organización (Rockart,1979).

Conjunto de acciones cuyo resultado es una combinación de entradas o recursos tan eficiente que incrementa la rentabilidad de la empresa. Importa pues encontrar las actividades que son responsables de la rentabilidad (Ronal, 1961).

Elementos cruciales para el éxito de una empresa durante el horizonte de la planeación. Por esta razón son temporales y específicos a cada gerente. Buena parte de los factores críticos de éxito tienen una duración de un año al cabo del cual, deben revisarse (Eccles, 1993).

Cuando los factores críticos de éxito se desdoblan a nivel operativo, se denominan factores operativos de éxito y se han definido como:

Variables que son percibidas por los gerentes como necesarias para ejecutar exitosamente un trabajo específico en una empresa específica. Así pues, cambian de empresa a empresa y de gerente a gerente. Pueden ser áreas cuyo desempeño es coyunturalmente crítico debido a que sus resultados están por debajo del nivel esperado (Robert, Dearden y Richard, 1972).

Objetivos intermedios cuya ejecución conduce a la implementación exitosa de la estrategia y con ello al logro de sus beneficios (Reed, 1988).

Áreas en las cuales un buen desempeño conlleva el cumplimiento de los objetivos (Rockart, 1982).

Todos estos enfoques son ampliamente utilizados para identificar los requisitos de rendimiento de una empresa (Rockart, 1982). Han sido una de las herramientas de gestión (Lee y Ahn, 2008) que se han utilizado como medidas en diferentes áreas tales como la industria manufacturera (Mohr y Spekman, 1994; Psomas, 2016), la gestión de proyectos (Ahimbisibwe, Daellenbach, Cavana, 2017; Davies, 2002), la gestión de la calidad (Singh y Gupta, 2014), y la implementación del sistema de inteligencia empresarial (Yeoh y Popovič, 2016).

Factores Críticos de Éxito de la Gestión de Seguridad de la Información

La identificación de los factores críticos de éxito adecuados para la gestión de seguridad de la información requiere una visión integral de la organización (Smith y Jamieson, 2006), mediante la combinación de los resultados, la revisión y la perspectiva de la alineación de valor, se agrupan estas cuestiones en cuatro factores clave: la alineación del negocio, apoyo de la dirección, conciencia organizacional y los controles de seguridad (Tu, Yuan, Archer, y Connelly, 2018). De acuerdo con la experiencia, BS7799 considera ocho factores como críticos para la implementación exitosa de seguridad de la información dentro de una organización (BS7799, 1999).

Literatura anterior ha indicado la importancia de la evaluación del desempeño de gestión de la seguridad de la información (Erkan, 2005; Herath, Herath y Bremser, 2010; Huang, Lee y Kao, 2006; Martin, Bulkan y Klempt, 2011; Nazaret y Choi, 2015). Y la medición del desempeño debe reflejar los valores comunes compartidos por los gestores, actores, empleados y consumidores. El cuadro de mando integral (BSC) (Kaplan y Norton, 1992; Kaplan y Norton, 1993) es un sistema común de medición de rendimiento de la organización, que se utiliza ampliamente en la práctica y ha sido ampliamente investigado (Marr y Schiuma, 2003).

El modelo genérico BSC se ha aplicado en el dominio de los sistemas de información para medir el desempeño de la administración de TI (Bremser y Chung, 2005; Huang *et al*., 2006; Kaplan y Norton, 2004). Huang *et al*. (2006) desarrollaron un modelo general de BSC para la gestión de seguridad de la información, traduciendo el mapa de estrategia de gestión de seguridad de la información en una modelo de cuadro de mando con cuatro perspectivas: financiera, clientes, procesos internos y aprendizaje y crecimiento. En su estudio, los 80 indicadores de rendimiento obtenidos de los estudios anteriores se transfirieron a 35 clave indicadores de rendimiento, 12 temas estratégicos y un modelo genérico y mapa de estrategia de gestión de seguridad de la información (Figura 1).

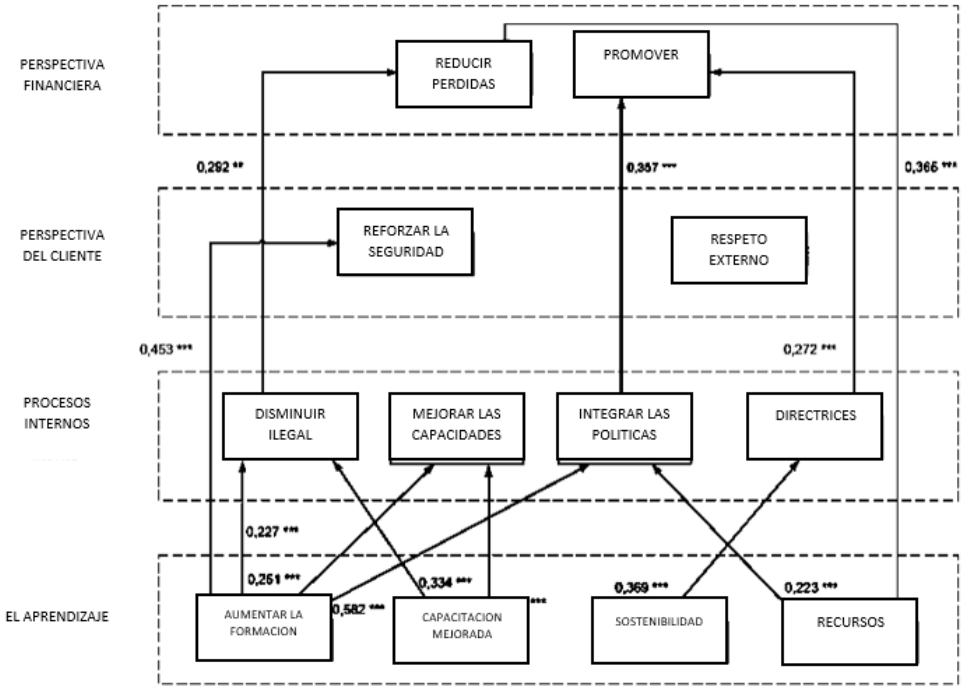


Figura 1. Mapa de estrategias para la gestión de seguridad de la información. Fuente: Huang et al. (2006).

Herath *et al*. (2010) también estableció un marco conceptual para la implementación estratégica de seguridad de la información, la gestión y del rendimiento mediante un cuadro de mando integral, con cuatro perspectivas interrelacionadas: el valor del negocio, la orientación de las partes interesadas, proceso interno, y la disposición futura (Figura 2).

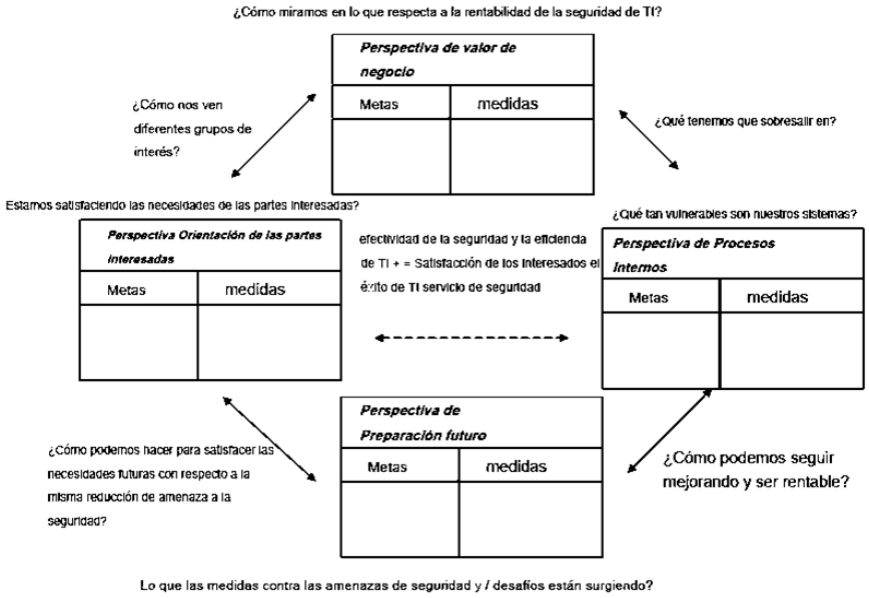


Figura 2. Modelo BSC propuesto para la Seguridad de la Información. Fuente: Herath et al. (2010).

Sin embargo, enfoques que usan el modelo BSC para la gestión de seguridad de la información necesitan mayor investigación empírica y validación.

Modelo de Éxito de Gestion de Seguridad de la Información

Tu, Yuan, Archer, y Connelly (2018), desarrollaron un modelo de investigación de cómo los Factores críticos de éxito contribuyen a la Gestion de seguridad de la información de la organización desde una perspectiva de alineación y valor estratégico. Este Modelo de éxito de Gestion de seguridad de la información[7] tiene cinco construcciones: la alineación del negocio, apoyo de la dirección, conciencia organizacional, los controles de seguridad y rendimiento de Gestion de seguridad de la información, que se mide a partir de cuatro dimensiones: valor de negocio, proceso interno, orientación del usuario y disposición a futuro (Figura 1). Y son definidas como:

Alineación del negocio

[7] Traducido del inglés *ISM success model*

Se refiere a la adecuación entre estrategia de gestión de seguridad de la información y estrategia de negocio en términos de abordar las necesidades, demandas, las metas, los objetivos y / o estructuras de Gestion de seguridad de la información. Debe asegurar los activos de información al tiempo que se permite el negocio. Lo estudios han señalado que la protección de los activos de información de las amenazas potenciales debe ser una parte de estrategia de negocios, ya que puede dar a la organización una ventaja competitiva (Soomro *et al.,* 2016). La alineación de los esfuerzos de colaboración entre la seguridad de la información y de negocios y los gerentes que pueden alinear las prácticas de gestión de seguridad de la información con las estrategias de negocio de la organización (Chang *et al.*, 2011). Esta alineación se puede lograr a través del entendimiento de planificadores de objetivos seguridad de la información de la organización, la comprensión mutua entre la alta dirección y los planificadores de seguridad de la información, y una vista aumentada de la función de seguridad de la información dentro de la organización (Ma *et al.,* 2009).

Apoyo de la alta dirección

Se refiere al compromiso de la alta dirección a través de la alineación, las iniciativas de seguridad de la información se abordan a nivel estratégico y por lo tanto son más propensos a ser reconocido y apoyado por la alta dirección (Johnston y Hale, 2009). La alta dirección pueda apreciar plenamente la importancia de los procesos de gestión de seguridad de la información en el marco de negocios (Smith y Jamieson, 2006; Werlinger *et al.*, 2009). A falta de ajuste entre los objetivos de seguridad y objetivos de negocio pueden conducir a situaciones en las políticas de seguridad de la información y presupuestos que no reflejan las necesidades de la empresa (Kayworth y Whitten, 2010; Siponen y Oinas- Kukkonen, 2007).

Conciencia organizacional

Se refiere al conocimiento de la organización sobre los riesgos de seguridad de la información, las políticas, y procedimientos relacionados (Lebek *et al*., 2014). Todos los empleados deben ser conscientes de las posibles amenazas a la seguridad, y tienen suficiente alfabetización de TI para proporcionar un nivel básico de los conceptos de seguridad y el vocabulario clave (Culnan *et al*., 2008). Todos los grupos relevantes en la organización deben

contar con la suficiente formación y materiales de referencia que les permita proteger los activos de información de manera efectiva (Straub y Welke, 1998).

La conciencia de la seguridad de la información necesita ser reconocido no sólo por parte del personal, sino también por la alta administración. De hecho, la seguridad debe ser comercializado de manera efectiva a todos los directivos y empleados (Von Solms, 1999). Políticas y procedimientos de seguridad que se integran con los objetivos de negocio ayudan a centrarse más atención en los riesgos de seguridad de la información, las políticas y procedimientos relacionados con los procesos de negocio (Spears y Barki, 2010).

Controles de seguridad

Se refieren a los controles técnicos y de procedimiento para la seguridad de la información, incluyendo el riesgo de la gestión, las políticas de seguridad, y la aplicación estándar de seguridad. Las organizaciones los necesitan para establecer la seguridad y control y practicarlos con el fin de proteger la seguridad de la información. Los estudios han afirmado que de una organización la implementación de los controles de seguridad de la información se ve afectada por la alineación estratégica (Doherty y Fulford, 2006; Hagen *et al*., 2008; Knapp *et al.*, 2009; Warkentin y Willison, 2009). Los controles de seguridad de la información deben reflejar y apoyar los objetivos de negocio generales de la organización y objetivos.

El rendimiento de la Gestion de seguridad de la información

Se refiere al progreso de la gestión de seguridad de la información hacia lograr metas, que se mide partir de perspectivas de la organización, incluyendo los valores empresariales, procesos internos, la orientación del usuario y preparación hacia el futuro.

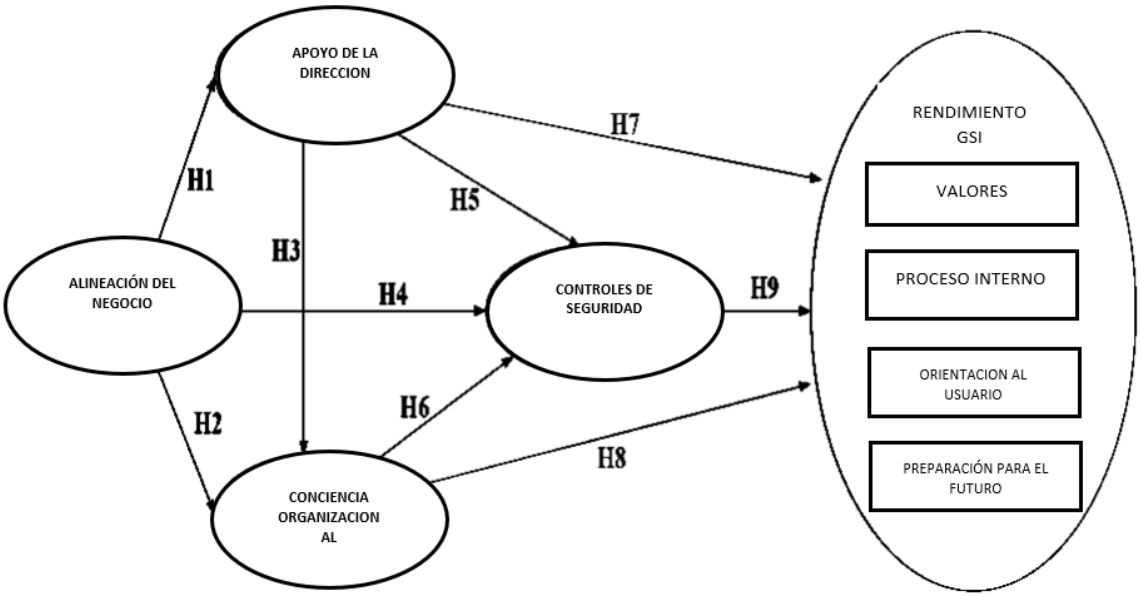


Figura 3. Modelo de éxito ISM. Fuente: Tu et al., 2018.

Este estudio se llevó a cabo en el norte del América, los participantes fueron los directores de TI, jefes de los Servicios de Seguridad, los administradores de TI, los administradores de seguridad de la información y el personal de TI de alto nivel. Las características demográficas de los participantes se resumen en la Tabla 2.

Tabla 2. *Características de los participantes*.

Característica	Grupo
Puesto de trabajo	Director de Información (CIO)
	Director de Seguridad (CSO)
	Gerente de TI
	Gerente de seguridad de la información
	El personal de TI de alto nivel
	Otro
Industria	Fabricación
	Al por menor y distribución
	Servicios financieros
	Tecnología
	Salud

	Telecomunicación
	Viajes, ocio y entretenimiento
	Educación
	Servicios públicos, energía y minería
	Gobierno
	Otro
Tipo de organización	Nacional
	Internacional
Tamaño de la organización	1-50
	51-200
	201-500
	Por encima de 500
Estándar de seguridad aplicada	Si 32%
	No 68%

Fuente: Adaptado de Tu *et al*., 2018.

Este modelo señala la importancia de la alineación estratégica siendo que esta se define como:

> La alineación estratégica de TI se refiere a la adecuación entre la estrategia de sistemas de información y la estrategia de negocios en términos de hacer frente a las necesidades, demandas, las metas, los objetivos y / o estructuras de cada estrategia y gestión[8] (Gerow, Grover, Thatcher y Roth 2014).

Entonces, empresas alineadas son más propensas a invertir en TI y asignar recursos para proyectos vinculados a los objetivos generales de la empresa y así aprovechar para crear una ventaja competitiva (Cumps, Martens, Backer, Haesen, Viaene, Dedene, Baesens y Snoeck, 2009; Rivard *et al*., 2006). Un metaanálisis confirmó las relaciones positivas entre las dimensiones de alineación y los resultados de rendimiento (Gerow e*t al*., 2014). Siguiendo la misma lógica en el contexto de gestión de seguridad de la información cuando la estrategia de seguridad de información de una organización está mejor alineado con la estrategia

[8] Traducido del inglés.

comercial de la empresa, entonces se le dará más soporte organizativo a la Gestion de seguridad de la información y se mejorará el nivel operativo, la conciencia organizacional de la seguridad de la información y los controles de seguridad puede ser mejor aprovechados y finalmente la Gestion de seguridad de la información de la organización será más exitoso.

Esta alineación se puede lograr a través del entendimiento de planificadores de seguridad de la información, la organización y los objetivos, la comprensión mutua entre la alta dirección y los planificadores y una vista aumentada de la función de seguridad de la información dentro de la organización (Ma, Schmidt y Pearson, 2009)

Y tenderá a promover a la alta dirección a apoyar y reforzar la conciencia de los riesgos de seguridad de la organización, mejorando así la implementación de controles de seguridad. Esto dará como resultado la consecución de éxito medido desde la gestión de seguridad de la información con perspectivas equilibradas e interrelacionadas, incluyendo el valor de negocio, la orientación de las partes interesadas, procesos internos y disposición a futuro.

Investigaciones en Seguridad de la Información

Las contribuciones en investigación con respecto a la seguridad de la información y su relación con las comunicaciones seguras, la gestión de la seguridad y el desarrollo de seguridad de la información, están relacionadas con los niveles técnicos, conceptuales y de organización. Las contribuciones de la comunicación segura se refieren principalmente al contexto técnico con un bajo nivel conceptual, aunque también hay soluciones que cubren tanto el nivel técnico y de organización dentro de la comunicación segura. Las contribuciones relacionadas con la gestión de la seguridad se refieren a los niveles organizativos y técnicos. Mientras que las contribuciones relativas al desarrollo de seguridad cubren los tres niveles: técnicos, conceptuales y de organización. A continuación, se presentan dentro de un orden cronológico (tabla 3) algunos de los estudios que se han desarrollado dentro del campo de seguridad de la información y sus aportaciones dentro de esta rama de estudio.

Tabla 3. *Estudios en seguridad de la información.*

Autor(res)	Nivel	Descripción
Boockholdt, 1989	Técnico Organizacional	Identifican los problemas de gestión en la implementación de seguridad.
Straub, 1990	Técnico	Eficacia de las medidas de seguridad.
Straub y Nance, 1990	Conceptual	El descubrimiento de seguridad de la información y la disciplina.
Loch *et al.* 1992	Técnico	Las amenazas únicas que existen en un entorno de red.
Baskerville 1993	Técnico	Métodos de seguridad en el desarrollo de sistemas.

Banerjee *et al.*, 1998, Harrington 1996	Organizacional	Actitudes de los empleados hacia la ética informática.
Straub y Welke 1998; Gattiker y Kelley, 1999; Dhillon y Backhouse, 2001	Técnico Organizacional	Características de los trabajadores involucrados en el abuso de seguridad de la información, los modelos de planificación de seguridad que proporcionan una síntesis de esta línea de investigación.
Knapp, Marshall, Rainer y Ford, 2006	Técnico Organizacional	Desarrollo de un instrumento no invasivo en seguridad de la información para animar a los encuestados a participar a fondo y abiertamente.
Dhillon y Torkzadeh, 2006	Técnico Organizacional	Identificar los valores generales de la gestión en seguridad.
Albrechtsen, 2007	Organizacional	Concienciación sobre la seguridad y el comportamiento prudente.
Baker y Wallace, 2007	Técnico Organizacional	Estudio enfocado en la calidad de seguridad de la información, para descubrir detalles de la implementación del control y centrarse en la calidad de la ejecución.
Rainer y Marshall (2007)	Técnico Organizacional	Estudio con el propósito de examinar las diferencias, si las hay, entre los profesionales de seguridad de la información y administradores de empresas en la importancia relativa de una serie de problemas de seguridad de la información.
Albrechtsen y Hovden, 2009	Técnico Organizacional	En este artículo se discutió la brecha digital en la seguridad de la información en cuanto a las diferencias existentes en las vistas de seguridad de la información y las expectativas entre los profesionales de seguridad de la información y de los usuarios.
Herath, 2009	Técnico Organizacional	La motivación intrínseca en el comportamiento de los trabajadores relacionados con el

		cumplimiento de las políticas de seguridad de la información.
Hedström, Karlsson y Allen (2011),	Técnico Organizacional	Estudio que tiene como propósito desarrollar un modelo nuevo para las prácticas de seguridad de la información en una organización, demuestran la capacidad de un modelo para identificar áreas de valor entorno a la seguridad de la información y la práctica asistencial.
Chander, Jain y Shankar (2012)	Técnico Organizacional	Estudio donde generado con los siguientes parámetros: compromiso de la dirección, identificación y clasificación de los activos de información, herramientas tecnológicas, estructura y los recursos de la organización, políticas y procedimientos, la sensibilización, la educación y formación, la motivación, la recompensa y el castigo y las auditorías de seguridad.
Tu, Yuan, Archer, y Connelly (2018)	Técnico Organizacional	Estudio basado en la complejidad de los problemas de gestión de la seguridad, los conflictos entre valores y las directrices profesionales y para hacer frente a esta brecha de investigación, este estudio se centró en la Gestion de seguridad de la información en el nivel organizacional, donde se estudian los factores organizativos que determinar el éxito de la Gestion de seguridad de la información.

Fuente: Autoría propia.

Los principales trabajos sobre seguridad de la información se enfocan en el área que identifican los problemas de gestión en la implementación de seguridad (Boockholdt, 1989), la eficacia de las medidas de seguridad (Straub, 1990), el descubrimiento y la disciplina (Straub y Nance 1990), las amenazas únicas que existen en un entorno de red (Loch *et al.* 1992), y métodos de seguridad en el desarrollo de sistemas (Baskerville 1993), sin embargo tambien existen investigaciones que se han centrado en las actitudes de los empleados hacia la ética informática (Banerjee *et al.*, 1998, Harrington 1996), las características de los trabajadores involucrados en el abuso de seguridad de la información y los modelos de

planificación de seguridad (Straub y Welke 1998; Gattiker y Kelley, 1999; Dhillon y Backhouse 2001)

El estudio de Knapp, Marshall, Rainer y Ford (2006), describen seis pasos principales que combinan técnicas cualitativas y cuantitativas. La parte cualitativa de la metodología se basó en la estrategia de investigación de la teoría fundamentada con el fin de analizar las respuestas a preguntas abiertas de 220 profesionales de la seguridad de la información. El objetivo de la investigación era crear un instrumento con una alta validez y fiabilidad y también reducir la percepción del encuestado de intrusión en el are de seguridad de la información. Anuncian que los instrumentos con preguntas redactadas intrusivas que cubren temas de organización sensibles pueden causar a los encuestados que sean menos directos en sus respuestas, por esta razón, el desarrollo de un instrumento no invasivo es importante para animar a los encuestados a participar a fondo y abiertamente en la investigación. En este caso, una de las principales funciones del panel de expertos fue la identificación de los ítems del cuestionario potencialmente intrusivos, después de varias rondas de evaluación de expertos y una prueba previa por nueve expertos y nueve académicos, se recogieron datos cuantitativos a través de una versión de encuesta web del instrumento desarrollado y los resultados se analizaron mediante modelos de ecuaciones estructurales.

Los autores concluyen que un factor limitante del modelo a tres constructos era el tamaño pequeño de la muestra de estudio y que los estudios de seguimiento también deberían mejorar en el rigor metodológico, reduciendo al mínimo común la varianza del método a través, por ejemplo, la introducción de los desfases entre la recolección de datos de las variables independientes y dependientes.

Presentan que la investigación futura también puede basarse en el modelo mediante la introducción de otros constructos de gestión. Por ejemplo, durante la parte de la metodología, o la fase de codificación produce una lista de 25 categorías desarrolladas a lo largo del tema. Los investigadores pueden considerar la adición de algunas de estas construcciones, como la conciencia de la formación, en un modelo ampliado que existen en las implicaciones para la profesión de seguridad.

El artículo, proporciona evidencia de que existe una relación significativa entre las importantes cuestiones de gestión de seguridad de la información y que los profesionales de la seguridad comprendan el impacto del apoyo de la dirección en el logro de la eficacia de la seguridad.

Con base en los hallazgos de este estudio, los autores precisan que los niveles bajos de apoyo ejecutivo producirán una cultura organizacional menos tolerantes a las buenas prácticas de seguridad. Los bajos niveles de apoyo también disminuirán el nivel de cumplimiento de las políticas de seguridad existentes. Como un experto en seguridad declaró: “La aplicación es sin duda el problema más crítico que la política de seguridad de la información”. Concluyendo, que mientras que una organización puede incluir lo que quiera en su política de seguridad, este contenido es prácticamente inútil a menos que se cumpla.

Dhillon y Torkzadeh (2006), en su estudio entrevistaron a 103 directivos de un amplio espectro de organizaciones para identificar los valores generales de la gestión en seguridad. Todos los encuestados tenían al menos 5 años de experiencia laboral relevante, todos los encuestados se basaron en la región suroeste de los Estados Unidos. La gama de industrias representada por los encuestados incluye la banca, farmacéutica, médica, hotel y entretenimiento. Los encuestados no eran necesariamente personas de los departamentos de TI, pero tenían experiencia significativa el uso de las TI en sus puestos de trabajo del día a día. Los hallazgos presentados en este documento son específicos a un determinado grupo basado en una región específica, los autores especifican que en la muestra hay una dimensión cultural a los valores individuales y de grupo.

Los resultados de este estudio, indica que una clase de medidas de seguridad está relacionada con una lista de verificación y que las listas de control siempre han sido un medio popular para garantizar la seguridad. La intención detrás de las listas de comprobación ha sido identificar todas las vulnerabilidades concebibles en un producto informático y proponer contramedidas. La investigación sugiere que los 103 gerentes entrevistados para este estudio no tuvieron en cuenta las listas de comprobación para ser el resumen de la seguridad, una mayoría de los encuestados consideró que el exceso de confianza en las medidas de seguridad predeterminados en realidad es perjudicial. Esto se ilustra por un entrevistado, que dijo:

“Cualquier tipo de medida de seguridad visible es en efecto neto de una vulnerabilidad”. Además, se indica que cuando la seguridad se convierte en un obstáculo para hacer el trabajo los empleados comienzan a tomar atajos para conseguirlo alrededor de o dejan de usar la seguridad de la información.

También, es interesante observar que la confidencialidad, integridad y disponibilidad de los datos son sólo una parte de la seguridad de la información como objetivos de seguridad identificados en esta investigación, ya que en el pasado las actividades de desarrollo de sistemas más seguros y las políticas de seguridad de la organización se han basado exclusivamente en los principios de confidencialidad, integridad y disponibilidad. Los autores mencionan que parte del problema está relacionado con nuestra incapacidad para gestionar y garantizar la seguridad y nuestra excesiva dependencia de estas tres cuestiones e ignorando al mismo tiempo las medidas de valor basadas organizativamente. La mayoría de los enfoques de gestión de riesgos dan por sentado que la confidencialidad, integridad y disponibilidad son los pilares de la seguridad y por lo tanto desarrollan metodologías completas alrededor sólo de estos conceptos.

Dhillon y Torkzadeh (2006), mencionan una cuarta categoría de investigación sobre seguridad, llamada los “enfoques suaves”. Esta corriente de investigación identifica las limitaciones de las listas de comprobación, análisis de riesgos y modelos formales que hacen de esta manera un llamado a una mayor gama de consideraciones socio-organizacional, tales como las prácticas éticas, la sensibilidad cultural, la responsabilidad y la conciencia entre otros.

Los hallazgos de esta investigación ponen una base para el desarrollo multidimensional en medidas de seguridad. Son revelados 86 objetivos, agrupados en 9 fundamentales y 16 objetivos significativos, esenciales para el mantenimiento de la seguridad de una organización. Los objetivos desarrollados en este estudio son socio-organizativos y sugieren una forma de avanzar en el desarrollo de medidas de seguridad.

Albrechtsen (2007), menciona que los usuarios juegan un papel importante en el rendimiento de seguridad de la información de las organizaciones mediante la concienciación sobre la seguridad y el comportamiento prudente. Presenta un estudio con entrevistas a los usuarios

en una empresa de tecnología y un banco que se analizaron cualitativamente con el fin de explorar la experiencia de los usuarios de la seguridad de la información y su papel personal en el trabajo de seguridad de la información. Los principales patrones del estudio fueron:

1. el usuario declara estar motivado para el trabajo seguridad de la información, pero no llevan a cabo muchas acciones de seguridad individual;
2. la carga de trabajo de alta seguridad de la información crea un conflicto de intereses entre la funcionalidad y la seguridad de la información; y
3. los requisitos documentados de comportamiento esperado seguridad de la información y las campañas de sensibilización general tienen poco efecto solo en el comportamiento del usuario y la conciencia.

Este estudio se concentra en usuarios que no tienen la responsabilidad de gestión y de bajo grado de concienciación sobre la seguridad de la información y el conocimiento sobre los sistemas de información. Se tiene como objetivo proporcionar el conocimiento de la experiencia de los usuarios en seguridad de la información y su papel de seguridad individual en el trabajo diario.

Hubo pruebas de un alto y un bajo grado de concienciación sobre la seguridad de la información, es decir, el grado en que los miembros de la organización comprenden la importancia de la seguridad de la información, el nivel de seguridad requerido por la organización y sus responsabilidades de seguridad individuales. En total había indicios más negativos que indicios que apuntan a un alto grado de conciencia de seguridad de la información. En el lado positivo, los informantes en las dos compañías informaron que la seguridad de la información era tan importante para ellos y para la empresa. También dijeron que estaban motivados para contribuir a la seguridad de la información de trabajo.

Por otro lado, no había indicios de que la conciencia de seguridad de la información era inadecuada: cada individuo lleva a cabo muy pocas acciones de seguridad de la información; los informantes no estaban familiarizados con las posibles amenazas; los usuarios entrevistados no estaban al tanto de las posibles consecuencias de las violaciones de seguridad; los informantes no vieron muchos problemas o potenciales de mejora en sus

propias condiciones de trabajo; y algunos de los informantes no podían ver el valor de su función de seguridad de la información en el trabajo de seguridad integral de la empresa.

Se asignan tres patrones principales de resultados: los usuarios que no realizan muchas acciones de seguridad de la información, usuarios que priorizan otras tareas de trabajo sobre la seguridad de la información y los usuarios que experimentan que las herramientas actuales como ineficaces para ese propósito. Las entrevistas indican que un problema principal con respecto al papel de los usuarios en el trabajo seguridad de la información es su falta de motivación y conocimientos sobre la seguridad de la información y el trabajo relacionado. Los autores mencionan que, si la percepción de riesgo es una cuestión de organización social, entonces la gestión del riesgo es un reto organizativo (Douglas y Wildavsky, 1982).

Los resultados son interpretaciones de las experiencias de seguridad de la información de algunos usuarios en su trabajo diario. Por lo tanto, se debe considerar si los hallazgos son transferibles a ciertas organizaciones, comparándolos con el contexto del estudio. Independiente de la transferibilidad, los hallazgos empíricos del estudio abren discusiones interesantes sobre gestión de seguridad de la información. Los principales patrones de resultados en el estudio son: Los usuarios son conscientes de que su papel en el trabajo total seguridad de la información es importante. Por otro lado, existe una brecha entre esta intención y el comportamiento real de los usuarios.

En medio de numerosas vulnerabilidades, amenazas complejas, una mayor regulación y reducción de los presupuestos, el reto es claro: cuando las organizaciones pueden identificar los controles apropiados para sus situaciones y las implementan eficientemente, pueden gestionar de forma eficaz los riesgos de seguridad de la información (Baker y Wallace 2007). Por lo cual Baker y Wallace (2007), llevaron a cabo un estudio enfocado en la calidad de seguridad de la información, realizaron una encuesta como un primer paso hacia el logro de este reto. Las encuestas de seguridad tienen como objetivo descubrir específicos detalles de la implementación del control y centrarse en la calidad de la ejecución. Con un conocimiento más preciso de las prácticas actuales, la gestión de seguridad de la información puede comenzar a seguir adecuadamente las estrategias eficaces para mejorar la calidad y reducir

los riesgos, estas representan una sección transversal de los controles que se encuentran en varias normas internacionales, entre ellas British Standard 7799 y el NIST.

Este estudio proporciona una descripción más precisa del estado actual de la gestión de seguridad de la información que estudios previos, no se puede decir si los niveles de calidad poco impresionantes son el resultado de los esfuerzos de las organizaciones predeterminadas para poner en práctica de manera óptima cada control. Las investigaciones futuras deben basarse en ese enfoque y desarrollar mejores indicadores de la fuerza de control y el costo eficiencia para optimizar el rendimiento de la inversión. Los investigadores concluyen que deben investigar más a fondo los beneficios de la combinación de varios niveles de técnica, de gestión y controles operacionales para lograr una verdadera seguridad integral contra una amplia gama de riesgos presentes y futuros. Aunque sus hallazgos revelan algunas tendencias positivas, las organizaciones necesitarán un mayor progreso antes de que realmente tengan la seguridad de la información "bajo control".

Rainer y Marshall (2007), realizaron un estudio con el propósito de examinar las diferencias, si las hay, entre los profesionales de seguridad de la información y administradores de empresas en la importancia relativa de una serie de problemas de seguridad de la información.

El estudio utilizó una encuesta en línea respondida por una muestra de 23 gerentes de empresas y 46 profesionales de la seguridad de la información. Los gerentes de negocios representaron una variedad de áreas funcionales en sus respectivas organizaciones: tecnología de la información (seis), contabilidad / finanzas (seis), marketing (cinco), operaciones (cuatro), y la gestión general (dos).

En primer lugar, se examinaron los diez puntos más importantes de acuerdo con los profesionales de la seguridad de la información, y los diez elementos más importantes de acuerdo con los gerentes de negocios. La implicación importante de los hallazgos es que, para una óptima organización de seguridad de información, gerentes de empresas y profesionales de la seguridad de la información deben moverse uno hacia el otro en la línea continua. Es decir, los gerentes de negocios deben tener un conocimiento básico de los aspectos más técnicos de los profesionales de seguridad de la información y los expertos en seguridad de la información debe tener una mejor comprensión de los aspectos de gestión de

seguridad de la información. Por lo tanto, para los profesionales de seguridad de la información que se mueven hacia el centro del continuo, tienen que aprender más acerca de las funciones de negocio, tales como contabilidad, finanzas, marketing, operaciones, recursos humanos, comportamiento organizacional y gestión de proyectos. Al aprender más acerca de la administración de empresas, los profesionales de seguridad de la información estarán en mejores condiciones de comprender todos los aspectos de seguridad de la información en un contexto organizativo. Ellos serán capaces de discutir las necesidades de seguridad de la información (por ejemplo, las solicitudes de presupuesto) en términos de retorno de la inversión, la productividad de los empleados compensaciones, y las métricas para medir el éxito de los esfuerzos de seguridad de la información. Además, el conocimiento de la administración de empresas puede proporcionar a los profesionales de seguridad de información con varios beneficios:

1. una mejor posición competitiva para la promoción en sus organizaciones,
2. una mejor posición competitiva para los trabajos de gestión en otras áreas funcionales de la organización,
3. posiciones en empresas de consultoría, o
4. convertirse en empresario y creación de una empresa.

Los autores concluyen que, en un mundo ideal, los gerentes de empresas querrían saber más acerca de los diversos aspectos técnicos de seguridad de la información, en lugar de depender totalmente de los profesionales de la seguridad de la información. Sin embargo, dada la carga de trabajo exigente y responsabilidades de la mayoría de los gerentes de empresas en el entorno competitivo actual, es poco probable que muchos administradores harán que el tiempo para aprender más sobre el aspecto técnico de seguridad de la información. Dicho esto, es recomendable que los profesionales de seguridad de la información toman clases de gestión y de negocio para ayudarles a aprender más acerca del entorno de la organización. Si lo hacen, van a ser más eficaces en el tratamiento de las cuestiones de gestión superior, que a su vez dará lugar a programas más eficaces de seguridad de la información.

Desde un punto de vista socio técnico, una brecha digital en la seguridad de la información puede ser vista como un conjunto de las diferencias existentes en cuanto a las habilidades de

seguridad de la información y el conocimiento, la percepción de seguridad de la información, las normas sociales, y las relaciones interpersonales, cualquiera o todos los cuales pueden resultar en las diferencias en el rendimiento de seguridad de información entre individuos. Una brecha digital en seguridad de la información dentro de las organizaciones por lo tanto no es sólo una cuestión de acceso a los sistemas de información que han puesto en práctica adecuada tecnología de seguridad de la información; también es una cuestión de diferencias considerables en las competencias, conocimientos, responsabilidades, las percepciones y las relaciones interpersonales entre los distintos miembros de la organización (Albrechtsen y Hovden, 2009). Desde esta perspectiva, varias brechas digitales pueden existir dentro de seguridad de la información, en relación con, por ejemplo, la edad, el género, la experiencia, educación y ocupación. En este artículo se discutió la brecha digital en la seguridad de la información en cuanto a las diferencias existentes en las vistas de seguridad de la información y las expectativas entre los profesionales de seguridad de la información y de los usuarios.

El artículo tiene como objetivo discutir una brecha digital seguridad de la información entre los administradores de seguridad de la información y de los usuarios mediante la exploración similitudes y diferencias entre sus puntos de vista sobre la experiencia y las prácticas de seguridad de la información en las organizaciones.

El propósito se acercó mirando cómo los administradores y usuarios ven su propio papel en comparación con la forma en que experimentan el papel del otro, y en cómo experimentan las medidas de seguridad administrativas.

El mantenimiento de seguridad de la información en una organización es tarea de la información del administrador de seguridad de la información. Los usuarios, por su parte, tienen otras igualmente importantes, tareas de trabajo, principalmente orientada hacia el logro de los objetivos de la organización. Sin embargo, los usuarios tienen la responsabilidad de mantener la seguridad de la información ya que esta es también uno de los objetivos de la organización. La brecha digital de seguridad de la información dentro de las organizaciones descritas en este artículo no es en sí mismo una amenaza para la funcionalidad de gestión de seguridad de la información. Sin embargo, las diferencias de enfoque, la experiencia, la comprensión y las prioridades entre los administradores y usuarios en este resultado de

campo en las estrategias de gestión basadas en la vista de prejuicios que los usuarios son más de una amenaza a la seguridad. Este enfoque es probable que mejore la comprensión de cada grupo de trabajo y para reducir la brecha entre ellos, con lo que las medidas de seguridad de la información sean más eficaces.

Herath (2009), llevó a cabo un estudio en colaboración con el Grupo de Trabajo de Cyber, División de Buffalo, Oficina Federal de Investigaciones (FBI). En el cual se pidió a los empleados de varias organizaciones a participar en una encuesta basada en la web, debido a la naturaleza del estudio, un permiso para llevar a cabo la encuesta a los empleados de la administración de cada organización. Se utilizo Smart PLS 2.0 para la validación de medición y prueba del modelo estructural.

Los resultados muestran que la motivación intrínseca juega un papel en el comportamiento de los trabajadores relacionados con el cumplimiento de la política de seguridad de la información. Se encontró que, si los empleados perciben que sus comportamientos de cumplimiento de seguridad tienen un impacto favorable en la organización o beneficio, son más propensos a tener este tipo de acciones. También, se muestra que las creencias normativas tienen una significación de impacto en el comportamiento de los empleados que sugieren que las creencias respecto a las expectativas de los superiores, la administración de TI y los compañeros parecen tener el mayor impacto en el comportamiento de seguridad de los empleados.

Ellos concluyen que, los comportamientos de seguridad para el usuario final son una parte importante de la seguridad de la información en toda la empresa. La investigación es un esfuerzo para examinar diversos factores de motivación que fomentan comportamientos de seguridad de la información en las organizaciones. En particular, este estudio explora la función de las sanciones, presiones y la contribución percibida como factores de comportamientos seguridad de la información motivadora. Para los investigadores de seguridad de la información, este estudio hace una contribución importante para la comprensión del problema de alentar conductas seguridad de la información de los empleados utilizando un enfoque basado en teoría bien fundamentada microeconómica, sociología y psicología. El documento integra diversos mecanismos de motivación en un

modelo empíricamente comprobable para alentar conductas de seguridad en las organizaciones. Al poner a prueba al mismo tiempo las relaciones entre las sanciones, influencia social, aportación de acciones de los empleados y las intenciones de cumplimiento de política, este estudio evalúa la eficacia de estos motivadores y ofrece sugerencias sobre cómo los administradores pueden mejorar el cumplimiento de la política de seguridad de la información en sus organizaciones.

Hedström, Karlsson y Allen (2011), publicaron un estudio que tiene como propósito desarrollar un modelo nuevo para las prácticas de seguridad de la información en una organización, y en este caso demuestran la capacidad del modelo para identificar áreas de valor entorno a la seguridad de la información y la práctica asistencial. Este estudio se llevó a cabo en un pequeño hospital del condado de Suecia en el centro de Suecia, el hospital sirve a aproximadamente 90 000 ciudadanos.

El modelo de cumplimiento basada en el valor guio su perspectiva, así como sirvió de base para la recopilación de datos y análisis. El enfoque durante la recogida de datos fue en comparaciones entre las NIA prescritos y NIA real (es decir, de cumplimiento) en cada clínica con el fin de identificar qué valor conflictos y racionalidades que existen en esa clínica específica subyacente. Los datos fueron recogidos a través de entrevistas, observaciones y documentos.

Una práctica de seguridad de la información involucra a toda la organización, de la alta dirección y el consejo de administración, al personal utilizando diferentes sistemas de información de la organización. Este estudio ofrece otra perspectiva de gestión de seguridad de la información, llevando a los gestores y diferentes racionalidades empleados como punto de partida para la gestión de seguridad de la información y el cumplimiento. Para la práctica, esto significa que la gestión de la seguridad de la información no sólo debe centrarse cumplimiento de las normas, pero ver como seguridad de la información contextual y ver a los usuarios como recursos y no como problemas. También significa la visualización de seguridad de la información como una cuestión estratégica que debe ser integrado con la gestión empresarial. Para la investigación que significa desarrollar y evaluar modelos,

procesos y herramientas de apoyo a una perspectiva basada en el valor de la gestión de seguridad de la información.

Chander, Jain y Shankar (2012), realizaron un estudio donde el ejercicio estaba generado con los siguientes parámetros: compromiso de la dirección, la identificación y clasificación de los activos de información, herramienta tecnológica, estructura y los recursos de la organización, es la política y los procedimientos, la sensibilización, la educación y la formación, la motivación, la recompensa y el castigo, físico y auditoría de seguridad ambiental

Este estudio ha tratado de estudiar las interrelaciones entre los diversas prácticas y la estructura subyacente en seguridad de la información. Según lo revelado por el diagrama de estudio del Modelado Estructural Interpretativo, todos los factores están afectando mutuamente y están estrechamente vinculados indicando que se requiere igual énfasis en cada uno de ellos de lograr es en una organización. Desde hay variables autónomas se han encontrado en el análisis anterior, se demuestra que todos variable de influencia de seguridad de la información. Estas conclusiones son de gran utilidad para los tomadores de decisiones estratégicas en una organización. El modelo gráfico es de importancia en la comprensión de cómo los diversos factores que afectan están en una interactúan organización e influencia entre sí.

El Modelado Estructural Interpretativo se ha puesto de manifiesto que las variables operativas relacionadas con la aplicación, tales como la identificación y clasificación de los activos de información, el uso de herramientas / soluciones tecnológicas y la protección del medio ambiente físico y son conducidos a través de apoyo de la dirección.

Para futuras investigaciones, los autores sugieren que la técnica de modelado de ecuaciones estructurales (SEM) puede utilizarse para corroborar los hallazgos del Modelado estructural interpretativo. Algunas de las variables han sido mancomunadamente ser parte de un subconjunto debido a su naturaleza similar, pero es posible tratarlos como variables independientes, investigaciones futuras podrán establecer sus interrelaciones también.

Finalmente, el modelo base del actual estudio de Tu, Yuan, Archer, y Connelly (2018), que presentan un estudio basado en la complejidad de los problemas de gestión de la seguridad, los conflictos entre valores y las directrices profesionales y para hacer frente a esta brecha de investigación, este estudio se centró en la Gestion de seguridad de la información en el nivel organizacional, donde se estudian los factores organizativos que determinar el éxito de la Gestion de seguridad de la información. Sobre la base de los estándares de la literatura y de la Gestion de seguridad de la información, este estudio intenta llenar el vacío en la comprensión de la eficacia de la Gestion de seguridad de la información mediante la identificación de factores críticos de éxito y la Gestion de seguridad de la información y el desarrollo de un modelo de actuación de Gestion de Seguridad de la información para probar empíricamente la validez de los factores críticos de éxito identificados.

Este estudio toma en cuenta los trabajos que han proporcionado vista conceptual de la Gestion de seguridad de la información a nivel de organización desde diferentes perspectivas: como un componente integrado en la empresa gobierno (Johnston y Hale, 2009; Posthumus y Von Solms, 2004; Tsohou *et al*, 2015;. Von Solms y Von Solms, 2006), como una forma de gestión de riesgos (Chang *et al*, 2011; Dhillon y Backhouse, 2001; Webb *et al*, 2014), y como un ciclo de vida de la toma de decisiones de fases múltiples dinámicas (Ma *et al*., 2009., Nazaret y Choi, 2015; Nyanchama, 2005; Pipkin, 2000).

Los autores mencionan los índices de rendimiento desarrollados para la Gestion de seguridad de la información con base en un modelo de cuadro de mando (Herath *et al.*, 2010). Finalmente se propone un el modelo teórico que puede ser llevado a cabo en diferentes países y las nuevas metodologías se pueden aplicar en el futuro de la investigación para el estudio de los factores críticos de éxito de rendimiento de la Gestion de seguridad de la información.

CAPÍTULO 2. MARCO CONTEXTUAL

Seguridad de la Información Contexto a Nivel Mundial

Los datos arrojados por diferentes instituciones muestran una perspectiva de la importancia de la seguridad de la información en la actualidad. El Informe de riesgo global del 2012 del Foro Económico Mundial, coloco los riesgos de ataques a sistemas informáticos o red entre los cinco principales que el mundo enfrentaría en la próxima década. Dentro del informe de riesgo global del 2017 se puede encontrar este riesgo por encima de la media de los riesgos a nivel global.

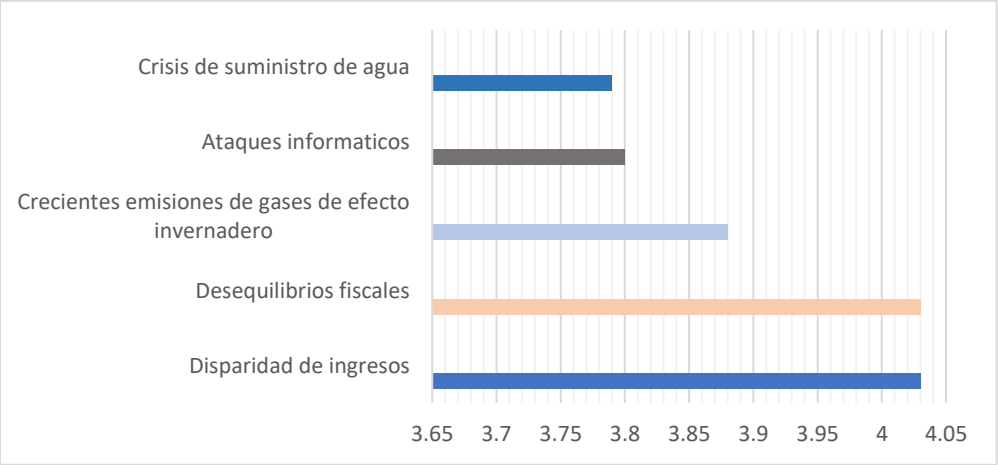


Figura 4. Top 5 Probabilidades en términos de riesgos a nivel mundial. Fuente: Adaptado Foro económico mundial, 2012.

Es difícil encontrar indicadores confiables del impacto financiero de los ataques en red en las organizaciones, sin embargo, con base a los datos del Ponemon Institute, el costo promedio del crimen de ataques cibernéticos para una muestra de 50 grandes empresas estadounidenses fue de US $ 5.9 millones por año, un incremento anual del 56%. Se sugiere que los riesgos a un sistema o red constituyen una amenaza significativa para las empresas, pero se necesita más información para permitir que las organizaciones evalúen el alcance del riesgo, ya que muchas siguen sin informarse (Foro económico mundial, 2012).

El informe de seguridad de Trustwaves 2018 resume que casi todas las industrias, países y tipos de datos estuvieron involucrados en una violación de algún tipo. La tendencia más obvia, basada en fuentes como la base de datos de vulnerabilidad nacional de los Estados Unidos, es que los incidentes de seguridad y las vulnerabilidades individuales han aumentado

(Trustwaves,2018). El informe muestra un aumento significativo en las debilidades que la base de datos de vulnerabilidad nacional de los Estados Unidos catalogó a partir del 2012, con un aumento particularmente grande en 2017.

El informe de Symantec para el mismo año destaca tendencias similares e incluso las pequeñas empresas, que antes tenían poco interés, ahora están en el foco de los atacantes. Nos muestra un aumento del 29% en las vulnerabilidades relacionadas con el sistema de control industrial y un 13% de incremento global en vulnerabilidades reportadas (Symantec, 2018).

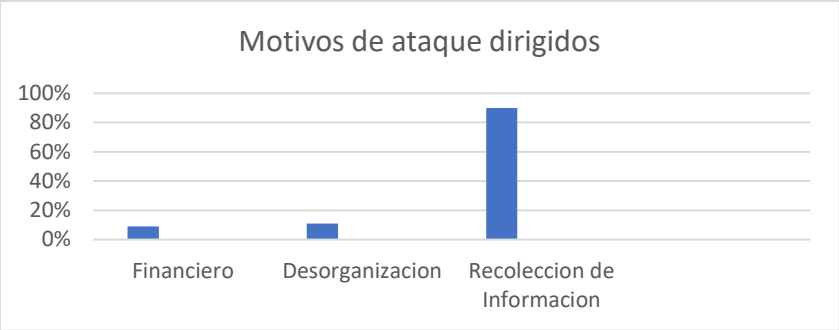


Figura 5. Motivos de ataques dirigidos. Fuente: Adaptado Symantec,2018.

Los datos de motivos conocidos de grupos de ataque dirigidos (Gráfico 3) nos dice que el 90% de los grupos se centran en la recopilación de información, un 11% en provocar desorganización y el 9% en el aspecto financiero (Symantec, 2018).

Con base a dichos datos se sabe que la información es uno de los bienes más propenso a vulnerabilidades al mismo tiempo es uno de los recursos importantes dentro de la organización, por lo cual es necesario protegerla de amenazas internas y externas. Esta concienciación se debió al hecho de que los incidentes de seguridad pueden llevar a consecuencias severamente adversas para las organizaciones, como pérdidas sustanciales para la industria a través de la pérdida directa de activos de información e impacto financiero, una pérdida en la reputación de la organización, la confianza del cliente y una pérdida de la productividad de los empleados o el riesgo de problemas legales (Palaniappan, 2015).

Principales Incidentes De Seguridad De La Información, Situación En América Latina

Al referirse específicamente a la problemática que concierne a América Latina, primero se debe reconocer que la región está desigualmente conectada, por lo que unos países enfrentan un mayor riesgo que otros. Aunado, a ello se tienen niveles bajos de defensa para ciberataques en América Latina (Martino, 2012).

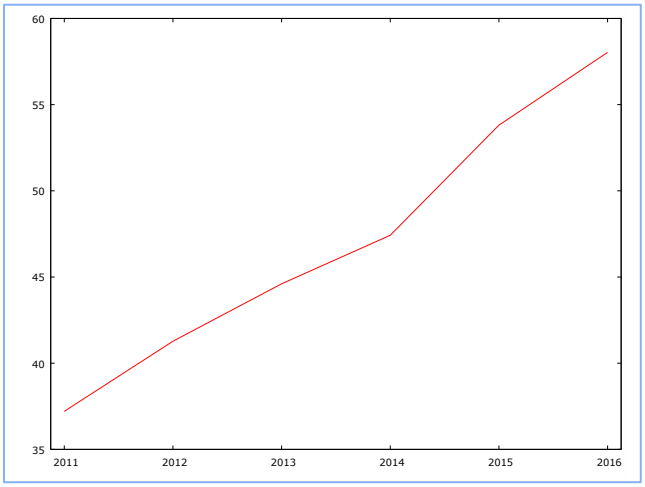
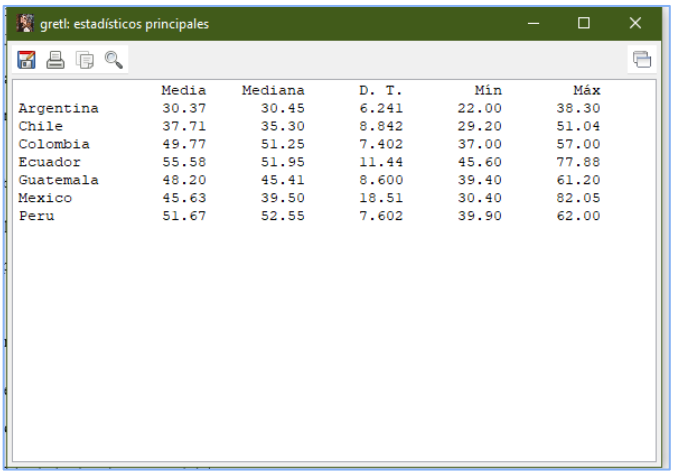


Figura 6. Uso de Internet en Latinoamérica. Fuente: Elaboración propia con base en Informes de Desarrollo Mundial de las TIC 2012-2017.

Los datos con base en el informe de Desarrollo Mundial de las Telecomunicaciones/TIC y bases de datos emitido por la Unión Internacional de Telecomunicaciones, indica que el uso de internet en los países de Latinoamérica tiene una tendencia al alza, por lo cual es necesario estar preparados para un entorno más grande y con mayores riesgos (Figura 4).

Chile es uno de los países de Latinoamérica con el mayor porcentaje de uso de internet (83 % de la población), seguido por argentina con un 70.9 %, mientras que Guatemala tiene uno de los porcentajes más bajos dentro de los países comparados con el 38.50 % de la población. Países como, Colombia, Ecuador y México, se encuentran con el 50 % de su población que usa internet dentro del país. Todos estos países muestran un aumento porcentual, durante el 2016 la media en estos países de Latinoamérica fue de 53% de población que hace uso de internet.

Después de conocer el alcance de internet en estos países, hay que analizar los incidentes que se han presentado en empresas de los países de América Latina, los datos que se presentan en *ESET Security Report* Latinoamérica 2017, muestra que la actividad maliciosa en los países latinoamericanos se observó de manera continua durante el año 2016 con un porcentaje promedio de 40.81% de ataques de malware. De acuerdo con los resultados de las encuestas aplicadas para este informe, Colombia tuvo el mayor número de incidentes con un 46.7%, un porcentaje mayor que el promedio anual. Mientras que Argentina tuvo el menor porcentaje de incidentes en el año con un 31.2 % de incidentes.



	Media	Mediana	D. T.	Mín	Máx
Argentina	30.37	30.45	6.241	22.00	38.30
Chile	37.71	35.30	8.842	29.20	51.04
Colombia	49.77	51.25	7.402	37.00	57.00
Ecuador	55.58	51.95	11.44	45.60	77.88
Guatemala	48.20	45.41	8.600	39.40	61.20
Mexico	45.63	39.50	18.51	30.40	82.05
Peru	51.67	52.55	7.602	39.90	62.00

Figura 7. Incidentes de malware países de Latinoamérica, periodo 2011-2017. Fuente: Elaboración propia con base en Informes ESET 2012-2017.

Al comparar la serie temporal desde el 2011 al 2016, se observa que, Ecuador tiene el promedio más alto un 55% durante este periodo (Figura 5). Mientras que Argentina tiene la media más baja con un 30% de incidentes registrados, en los países comparados de Latinoamérica en este periodo.

Lo anterior coloca, nuevamente, a los códigos maliciosos como la principal fuente de eventos no deseados e inesperados en América Latina, aunque con ligeros cambios al año anterior.

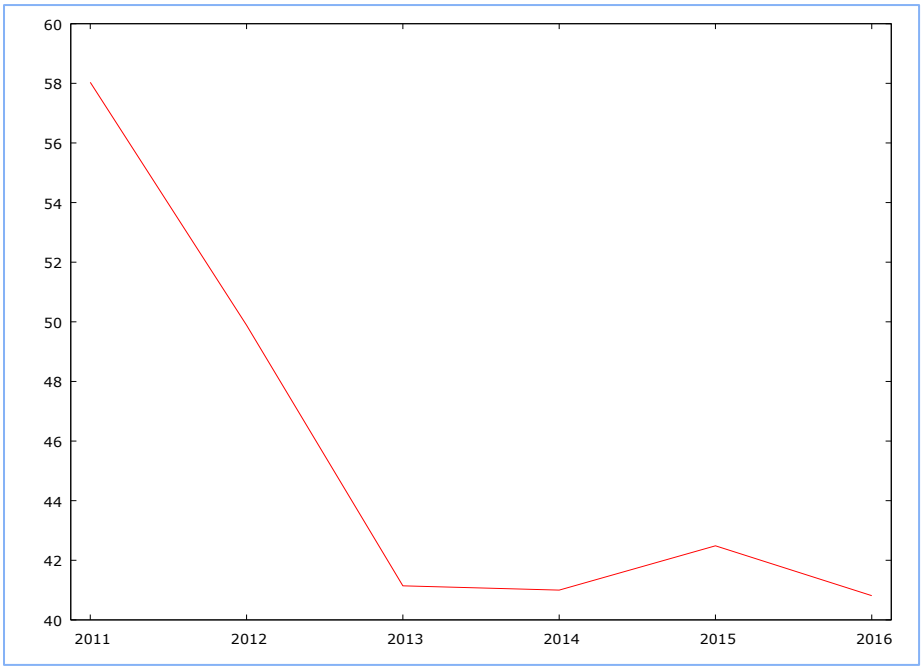


Figura 8. Incidentes de malware países de Latinoamérica. Fuente: Elaboración propia con base en informes ESET 2012-2017.

Si comparamos los datos recopilados acerca del porcentaje de infecciones por malware que sufrieron las empresas, destaca que se redujo ligeramente respecto a la edición anterior del informe, pasando en el 2015 del 42% a 40% durante el 2016. Sin embargo, al revisar los resultados históricos del ESET Security Report, observamos una tendencia que se mantiene con el paso de los años (Figura 6).

Ecuador tiene el promedio más alto en incidentes de malware durante el periodo y comparado con el promedio anual es representativamente más alto en cada uno de los años; lo cual no muestra un buen indicador para el país respecto a su entorno de seguridad de la información (Figura 7), por lo cual es necesario que Ecuador aumente su nivel se seguridad para disminuir el riesgo que representa.

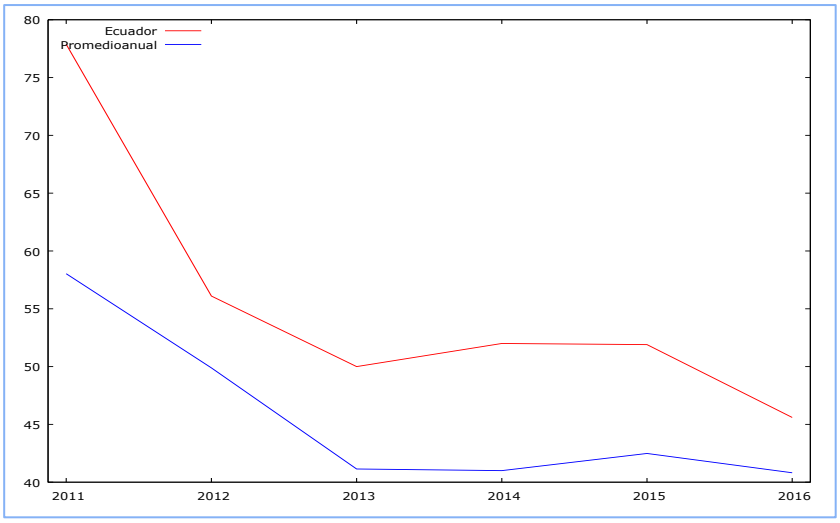


Figura 9. Incidentes de malware Ecuador. Fuente: Elaboración propia con base en informes ESET 2012-2017.

Mientras que la comparación con Argentina (Figura 8) que es el país con el menor promedio de incidentes nos muestra como el porcentaje es mucho menor que la media del resto, demostrando que a pesar de ser uno de los países con más uso de comunicación en línea tiene un menor porcentaje de incidentes dentro de Latinoamérica.

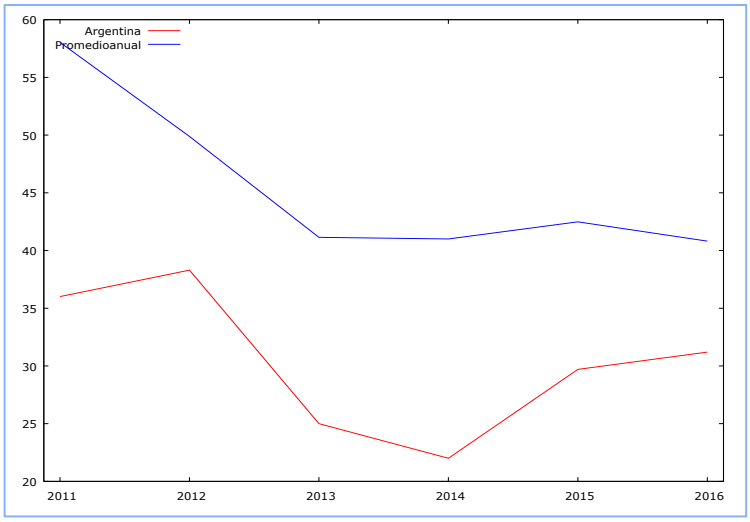


Figura 10. Incidentes de seguridad argentina. Fuente: Elaboración propia con base en informes ESET 2012-2017.

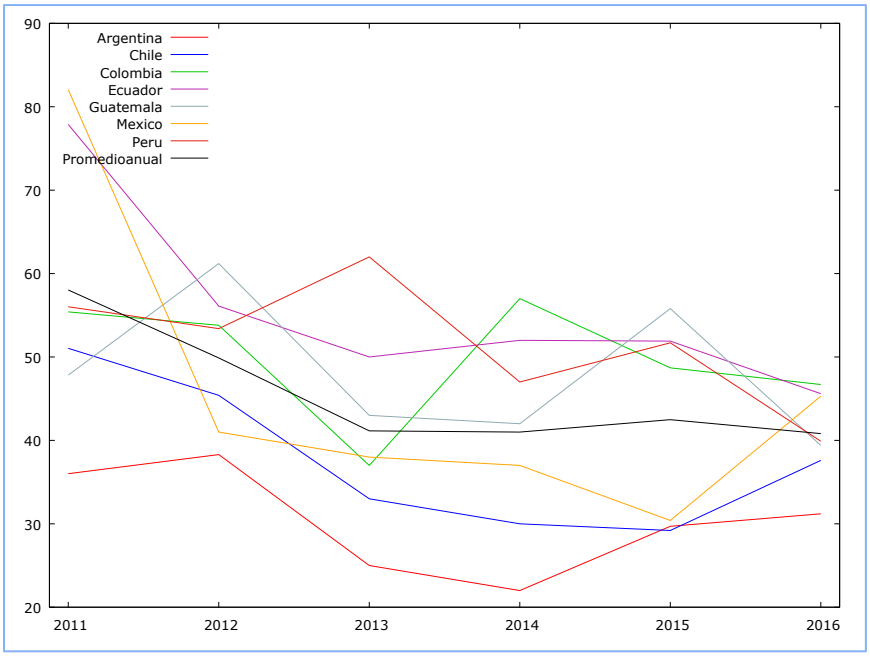


Figura 11. Incidentes de seguridad América Latina. Fuente: Elaboración propia con base en informes ESET 2012-2017.

Por último, en cuanto a la situación en México existe una disminución de incidentes de gran impacto en el 2012 manteniéndose debajo de la media hasta el año 2016, donde se obtuvo un incremento porcentual. Mientras que Chile sigue la tendencia de Argentina teniendo un porcentual menor al promedio.

Seguridad De La Información En Las Instituciones Educativas De Nivel Superior En México

En México la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) a través de su encuesta nacional de las TIC es la encargada de censar a las instituciones superiores y dar a conocer aspectos relacionados con la seguridad de la información dentro de las Instituciones de Educación Superior en México (ANUIES,2017).

Las Políticas de seguridad de la información, de las Instituciones de Educación Superior (IES) encuestadas un 62% cuenta con una política de seguridad establecida, mientras que el 37% no tiene una política en referencia a la seguridad. De las 91 IES que tienen una política de seguridad establecida, un 35% está alineada a los objetivos institucionales, un 21% no

incluye objetivos y un 5% indica que existen políticas que incluyen objetivos (Figura 10), pero no están alineados a los institucionales (ANUIES,2017).

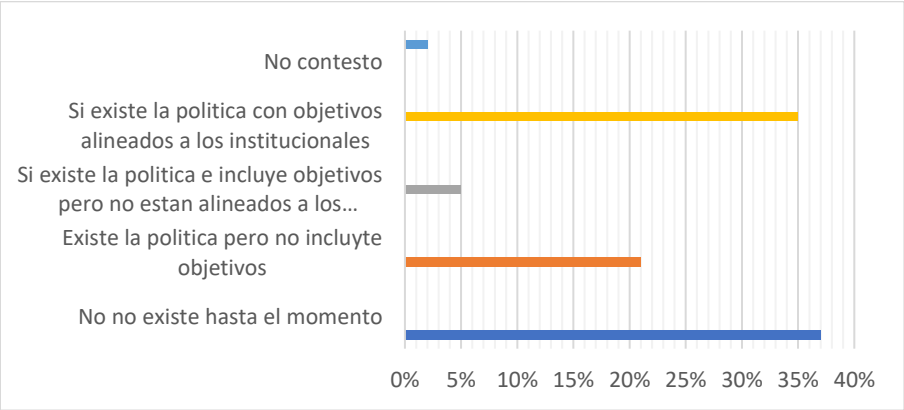


Figura 12. Porcentaje de IES que cuentan con una política de seguridad de la información. Fuente: Adaptado de ANUIES,2017.

Existe una creciente tendencia entre las Instituciones de Educación Superior, a alinear sus políticas de seguridad con los objetivos de la institución. Esto demuestra un avance por parte de las IES, respecto al año anterior, que les permite incorporar la seguridad de la información a las distintas estrategias del ciclo de vida institucional, es decir, en sus personas, procesos y tecnologías.

Marco de referencia de seguridad de la información. El resultado del indicador y su comparativo contra el 2016 determina que las Instituciones de Educación Superior entrevistadas aumentaron un 6% en la aplicación de marcos de referencia de seguridad de la información. Éste mismo se ve reflejado en la disminución de instituciones que no hace uso de marcos de referencia. Sin embargo, de las IES que hacen uso de marcos de referencia solo el 33% lo implementa de manera parcial en algunas áreas (Figura 11).

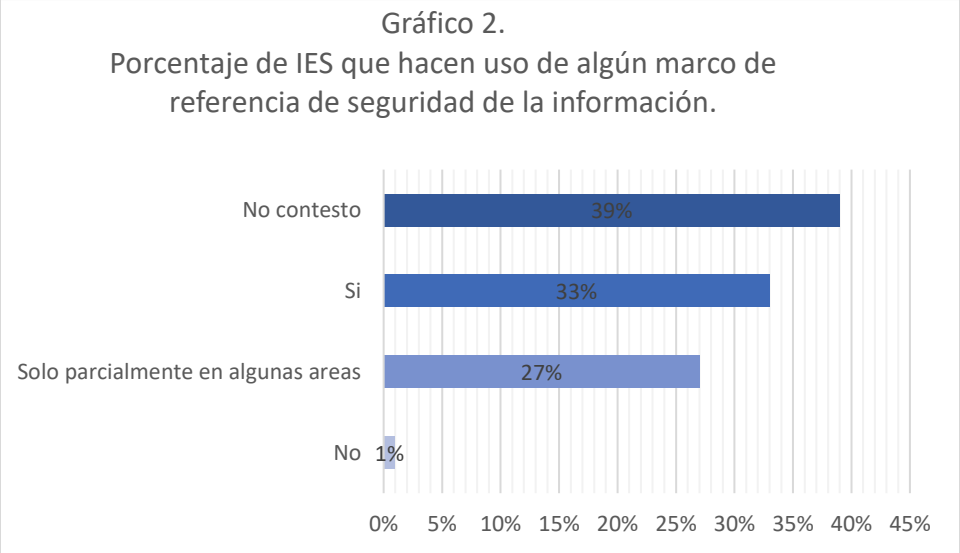


Figura 13. Porcentaje de IES que hacen uso de algún marco de referencia de seguridad de la información. Fuente: Adaptado de ANUIES,2017.

Auditorías de seguridad informática. De las IES que llevan a cabo auditorías un 10% se realiza en específico hacia la seguridad informática, un 29% lleva a cabo auditorías administrativas incluyendo aspectos de TI y seguridad informática, un 8% realiza auditorías específicas y periódicas de seguridad informática y un 52% no realizan auditorías. El resultado del indicador y su comparativo contra el 2016 determina que las Instituciones de Educación Superior entrevistadas dejaron de aplicar cualquier tipo de auditorías de seguridad informática en un 5%. Disminuyendo de la misma manera, las auditorías específicas en 14% y en 6% las auditorías específicas y periódicas. Mientras que las auditorías administrativas aumentaron un 14%.

Metodologías o estándares utilizados para el análisis de riesgos. La gestión de la seguridad de la información en las organizaciones requiere la aplicación de una serie de controles de seguridad formales, informales y técnicos para abordar los riesgos de seguridad complejos (Ahmad, 2011). El estudio de los estándares de calidad de seguridad de la información proporciona ventajas para minimizar los riesgos de daño, robo o fuga de información; permitiendo mantener la integridad, confidencialidad y disponibilidad de la información, además de garantizar la autenticidad y el no rechazo de la misma. También repercute en el

uso debido de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir eficientemente con sus actividades.

El resultado del indicador y su comparativo contra el 2016 determina que las Instituciones de Educación Superior entrevistadas han mejorado respecto al año pasado, aumentando el uso de las metodologías de análisis de riesgos, aunque aún falta el 50% de IES en implementar un estándar de análisis de riesgo.

Plan de continuidad de la operación de TI. Del total de las IES encuestadas un 37% no cuentan con un plan de continuidad documentado, mientras que un 42% cuenta con planes solo para servicios específicos, un 17% tiene implantado un plan de recuperación de desastres, mientras que un 3% cuenta con un plan de continuidad del negocio que incluye un análisis de impacto al negocio.

Los Incidentes de seguridad de la información. Los ataques de seguridad informática a los que se han visto expuestas las IES encuestadas son diversos, siendo los más frecuentes el software malicioso, fallas de energía eléctrica, el correo spam; también se observa que se presentan en las IES ataques informáticos como robo de equipo de cómputo, Phishing scam y fallas de equipo por condiciones ambientales inadecuadas (Tabla 3).

Tabla 4. *Porcentaje de tipos de incidentes de seguridad presentados en las IES.*

	2016	2017	Variación
Otros	1%	2%	1%
Robo de credenciales.	3%	4%	1%
Phishing scam.	7%	8%	1%
Usurpación de identidad en sitios web.	1%	2%	1%
Usurpación de identidad en correo electrónico.	2%	3%	1%

Usurpación de identidad en redes sociales.	2%	3%	1%
Robo de equipo de cómputo.	7%	9%	2%
Correo spam.	14%	12%	-2%
Software malicioso.	13%	13%	0%
Ejecución de comandos o privilegios no autorizados.	2%	2%	0%
Denegación de servicio.	5%	4%	-1%
Puertas traseras en servidores o aplicaciones.	3%	2%	-1%
Sabotaje o vandalismo.	1%	2%	1%
Fallas en energía eléctrica.	18%	13%	-5%
Agua, humedad, temperaturas extremas, etc.	5%	7%	2%
Fallas en equipos por condiciones ambientales inadecuadas.	8%	6%	-2%
Incendios.	0%	1%	1%
Desastres naturales.	3%	2%	-1%
Sabotaje interno.	2%	1%	-1%
Robo de sesión o terminal.	1%	1%	0%
Espionaje.	1%	1%	0%

No tenemos registros sobre incidentes de seguridad.	1%	3%	2%

Fuente: Adaptado de ANUIES,2017.

El resultado del indicador y su comparativo contra el 2016 determina que las Instituciones de Educación Superior entrevistadas no han variado mucho respecto al año pasado. Sin embargo, las IES han aumentado incidentes como el robo de equipos de cómputo, y humedad y temperaturas extremas en sus instalaciones.

El conocimiento de estos datos muestra la brecha que existe dentro de la IES en cuanto a la implementación de buenas prácticas en seguridad de la información. Mediante el análisis de seguridad de la información, dentro de las instituciones públicas de educación superior podemos conocer y aplicar controles de seguridad, que se operan para asegurarla y que ésta sea utilizada adecuadamente y solo tenga acceso de personas autorizadas.

El desarrollo del análisis de seguridad de la información permitirá conocer las vulnerabilidades existentes en el manejo y gestión de seguridad de la información, de tal forma que se puedan tomar acciones preventivas y correctivas dentro de la institución para evitar que se lleguen a comprometer datos confidenciales. Esto puede favorecer a que otras instituciones tomen el ejemplo de implantación de controles y estrategias.

CAPÍTULO 3. CASO DE ESTUDIO

UNIVERSIDAD DE GUANAJUATO

Antecedentes de la Universidad de Guanajuato

La Universidad de Guanajuato, tiene sus inicios en 1732 como el Hospicio de la Santísima Trinidad, sin embargo, es hasta 1870 que se transforma en el Colegio del Estado. En el año de 1945, el congreso del estado establece la creación de la Universidad de Guanajuato, pero hasta 1994 obtiene su autonomía para gobernarse. A lo largo de su historia, la Universidad ha experimentado cambios, teniendo la capacidad para adaptarse y responder a las demandas que se le presenta en estos tiempos.

Actualmente la universidad cuenta con una población estudiantil cerca de los 42 mil alumnos inscritos en los diferentes niveles educativos, distribuidos en los 4 campus y las 11 escuelas del nivel medio superior, con presencia en 12 municipios en el estado de Guanajuato. En los últimos 100 años la Universidad se ha encontrado en un profundo proceso de modernización y expansión que en conjunto con la transformación de su estructura académico administrativo busca renovar y mejorar la calidad en sus sistemas educativos, donde se busca promover la equidad en el acceso a la educación e incrementar la cobertura para aumentar su presencia en el estado de Guanajuato.

Dirección de Servicios y Tecnologías de la Información (DSTI)

La DSTI surgió en el marco de la nueva estructura académico–administrativa de la Universidad de Guanajuato en el mes de octubre de 2011, con el objetivo de construir vías de comunicación entre la comunidad universitaria y con la sociedad en su conjunto. La Dirección de Servicios y Tecnologías de la Información fue instituida para operar y mantener el funcionamiento de la infraestructura de tecnologías de la información, así como el Sistema Bibliotecario de la Universidad.

En 1991 surge la “Red Universitaria de Teleinformática y Comunicaciones (RUTyC)” como un proyecto innovador en la institución, cuando inicia este proyecto, la Universidad de Guanajuato era la quinta universidad en registrar su dominio ugto.mx ante el NIC. En 1995, desaparece el proyecto RUTyC, dando paso al Departamento de Telecomunicaciones y

Cómputo como una estructura formal dentro de la Institución. Las funciones de este nuevo departamento eran desplegar la conectividad en todas las dependencias administrativas y académicas de la Universidad de Guanajuato, además de proveer de servicios de red como; el correo electrónico, el acceso a la www y el soporte técnico. En 1994 se incorpora el Departamento de Telefonía al Departamento de Telecomunicaciones y Cómputo siendo su función dar servicios de voz que satisficieran las necesidades de la Institución. En enero de 2004 fue creada la Coordinación General de Sistemas y Telecomunicaciones, dependiente de la Secretaría Administrativa quedando integrados los departamentos de Telecomunicaciones, Telefonía e Informática. En enero de 2009 se cambió la estructura orgánica en la Universidad de Guanajuato a un modelo por Campus y un Colegio de Nivel Medio Superior con una Rectoría General, impactando a la estructura de la Coordinación General de Sistemas y Telecomunicaciones la cual se desintegra, quedando en diferentes Secretarías; como Coordinación de Telefonía, Departamento de Telecomunicaciones y Departamento de Sistemas de Información. En diciembre de mismo año, se crea la Dirección de Tecnologías de la Información la cual se compone por el Departamento de Telecomunicaciones y la Coordinación de Telefonía, su visión se plasma sobre el despliegue de las Tecnologías de la Información y Comunicación a toda la comunidad Universitaria. Por otro lado, en 1995, se creó la Dirección General de Apoyo Académico, esta Dirección tomó en sus manos los servicios bibliotecarios y de telecomunicaciones. En 1999, se unió a dicha dependencia administrativa la recién creada Dirección de Archivos y Fondos Históricos. Entre 2004-2005 durante el periodo del Rector Arturo Lara López, desapareció la Dirección General de Apoyo Académico. En 2009 la Dirección de Apoyo Académico, se conforma por los departamentos de Sistema Bibliotecario y Fondos Históricos y Biblioteca Armando Olivares Carrillo, además de apoyar de manera conjunta las acciones de la Coordinación del Archivo General. En octubre de 2011, se crea la Dirección de Servicios y Tecnologías de la Información, cuando debido a cambios en la estructura administrativa y en base a las crecientes necesidades de la comunidad universitaria, se decide fusionar la Dirección de Tecnologías de la Información con la Dirección de Apoyo Académico.

Funciones de la Dirección de tecnologías de la información

1. Proyectar, implementar y administrar la infraestructura y servicios de tecnologías de la información y la comunicación para la comunidad universitaria;
2. Proyectar y generar las herramientas informáticas que faciliten y sustenten la toma de decisiones en la institución;
3. Analizar, proponer y desarrollar herramientas que ayuden a cerrar la brecha digital en los procesos administrativos y académicos;
4. Difundir los servicios que ofrece la Dirección;
5. Realizar las actividades adicionales derivadas de la naturaleza del área;
6. Las demás que le sean encomendadas por la Rectoría General, Secretaría General, así como los órganos colegiados, de conformidad con sus atribuciones; y
7. Administrar sus archivos y gestión documental en base al Sistema Institucional de Archivos.

Misión

La DSTI es el área encargada de proyectar, implementar y administrar la infraestructura y servicios de tecnologías de la información y la comunicación para la comunidad universitaria, en apoyo a las funciones sustantivas con un enfoque de mejora continua.

Visión

Ser el área líder en tecnologías de información y comunicación, que provee servicios de alta calidad a la comunidad universitaria para el desarrollo de sus actividades, soportados en una infraestructura de vanguardia y capital humano altamente capacitado y comprometido, convirtiéndose en un referente dentro de la comunidad académica internacional.

Valores

- La verdad
- La libertad
- El respeto
- La responsabilidad
- La justicia
- La honestidad
- El compromiso

Coordinación de Seguridad y Monitoreo

Entonces, hablamos de la Coordinación de Seguridad y Monitoreo ya que esta es el área específica en seguridad descrita en el organigrama de la institución (Anexo 1), dirige sus acciones, esfuerzos en proteger y monitorear la infraestructura de red de los Campus y Sedes de la Universidad de Guanajuato del mal uso, actos malintencionados e incidentes relacionados con la seguridad de la red para mantener y asegurar la disponibilidad del servicio de internet e intranet a los usuarios aplicando metodologías, uso de herramientas y estándares internacionales que nos ayuden a asegurar la confidencialidad, integridad y disponibilidad de los servicios de red (Manual Organizacional UG, 2019)

Funciones

- Promover y proponer la incorporación de medidas tecnológicas y metodologías que contribuyan a mejorar la calidad de los servicios educativos dentro de la Institución.
- Formular y presentar las propuestas de normas, políticas y proyectos para mejorar, optimizar los servicios de red y proporcionar un ambiente seguro que provea la integridad de la información que transmite por la red.
- Administrar y supervisar el tráfico que transita por la red Institucional para proporcionar la seguridad requerida en las unidades y dependencias de la Universidad.
- Realizar estudios de viabilidad, compatibilidad y rentabilidad para apoyar la toma de decisiones en la propuesta de adquisición de software y hardware que fortalezca los esquemas de seguridad de la red institucional.
- Realizar un monitoreo permanente con el apoyo de herramientas tecnológicas de seguridad y monitoreo, para garantizar un servicio seguro y óptimo de red e internet.
- Proporcionar soporte técnico en la instalación, configuración, administración y utilización del antivirus institucional.
- Definir, evaluar y proponer la implantación de mecanismos de protección y seguridad de la infraestructura institucional, en coordinación con los demás departamentos de la DSTI.

- Apoyar en el crecimiento de infraestructura para las redes locales, metropolitana y de área amplia en conjunto con las coordinaciones correspondientes para asegurar que la infraestructura este a la vanguardia de las nuevas tecnologías cubriendo las necesidades actuales y futuras de los clientes.
- Identificar y aplicar acciones de mejora continua en el área para mantener altos estándares de calidad en los servicios que se ofrecemos.
- Definir, evaluar y proponer metodologías para los procesos de diagnóstico de vulnerabilidades en los sistemas.
- Mantener estrecha comunicación con instituciones externas para promover acciones de colaboración de beneficio mutuo.

Incidentes frecuentes de seguridad en la Universidad de Guanajuato

Existen diferentes tipos de incidentes que se presentan dentro de la institución, ya que la universidad tiene un alto número de entrada y salida de datos mensualmente (Anexo 2), debido a esto se presentan incidentes siendo los más frecuentes los descritos a continuación.

SPAM: El spam es el abuso de los sistemas de mensajería electrónica para enviar mensajes no solicitados de forma indiscriminada. Si bien la forma más reconocida de spam es el correo electrónico no deseado, el término se aplica a abusos similares en otros medios y medios (Whitworth y Whitworth, 2004).

Phishing : un ataque de phishing es uno de los ataques de ingeniería social. El phishing se trata como el proceso de atraer a una víctima a un sitio web falso haciendo clic en un enlace determinado. En general, la víctima se encuentra con el enlace en un mensaje de correo electrónico enviado a él o en una página web que está navegando por él. Los usuarios deben ser conscientes de no hacer clic, descargar o abrir un archivo recibido en archivos adjuntos de correo electrónico, ya que puede contener malware . Los atacantes pueden utilizar correos electrónicos no autorizados, es decir, phishing para robar la información importante del usuario, como las credenciales de la cuenta bancaria, incluido el inicio de sesión del usuario , la contraseña y el número de la tarjeta de crédito (Srinivas, Kumar Das, y Kumar, 2019).

Por ejemplo, la dirección de la página real www.facebook.com y una página falsa seria www.wfacebook.com, que tiene una "w" es una página diferente ya que se encuentra con otro dominio, pero tienen exactamente el mismo contenido que hace que pase desapercibida para los ojos inexpertos del usuario común y provoca que el usuario caiga en la trampa, este ataque también es usado para generar correos aparentemente provenientes de direcciones legitimas que tienen objetivos malintencionados.

Equipo con la seguridad comprometida (equipo hackeado): En algunas ocasiones los cibercriminales después de lograr vulnerar un equipo o algún servidor que no contaba con las medidas de seguridad suficientes o las actualizaciones más recientes, pueden ser accedidos remotamente realizar alguna actividad ilegal o malintencionada, que van desde el envío de SPAM, distribución de malware, ataques de DOS, ataques de fuerza bruta o para montar sitios web falsos en algún subdirectorio con el objetivo de robar información o para distribuir pornografía; cualquier tipo de actividad es considerada ilegal ya que se realiza sin el consentimiento del administrador. Aunque esto se realiza sin el conocimiento del administrador, él y la empresa son los responsables de todos los daños que esto llegue a provocar, por este motivo los cibercriminales realizan estas actividades de otros equipos de manera anónima ocultando su identidad y controlando el equipo a través de conexiones remotas ocultas con diferentes técnicas de anonimato para dificultar su rastreabilidad.

Infecciones de malware: Malware es un software que se ejecuta de manera muy similar a otros programas. La diferencia clave entre malware y no malware (benigno) está en el comportamiento de ese software en particular. Si una parte del software muestra actividades maliciosas como robar datos del usuario, replicar, deshabilitar cierta función de seguridad, servir como puerta trasera o ejecutar comandos no previstos por el usuario, entonces puede considerarse como malware (Shaid y Maraaof, 2014).

Dentro la UG las infecciones por malware más comunes son realizadas por medio de los dispositivos extraíbles (USB), pero también se han presentado infecciones por correo SPAM y en ocasiones por realizar instalaciones de software pirata ya que en su mayoría contienen “Cracks o activadores” que generalmente se encuentra infectados por algún tipo de malware,

que por eso no es de extrañarse que en la mayoría de los casos soliciten deshabilitar el antivirus para poder ejecutarlo de manera adecuada.

Botnets: Son redes formadas por bots, que son alimentadas por equipos infectados por malware, y son controlados de manera remota para realizar ciertas actividades ilegales. El nombre dado botnet, que es una combinación de bot y red. Dado que Internet contiene grandes cantidades de capacidad de procesamiento y ancho de banda de red no utilizados, los actores malintencionados encontraron formas de utilizar esas máquinas para sus objetivos (Vormayr, Zseby y Fabini, 2017). En ocasiones el mismo bot puede realizar tareas de espionaje en el equipo del usuario e incluso pueden recibir instrucciones para realizar ataques masivos como DDOS de forma simultánea contra algún sitio web.

Defacements: La degradación del sitio web es la forma más obvia de piratería en la que un atacante intenta comprometer un servidor y luego reemplaza el contenido legítimo y autorizado del sitio web con imágenes y texto propios.

CAPÍTULO 4. MARCO METODOLOGICO

Metodología

En este capítulo se presentan los aspectos metodológicos de la investigación. Se expone la perspectiva de indagación que se adoptó, el tipo de investigación a seguir y se determinaron las técnicas y los instrumentos a utilizar.

La investigación que aquí se presenta se describe como un análisis cualitativo, transversal de diseño no experimental sustentado por una estrategia de estudio de caso de tipo descriptivo con enfoque interpretativo, que tiene por objeto el abordaje del fenómeno organizativo dentro de un contexto real. Para abordar el objeto de este estudio, se propone como estrategia de investigación la que a continuación se presenta:

1. Marco conceptual de seguridad de la información y de los factores críticos potenciales.
2. Aplicación de un instrumento cualitativo (entrevistas).
3. Análisis, interpretación e informe de los resultados globales.

El marco teórico y conceptual permitirá conocer los principales conceptos sobre el tema y con esto ampliar la comprensión de este. De entre las numerosas estrategias de investigación existentes para la recopilación de datos que faciliten la construcción de la comprensión interpretativa, se optó por seleccionar la entrevista con informantes de calidad cuya función es clave en el proceso de implementación y mantenimiento de la Gestión de seguridad de la información, con el objetivo de explorar sus características mediante la inclusión de preguntas abiertas y con ello identificar los factores críticos de éxito.

Investigación cualitativa

Entonces, al ser este un estudio planteado como una investigación cualitativa. Nos referimos a la metodología cualitativa a la investigación que produce datos descriptivos: las propias palabras de las personas, habladas o escritas, y la conducta observable (Taylor y Bogdan, 1992), que tienen el significado de las experiencias de vida o la historia de vida personal, que no se dan en la metodología cuantitativa con un cuestionario estadístico. Así el acceso a la información se realiza a partir de técnicas como la observación participante, las entrevistas, los documentos, los registros, etc.

Como resultado, la metodología cualitativa busca entender la realidad o fragmentos de ella tal como la construye o da significado la propia persona (Pizarro, 2000).

Informantes Clave

Dentro de cualquier estudio cualitativo, los informantes o los participantes de la investigación son los elementos más imprescindibles, ya que ellos aportan gran parte de la información principal sobre el tema de investigación.

En este estudio, estas personas son a quienes se les solicito información y se les realizó entrevistas semiestructuradas para poder profundizar en la problemática en cuestión. Con ellas se obtiene el grueso de la información que permite comprender el problema y realizar las interpretaciones correspondientes.

Para este análisis, se consideran como informantes clave a las personas que participan el área de tecnologías de información de la Universidad de Guanajuato específicamente los involucrados en seguridad de la información y a su vez quienes poseen los conocimientos e información necesaria sobre el problema a investigar (Tabla 4). La selección de estos informantes recae en los siguientes criterios:

1) Son las personas que tienen acceso a la información más importante sobre la problemática en estudio.

2) Son las personas que tienen la experiencia y conocimiento sobre el tema que se está abordando.

3) Son las personas que tienen la voluntad para cooperar en la investigación.

Tabla 5. *Informantes clave.*

Nombre del puesto	Motivo de la entrevista
Jefe de servicios administrativos	Área encargada de colaborar en proyectos de implementación de Gobierno de Tecnologías de la Información, de Control Interno y de mejores prácticas para mejorar los servicios que presta la

	Dirección y hacer más eficiente y controlado el desarrollo de sus funciones.
Jefe de sistemas de información	Área encargada de validar proyectos de implementación de seguridad de la información en conjunto con el Jefe de Redes y Conectividad para asegurar la integridad, confidencialidad y respaldo de la información contenida en la infraestructura a cargo de la Dirección, de acuerdo con las necesidades de la Institución y a la normativa.
Jefe de Redes y Conectividad	Área encargada de administrar planes y programas de mantenimiento correctivo y preventivo para mantener la adecuada operación de la infraestructura de Redes, Conectividad y Centros de Datos.
Coordinador de Seguridad y Monitoreo	Área encargada de coordinar la administración de las plataformas de monitoreo y seguridad institucionales; implementar estrategias de seguridad de la información y redes; participar con los administradores de redes de los campus para diagnosticar y dar solución a contingencias de seguridad en Tecnologías de la Información.
Asistente de seguridad y redes inalámbricas	Área encargada de instalar, operar, dar mantenimiento a servidores (sensores) para funciones de seguridad y monitoreo de la red inalámbrica institucional.
Asistente de seguridad y monitoreo	Área encargada de elaborar y enviar reportes acerca de las fallas de la red (enlaces y equipos activos de red) y sistemas de cómputo institucionales (servidores y almacenamiento) para tomar acciones pertinentes en caso de contingencias o incidentes de seguridad.
Asistente de seguridad	Área encargada de los incidentes presentados en el campo del correo institucional.

Jefe de proyectos estratégicos	Área encargada de administrar los proyectos y planes estratégicos de la Dirección de Servicios y Tecnologías de la Información, con un enfoque de innovación y mejora continua, en apoyo a las funciones sustantivas y adjetivas de la institución y en beneficio de los usuarios de los servicios que brinda la Dirección.

Fuente: Autoría propia.

Variables de interés

Nuestras variables de interés están definidas como:

Variable independiente

- Seguridad de la información

Variable dependiente

- Factores críticos de éxito

Instrumentos de Recolección de Información

El instrumento aplicado en la presente investigación es: La entrevista semiestructurada.

Entrevista Semiestructurada

En esta sección se define la técnica de la entrevista semiestructurada, la cual ha sido la herramienta utilizada durante el desarrollo de esta investigación.

Valle (2007) enfatiza que la entrevista es una técnica que sirve para la obtención de información relevante para los objetivos de estudio. Este instrumento combina los enfoques prácticos, analíticos e interpretativos implícitos en el proceso que tiene la comunicación (Galindo, 1998).

El uso de la entrevista semiestructurada se entiende como una técnica que permite obtener información y opiniones que no se podrían obtener con una entrevista estructurada y donde

las respuestas están sujetas a preguntas muy concretas (Ortiz, 2007). Por lo que la ausencia de la estructura es lo que se busca, ya que deja al investigador poder aundar varias veces sobre la esencia de una misma pregunta. Por esta razón, la entrevista semiestructurada representa uno de los instrumentos más representativos de la investigación cualitativa.

Esta técnica de recopilación de datos permite obtener información que apoyará la compresión de la problemática que se está investigando, pudiendo establecer preguntas estructuradas y preguntas espontáneas que explican la problemática a investigar. En este sentido, las palabras y los enfoques de los entrevistados son una riqueza de información que el investigador debe aprovechar para poder responder el objetivo propuesto.

Con este acercamiento de lo que es la entrevista, se pudo comenzar a generar la guía de preguntas (Véase Anexos 3), la cual fue adaptada para cada informante clave, debido a que cada uno representaba áreas diferentes dentro de la Universidad de Guanajuato, de esta manera se mantuvo la búsqueda del objetivo general y de los particulares expresados.

Estas entrevistas semiestructuradas aplicadas ayudaron a tener un acercamiento real de lo que es transmitido por el personal en cuanto a su visión de gestión de seguridad de la información que transita por el departamento de la institución y así conocer las diferentes ideas, visiones, perspectivas, etc., que puedan ayudar a comprender la problemática dentro de la Universidad.

Diseño de la Entrevista

Ahora bien, el diseño de la entrevista gira en torno a las dimensiones descritas por el modelo de Tu, Yuan, Archer, y Connelly (2018), sobre los factores críticos de éxito de la Gestion de seguridad de la información que son y han descritos anteriormente:

- Alineación del negocio
- Apoyo de la dirección
- Conciencia organizacional
- Riesgos y controles
- Rendimiento de la Gestion de seguridad de la información

Análisis de Datos

Al término de las entrevistas, se procedió por realizar la transcripción correspondiente para que de esta manera se pudiera trabajar el análisis de éstas.

Se utilizó el programa ATLAS/ti, para los textos obtenidos, de esta manera utilizando los códigos, familias y redes para obtener los resultados de este trabajo. En primer lugar, se hizo una trascripción de las entrevistas grabadas, a partir de las cuales se procedió a la redacción del conjunto de datos. Se analizaron los datos de las entrevistas con el programa ATLAS/ti.

ATLAS/ti es un banco de trabajo de gran alcance para análisis cualitativo de los cuerpos grandes de datos textuales, gráficos y audio. Ofrece una variedad de herramientas para lograr las tareas asociadas a cualquier acercamiento sistemático a los datos, material que no puede ser analizado por acercamientos formales, estadísticos de maneras significativas. En el curso de un análisis tan cualitativo ATLAS/ti ayuda a destapar los fenómenos complejos ocultado en sus datos de una manera exploratoria. Para hacer frente a la inherente complejidad de las tareas y de los datos, ATLAS/ti ofrece un gran alcance e intuitivo ambiente de subsistencias que se centró en los materiales analizados. Ofrece las herramientas para manejar, extraer, comparar, explorar, y vuelva a montar los pedazos significativos de las cantidades de datos en un creativo y flexible ambiente.

Dentro de la investigación social es frecuente que se recurra a la Hermenéutica-Analógica como técnica para la interpretación de textos (Velázquez y Nava, 2014), o más bien para la interpretación de las entrevistas semiestructuradas realizadas a los usuarios de los diferentes departamentos seleccionados para esta tesis.

La hermenéutica como tal, nace con Platón durante la Edad Media y la cual consistía en establecer reglas para la interpretación de textos sagrados (Velázquez y Nava, 2014). En grandes rasgos, consistía en un arte para interpretar textos que estaban enfocados a la poesía, literatura, etc., que contienen un contexto difícil por explicar (Alcalá, 2011). Ante el riesgo de generar una sola interpretación o de inmensas interpretaciones se recurre a la analógica ya que ésta cuenta con una proporción para delimitar las interpretaciones (Velázquez y Nava, 2014).

Beuchot (2015), en su escrito “Elementos esenciales de una hermenéutica analógica”, comenta que la Hermenéutica-Analógica evita llegar a esos extremos de interpretación que hacen referencia a una hermenéutica univocista, (es decir, solo acepta una interpretación válida mientras que las demás son inadecuadas) y de una hermenéutica equivocista (la cual considera todas las interpretaciones son válidas, llegando a la ambigüedad), de ahí que la hermenéutica analógica representa un parámetro medio que evita llegar a extremos y aprovecha las ventajas de ambas hermenéuticas.

Velázquez y Nava (2014) establecen que la construcción de la hermenéutica analógica comienza con preguntas interpretativas ¿Qué me dice esto? ¿qué quiere decir? ¿qué dice ahora? Por tanto, en esta investigación en cuestión se hizo uso de la pregunta Hermenéutica-Analógica: ¿De qué manera los factores críticos de éxito inciden con la Gestion de seguridad de la información?, lo que ayudó a generar un constructo explicativo para esta investigación en cuestión.

Por consiguiente, la Hermenéutica-Analógica presenta ventajas con respecto a la interpretación aplicada en las entrevistas enfocadas en la gestión de seguridad de la información en la Universidad de Guanajuato, ya que estableció un límite para no considerar que todo lo dicho por informantes claves representaba la verdad y adquirió el punto de vista propio para poder segmentar aquella información sobresaliente que explicaba los objetivos propuestos en esta investigación.

CAPÍTULO 5.
RESULTADOS

Resultados

En este capítulo se presenta los resultados obtenidos de este estudio, los cuales están enfocados en los objetivos planteados al inicio de esta tesis, y éstos recaen en el análisis de la aplicación de las entrevistas semiestructuradas aplicadas a los diversos informantes claves. El análisis e interpretación de los resultados se realizó en base a la teoría del análisis cualitativo, a partir del método de la hermenéutica analógica, es decir, haciendo un proceso de conocimiento de las realidades percibidas por los sujetos entrevistados; para discriminar sus componentes, establecer sus relaciones y sintetizar los elementos.

Las entrevistas en un primer momento fueron grabadas, transcritas y convertidas en forma de textos, este es llamado el documento primario. Los textos están interpretados con el programa ATLAS Ti V 8.2 por partes, a códigos y citas. Las citas que observarán en seguida son segmentos del documento primario que es considerado importante para analizar los resultados. Los códigos son clasificaciones de diferentes niveles de abstracciones para crear grupos de diferentes recortes de información, son piezas de texto que hacen referencia a otro y están clasificados en grandes números de unidades textuales. En seguida los códigos están agrupados en familias para formar un racimo de entidades, para comprender más fácil la información. Luego observarán las redes que muestran una estructura que trabaja con conjuntos de elementos y se establecen relaciones semánticas entre estos elementos y casi todos están conectados en una red.

Nube de palabras

Entonces, como resultado del proceso de análisis de las entrevistas con ayuda del software Atlas Ti V 8.2, mediante un análisis de contenido que permitió identificar, organizar y analizar la información obtenida a través de la lectura de las entrevistas se realizó una cuantificación de los datos mediante la medición de la frecuencia de códigos, en este caso el principal propósito de codificación es realizar conexiones entre las diferentes partes de la información.

Figura 14. Nube de palabras a partir de la codificación de entrevistas.

Estos códigos representan un segmento o elemento básico de información que se puede considerar como significativa en relación con el tema bajo estudio, así mismo, en este caso Atlas Ti permite generar esta nube de palabras (en este caso códigos) en donde muestra la frecuencia con la que fueron mencionados por los participantes y los códigos que están relacionados con los indicadores usados en esta investigación. Como se puede observar el código más mencionado está relacionado con la cultura organización de seguridad de la información, seguido de los procesos, la alineación institucional y el rendimiento de la gestión de seguridad de la información, entonces la frecuencia de mención de estos nos indica como la realidad se ve reflejada en el caso de estudio. Finalmente, las metas y el presupuesto son los factores menos mencionados en nuestro caso.

A continuación, se indican los hallazgos en cada una de las dimensiones establecidas en el instrumento relacionados con los factores críticos de éxito del modelo de Tu, Yuan, Archer, y Connelly (2018).

Conciencia organizacional

La conciencia organizacional está definida por los códigos y algunas de las citas determinadas son mencionadas a continuación.

- **Conceptos básicos**

"… la seguridad de la información es el conjunto de medidas preventivas y reactivas que buscan mantener la confidencialidad integridad y disponibilidad de la información".

"… seguridad de la información, es más relacionado a los temas o cómo decirlo, si los temas o la información como tal y como acción contra palabras que se maneja de alguna persona o institución no sé cómo información personal".

"… algunos protocolos que se usan para, proteger la información de cualquier cosa información de una persona o un equipo o de cualquier proceso también".

- **Cultura organizacional de seguridad de la información**

"… los ejecutivos entonces ellos a veces no tienen el conocimiento para poder identificar ese tipo de incidentes. Entonces puede llegar un correo malicioso o le dan un clic se infecta su computadora con malware. Y de su computadora pues puede infectar se lleva además dispositivos que están en la red".

"… el correo electrónico en ocasiones pues es complicado porque a veces depende mucho de la cultura que tienen las personas. Entonces si no tienen unas buenas bases de conocimiento de seguridad pues caen en cualquier correo falso ven el logo de la Universidad que en realidad no es de la Universidad".

"… los factores que impactan en que sea efectivo las medidas de seguridad pues como primero como la cultura sino como falta de información de los usuarios es lo que nos impacta".

"… pues ahí sería el factor humano es el que más impacta. Aunque tengamos los equipos más seguros. Las computadoras más seguras los sistemas más seguros. Si el usuario que no tiene no tiene una cultura de informática sobre seguridad este por lo menos las bases. Si le llega un correo que dice que es de la Universidad, pero ni siquiera verifica que venga del dominio y le dan clic pues todo nuestro trabajo este digamos que no tiene razón de ser porque el usuario le dio clic".

- **Políticas**

"…actualmente no tenemos una política sólo tenemos lineamientos normativos, pero no hay una política en sí que que, nos que nos apoye o nos ayude a tomar medidas o un poquito más más mm predecirse o más firmes o más este. Que tengan una responsabilidad un poquito mayorcon los usuarios o sea sólo podemos hasta este punto nada más que hacerles recomendaciones".

"… la política actual, no contamos con políticas creo".

"… no es como de esta política es para esta cosa no sé si alguien intentó robar tus datos aquí vamos a aplicar esto no no aquí es muy global".

"…en este informe les compartimos los hallazgos y las recomendaciones y los riesgos que pueden tener siendo los parches y estos se los compartimos a los dueños o administradores de los sistemas, pero como final de cuentas son recomendaciones nosotros no podemos obligarlos a que debido a que no tenemos políticas no podemos obligarlos a que los cumplan".

- **Procesos**

"…sí tenemos, aunque no tenemos totalmente documentado todo, pero sí tenemos algunos procesos para que la disponibilidad para que la infraestructura y el servicio de internet y de red esté lo más disponible".

"…los procesos ahorita nos encontramos este formalizando o digamos analizando todos los procesos. Este realmente ahorita tenemos pocos este los demás no los realizamos, pero no los tenemos documentados. Por ejemplo, uno relacionado con la seguridad de la infraestructura de red ataques que tenemos directamente a nuestro servicio de internet que es en conjunto con el proveedor de Internet. Sí seria digamos un procedimiento otro procedimiento que tenemos también documentado. Va relacionado con los ataques de ataques con relacionados con correo electrónico todas las medidas que tenemos que tomar en diferentes plataformas dependiendo el incidente".

"… que este haya una un proceso de aseguramiento la información sea más eficiente e involucra muchas áreas no sólo al área tecnológica".

"… este realmente ahorita tenemos pocos este los demás los realizamos, pero no los tenemos documentados".

"… así nos faltan muchos procesos en cuanto seguridad en información".

- **Incidentes de seguridad**

"… los más importantes o los más críticos diría yo serían los incidentes con el correo electrónico incidentes de phishing estafas de correo electrónico. Mm Facturas falsas correos adjuntos falsos. Estos son los que los que tenemos más incidentes registrados hay ataques a la Red las 24 horas también todo el tiempo, pero ahí los equipos de seguridad perimetral nos ayudan en este caso".

"… el correo electrónico en ocasiones pues es complicado porque a veces depende mucho de la cultura que tienen las personas, entonces si no tienen unas buenas bases de conocimiento de seguridad pues caen en cualquier correo falso ven el logo de la Universidad que en realidad no es de la Universidad".

"…yo creo que es en cuanto a la información. Lo que más pega es precisamente lo que te comentaba al inicio del usuario y lo que más pega son los correos electrónicos".

"…los que más se presentan son los de spam.o phishing, por a través del correo electrónico. Y pues rara vez de malware, es lo que más tenemos aquí".

En las citas se encontraron distintas expresiones para decir qué es la seguridad de la información: como proteger con medidas o protocolos la información. Resaltando elementos como son la confidencialidad integridad y disponibilidad de la información, que son principios básicos en el tema de seguridad de la información.

La cultura organizacional en seguridad de la información es la dimensión que fue la más mencionada, con base en el análisis de la nube de palabras mostrada anteriormente, la cultura

organizacional es definida por nuestros diferentes participantes como la conducta que tiene el usuario ante el manejo de la información, también nos mencionan el comportamiento del usuario ante un incidente y en su mayoría estos no saben como manejar estas situaciones, haciendo más vulnerable la información que manejan.

Al mencionar las políticas y describir esta dimensión los participantes nos indican como esta es inexistente dentro de la institución, además que la relacionan directamente con la falta de cultura en seguridad de la información dentro de la misma, y como es que esta inexistencia afecta el apoyo de los usuarios y aumenta las vulnerabilidades existentes.

Los procesos al igual que las políticas son vistos casi inexistentes de manera formal dentro de la institución, los participantes los describen como una forma intuitiva de trabajar y no como procesos establecidos dentro de un manual institucional. Además, nos mencionan reiteradamente la falta de formalización de los procesos del área.

En los incidentes de seguridad mencionados se observó la relación directa con la cultura organizacional, siendo los incidentes citados muy relacionados con el manejo de correos electrónicos por parte de los usuarios.

Alineación institucional

Como se mencionó anteriormente la alineación es un factor relevante para una gestión de seguridad exitosa, los códigos y citas que muestran las características de la alineación institucional son:

- **Alineación institucional**

> "…este, desde mi punto de vista sería mantener un gobierno de tecnologías de información. Esto con la finalidad de tener líneas estratégicas para, porque la seguridad de la información no sólo es el área de tecnologías sino conlleva todas las áreas administrativas y tiene que haber un control este y un una área que se encargue de coordinar todo para que este haya una un proceso de aseguramiento la información sea más eficiente e involucra muchas áreas no sólo al área tecnológica".

"… involucra al área financiera, el área de Recursos Humanos es prácticamente todo hasta la secretaria y la que hace la limpieza".

"… no todas las instituciones tienen un área de seguridad y monitoreo tanto en infraestructura como información".

"… cada área tiene su equipo tanto de desarrollo como de soporte a la información y realmente no sé muy bien como manejen ellos y nosotros no podemos como apoyarlos hasta cierto punto debido a la falta de políticas, pero podemos orientarlos nada más a darles un pequeño empujoncito ".

"… este mm no. No considero que es suficiente, este digamos ahorita la seguridad está enfocada nada más en la parte de tecnologías. Bueno, todos piensan eso igual, pero rápidamente en el proceso de aseguramiento es un proceso permanente entonces sí involucra a todas las áreas. Entonces no es suficiente, necesitamos involucrar a las áreas administrativas".

Metas

"…si tenemos este, este uno de ellos van enfocados hacia las plataformas donde se administra la información. Por ejemplo, intra UG plataformas de recursos humanos para digamos este fortalecerlos las aplicaciones y adicionalmente protegerlas con un Firewall de aplicaciones web esto es para incidentes o incidentes relacionados desde dentro de la red de la universidad y fuera de la red que serían por ejemplo inyecciones de SQL, defacement, ataques contra cross scripting".

"… vamos acomodando todas las actividades y proyectos fuertes para los que formamos parte de la coordinación de seguridad y monitoreo".

"… dependiendo de las capacidades de cada una, pero así como yo tengo ese proyecto mis otras dos compañeras que están ahí también tienen proyectos individuales por así decirlo de alguna forma individuales porque como quiera todas colaboramos uno con otro".

El código alineación institucional descrito mediante las diferentes citas nos muestra como característica esencial la participación de todos los niveles de la organización, pero también observamos la falta de participación de otros en los temas de seguridad dentro de la institución, de forma positiva se observa la existencia de una parte especializada dentro del organigrama, aunque la distribución de las áreas dentro del organigrama institucional indica que no existe una comunicación efectiva entre las partes. Podemos observar, que los participantes también nos mencionan la relación de esta dimensión con las políticas institucionales.

Las citas del código metas, nos muestra de forma positiva como las metas de los proyectos por parte de los participantes si han sido definidos en cada una de sus partes, dando así una guía de las metas a seguir.

Apoyo de la alta dirección

Los códigos y algunas de las citas que muestran las características del apoyo de la alta dirección son:

- **Políticas**

> "…pero a lo que sé me parece que no, debido a que es de las políticas aquí como somos una institución de gobierno ni institución grande este en parte Gobierno. Las políticas se manejan de forma muy global, no es como de esta política es para esta cosa no sé si alguien intentó robar tus datos aquí vamos a aplicar esto no no aquí es muy global".

> "… en cuanto a políticas y todo eso. De hecho, entré en temporada de auditoría, en cuanto a políticas creo que no se tocó ningún punto con que no estoy segura no se tocó ningún punto en cuanto a políticas y solamente tenemos, así como bien visualizado cuál es nuestra misión cuál es nuestra visión, pero políticas así que tú digas están escritas aquí no".

- **Alta dirección**

"…yo considero que posiblemente todavía falta un poco de madurez en la parte de alta gerencia donde ahorita la ciberseguridad es un tema en auge que apenas ahorita están volteando a ver esta parte. Entonces ahorita tenemos un poco de esperanzas para que se fortalezca esto un poco, pero sí falta un poco de madurez de parte de la alta gerencia".

"…no, no participan. Solo, sólo lo desarrolla ahorita meramente la Dirección de Tecnologías nada más pero ahorita no están participando en esa toma de decisiones, para priorizar los proyectos".

"…en los temas de auge que es la ciberseguridad ya un poquito la alta dirección está volteando para acá entonces estamos empujando un poquito para que sea área madure un poquito más y tomen un poquito más importancia al área de seguridad".

"… no, no participan. solo, sólo lo desarrolla ahorita meramente la Dirección de Tecnologías".

- **Presupuesto**

"… presupuestos normalmente lo ven como entre jefes y coordinadores".

"… sí claro cada año se tiene se hace un presupuesto este tanto para la renovación de la infraestructura actual como para ampliar y mejorar con nuevas herramientas este la seguridad y eficientar tanto las actividades operativas del personal como el área de las actividades preventivas para que no pasen incidentes o detectarlos a tiempo y reducir el riesgo".

".. sí si hay un presupuesto hasta donde yo sé por qué existe un contador para nuestra área de seguridad y infraestructura de red".

"… nada más es como ir con el proveedor darles tu propuesta y pedir lo que se quiere. Cuando es una cantidad mayor pues si tienen el producto de tantos proveedores tienen que y tienen que competir y el que gane pasa".

El código políticas también es parte de la dimensión apoyo de la dirección ya que estas se relación entre sí, nuevamente observamos la inexistencia de estas y como una alta dirección no ha implementado ninguna política en seguridad de la información como parte de la visión y misión de la dirección de tecnologías, ni de la institución en sí.

El código alta dirección nos muestra como sus participantes ven la falta de apoyo en temas de seguridad de la información por parte de sus superiores en el organigrama y como esto ha afectado la implementación en medidas de seguridad de la información.

Al mencionar el presupuesto se ve una dirección positiva, ya que se muestra que existe un presupuesto para cada una de las herramientas necesarias además de que se mantienen actualizados.

Controles y herramientas de seguridad

Los siguientes códigos y citas nos describen los controles y las herramientas de seguridad dentro de la Universidad:

- **Herramientas y controles**

"… hasta ahorita lo que tenemos es nuestra seguridad perimetral de hardware".

"… en las herramientas de seguridad de la información pues sería el juego de aplicaciones web. Las otras herramientas serían los procesos de respaldo en cuestión de infraestructura de red tenemos este ids que son sistemas detectores de intrusos. Tenemos un firewall y un IPS que es un sistema de protección contra intrusos".

"…adicionalmente protegerlas con un Firewall de aplicaciones web esto es para incidentes o incidentes relacionados desde dentro de la red de la universidad".

- **Formación**

"…hemos tenido cursos y como que ahorita poco a poco cada quien cada área se está alineando un poco a tomar esa metodología, pero no se está siguiendo no se está usando como una metodología rigurosa sólo se usa como referencia".

"…por parte de la institución digamos no bueno directamente externos sí o sea personal externo que contrata la universidad para que nos dé capacitación o por medio de los diplomados que contrata la universidad".

"… estos temas de la seguridad es un área muy grande cuatro personas es muy poco para poder tenemos que tener especialistas en aplicaciones web especialistas en redes inalámbricas especialistas en análisis de tráfico especialistas en respuesta a incidentes entonces este tenemos una parte de todo pero a veces la operación no te permite enfocarte en un área específica".

- **Estándares**

"… ahorita no aplicamos ninguno usamos como referencia COBIT para la parte de seguridad y usamos ITIL para la parte de los servicios, aunque no es un marco de referencia más bien es si es un marco de referencia, pero no de seguridad completamente, pero sí involucra ayuda a analizar los procesos".

".. seguridad seguridad no está muy soportado bajo bajo ninguna ISO ni nada de eso".

".. es de la mayoría si así tenemos no escrito ni nada de eso, pero sé que si pasa esto ya sé que hacer, si lo tenemos ya en la cabeza, pero no registrado".

Las citas del código herramientas y controles, nos muestran algunas de las herramientas implementadas en el área de seguridad de la información, observamos de manera positiva el manejo de estas y su implementación por parte de los expertos del área.

Observamos con base en las citas del código formación, de forma positiva que los expertos en del área son capacitados de forma externa por entidades especializadas, pero también vemos la parte negativa de que a pesar de tener expertos en el área el resto de los usuarios no tienen la formación básica en temas de seguridad de la información siendo así para el área el eslabón más vulnerable para la protección de la información.

El código estándares nos indica que se conocen los diferentes estándares que se pueden implementar dentro del área de seguridad de la información, sin embargo, no son implementadas de manera precisa y actualmente no se tiene ningún tipo de certificación.

Rendimiento de gestión de seguridad de la información

- **Rendimiento GSI**

"… no no no se presentan informes sólo se presentaron informes cuando hay un incidente este crítico".

"… estos temas de la seguridad es un área muy grande cuatro personas es muy poco para poder tenemos que tener especialistas en aplicaciones web especialistas en redes inalámbricas especialistas en análisis de tráfico especialistas en respuesta a incidentes entonces este tenemos una parte de todo pero a veces la operación no te permite enfocarte en un área específica".

"… en general los proyectos se sacan dependiendo de la necesidad o sea en caso de que se ocupe algo se solicita".

- **Valores**

"… el trabajo en equipo es el principal".

"… el trabajo en equipo en la parte de respuesta a incidentes entre mejor colaboración hay entre las áreas es más rápido".

"… la honestidad o la ética porque a veces tenemos acceso a información confidencial y tienes que tener tienes que manejarla de la forma adecuada".

"… sobre todo trabajo en equipo. Tenemos que trabajar mucho en equipo".

Al observar las citas del código rendimiento de GSI nos define que la gestión en seguridad de la información no esta formalizada ya que no hay informes establecidos de forma periódica ni se tienen proyectos determinados en el tiempo, y se van determinando solo de

forma reactiva y no preventiva, además que nos indican la falta de puestos para mejora en los procesos.

El código valores, nos define por parte de los participantes de forma positiva los valores que se aplican dentro del área nos mencionan como principales: trabajo en equipo, honestidad y ética.

Red de gestión de seguridad de la información

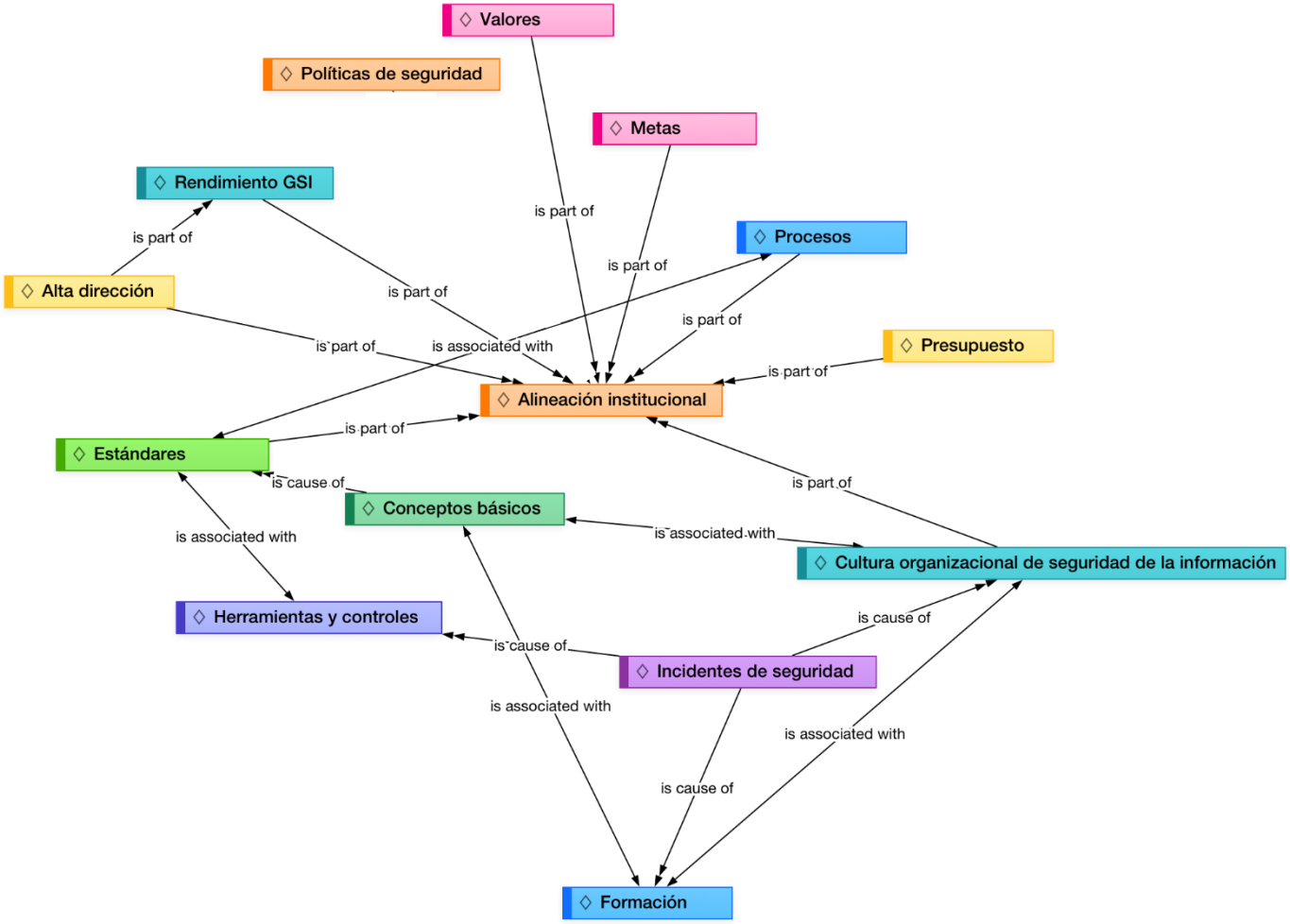


Figura 15. Red de Gestion de Seguridad de la Información.

En esta red se establecieron relaciones entre los códigos encontrados en el análisis de gestión de seguridad de la información en la Universidad de Guanajuato y como cada uno está interconectado. La Alineación institucional funciona como un núcleo ya que el resto de los códigos giran alrededor de este o se relacionan directamente.

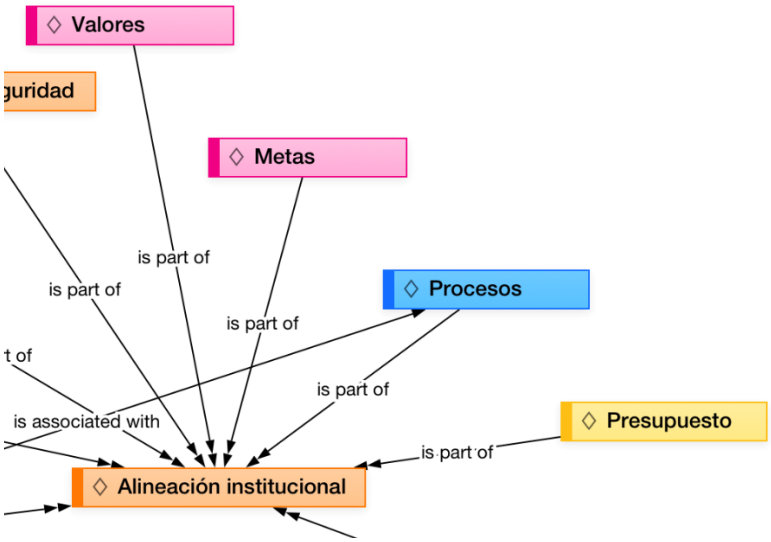


Figura 16. Códigos asociados al código Valores.

Los Valores son parte positiva de la Alineación institucional ya que son parte de la cultura y estos están descritos en cada uno de sus manuales dentro de las diferentes áreas de la universidad y que son implementados por los participantes. De la misma forma positiva se integran las Metas relacionadas con la seguridad de la información que se establecen periódicamente dentro de la institución y se encuentran alineadas a las metas institucionales.

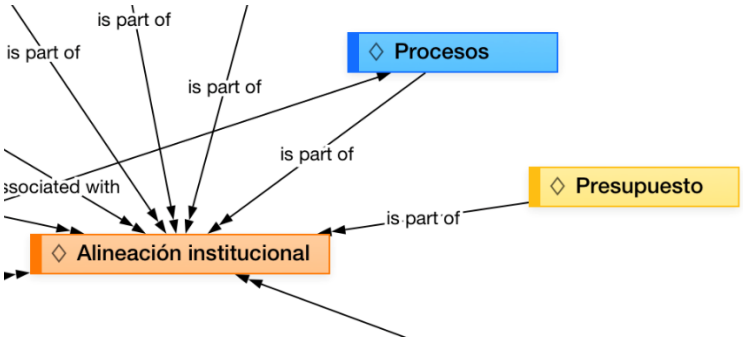


Figura 17. Códigos asociados al código Procesos.

Los Procesos están asociados con los Estándares en seguridad de la información ya que en este caso un estándar establece las herramientas y fases que hay que realizar para ejercer una seguridad de la información efectiva al mismo tiempo que el Estándar debe estar alineado a la institución de forma positiva. El Presupuesto también es parte de la Alineación institucional, ya que esté se establece con base a los objetivos de la institución.

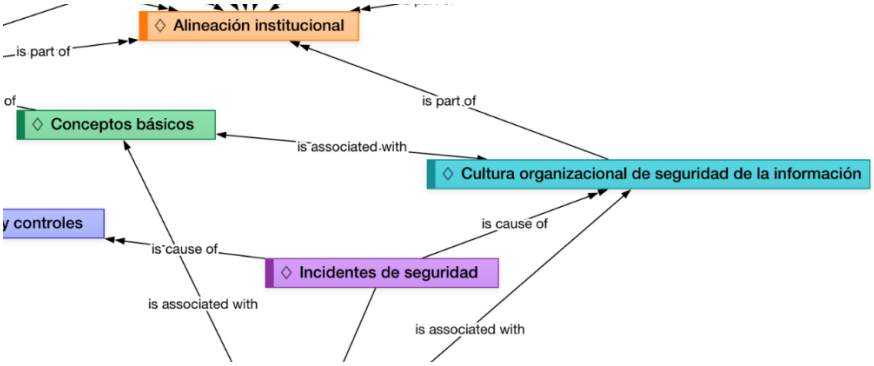


Figura 18. Códigos asociados al código Cultura de seguridad de la información.

Por su parte la Cultura de seguridad de la información es parte de la Alineación institucional ya que se forma de la cultura institucional, como parte de los conceptos básicos que deben tener los usuarios y empleados de la institución, los cuales emprenden de los Estándares en seguridad de la información, y la Formación está directamente relacionada con los Conceptos básicos en seguridad de la información y la Cultura organizacional de seguridad de la información, pero entonces los Incidentes de seguridad son ahora causa de la Cultura institucional en seguridad de la información, de la Formación y las Herramientas y controles implementados.

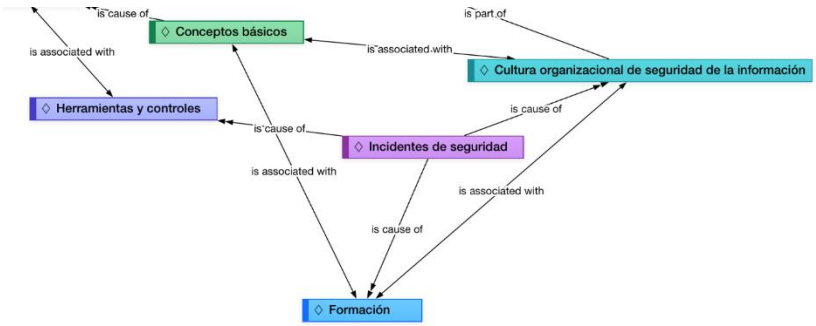


Figura 19. Códigos asociados al código Herramientas y controles.

Las Herramientas y controles están directamente relacionados con los Estándares en seguridad de la información. El Rendimiento de la GSI forma parte de la Alta dirección ya que esta gestión depende directamente de los altos mandos de la institución, de la misma manera esta debe estar alineada a la institución.

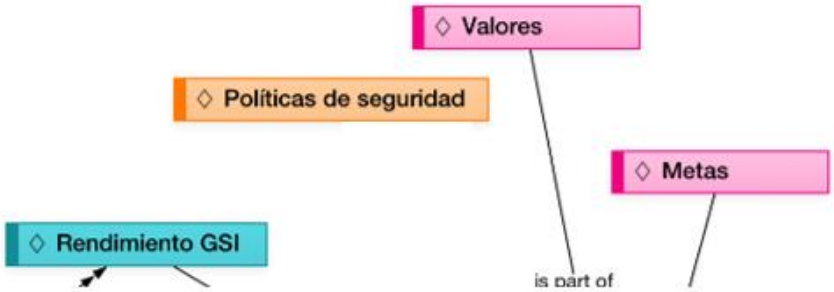


Figura 20. Códigos asociados al código Políticas de seguridad.

Finalmente, es evidente que las Políticas en gestión de seguridad de la información no se encuentran relacionadas ya que son inexistente en la actualidad dentro de la institución.

CAPÍTULO 6.
CONCLUSIONES

CONCLUSIONES

Posterior a la revisión del marco teórico y de los resultados del instrumento de la presente investigación, se describen las siguientes conclusiones de la presente tesis.

Comenzamos con el uso propio de una seguridad de la información que toma en cuenta los procesos, procedimientos, el personal y la tecnología que son los encargados o implicados de proteger los activos de información en cualquier organización o institución. Seguido de este otro concepto relacionado que es la gestión de seguridad de la información el cual usamos como un proceso de administración de las personas, las políticas y programas con el objetivo de asegurar la continuidad de las operaciones esto mientras se mantiene la alineación estratégica con la misión de la institución. Estos conceptos fueron básicos para el presente estudio ya que sin estas definiciones podríamos haber caído en una seguridad de la información meramente técnica u operativa.

Los datos arrojados muestran una perspectiva de la importancia de la seguridad de la información en la actualidad. Se destacan tendencias similares en diferentes empresas incluso las pequeñas empresas, que antes tenían poco interés, ahora son parte de los incidentes implicados en seguridad de la información. Latinoamérica tiene una tendencia al alza hacia el uso de internet, por lo cual es necesario estar preparados para un entorno más grande y con mayores riesgos. El conocimiento de estos datos muestra la brecha que existe dentro de la IES en cuanto a la implementación de buenas prácticas en seguridad de la información.

Como caso de estudio y de aplicación se seleccionó a la Universidad de Guanajuato, porque representa la principal IES del Estado de Guanajuato, la cual se ha visto inmersa en diferentes procesos de reformas administrativas en su vida como institución. Asimismo, la Universidad tiene una infraestructura y de equipamiento significativo y se ha preocupado por mantener una participación con la sociedad a través de la transparencia de la información.

Ahora bien, se pudo apreciar que la metodología utilizada para llevar a cabo este trabajo representa una técnica que implica un diagnóstico, es decir, el investigador deseó conocer la problemática, para analizar y retroalimentar los descubrimientos obtenidos, estuvo enfocada

en lo cualitativo, lo cual ayudó para comprender aquellas experiencias e ideas que tienen las personas en la Universidad de Guanajuato, por consiguiente, se ha incorporado la teoría y la práctica organizacional.

Se pudieron lograr los objetivos particulares plateados en esta investigación, lo que ayudó a detectar las problemáticas que presenta la gestión de seguridad de la información dentro de la institución. En primera instancia, el conocer los Factores Críticos de Éxito de la Gestión de Seguridad de la Información, se detectó a través de la búsqueda teórica que nos habla de los factores críticos de éxito siendo nuestro modelo guía el desarrollado por Tu, Yuan, Archer y Connelly (2018), de cómo los Factores críticos de éxito contribuyen a la Gestion de seguridad de la información de la organización desde una perspectiva de alineación y valor estratégico, ya que este nos muestra una dinámica clara de las dimensiones que lo integran, así como ser un modelo de factores críticos de éxito global que se desarrolló y validó empíricamente en el campo de la Gestion de seguridad de la información.

Con respecto al siguiente objetivo particular, analizar e identificar los elementos clave de la gestión de seguridad de la información actualmente implementados en la Universidad de Guanajuato, se detectó que, sí existen factores implementados por la institución, aunque existen puntos negativos y positivos en su implementación. Se detectó que la cultura organizacional en seguridad de la información representa uno de los factores primordiales ya que los individuos de la Universidad de Guanajuato aún no tienen una visión de la seguridad de la información, es decir, la ven como parte de las tecnologías y solo como una herramienta de operatividad y no se sensibilizan en que éstas proporcionaran un flujo que favorecerá a la organización. Observamos como la cultura en seguridad de la información es un factor importante, aunque negativamente aún no se encuentra adaptado en los usuarios.

Por ello, la cultura organizacional vista desde la parte de la gestión es un punto primordial para que se tenga una dinámica que auxilie a que fluyan las estrategias y sean implementadas más fácil y rápidamente. El problema recae en que aún no existen acuerdos entre departamentos para establecer un mismo contexto de los objetivos, lo que provoca que se obstruya la comunicación, debido a que no se retroalimenta y eso hace deficiente la gestión, así como los pocos procesos ya establecidos.

Además, otra situación que recae de lo anterior es que no hay un total de procesos entre departamentos, lo cual es importante implantarlos, puesto que, al no existir, no se pueden implementar las estrategias necesarias. Pero esto se debe a que los usuarios no cuentan con una cultura enfocada en la Gestión de seguridad de la información y por ello no se puede crear un sistema integral que conjunte la información (procesos) de cada departamento, lo que ocasiona que la información este fragmenta. Por ello, se debe ver a los procesos como actividades que no pueden ser aisladas, ya que es lo que permitirá tener una comunicación eficaz entre departamentos y usuarios.

El establecer procesos dentro del desarrollo de cualquier organización, sobre todo en las Universidades se vuelve el instrumento más importante que apoya a la dirección, para poder administrar y planear de manera estratégica. En este sentido, no basta con contener una infraestructura tecnológica si esta no será utilizada a su máximo potencial, por eso se debe desarrollar una cultura de seguridad de la información que comprenda y esté dispuesta a tener un enfoque estratégico.

La inexistencia de políticas institucionales en seguridad de la información es otro factor significativo dentro de la Universidad, ya que sin la formulación y aplicación de estas es difícil alcanzar y tener establecidas las responsabilidades y objetivos en materia de seguridad de la información, también nos permiten adoptar y al mismo tiempo adaptar a las necesidades propias de la institución las mejores prácticas de seguridad de la información, funcionando estas como un marco normativo siempre en función de la alineación estratégica dentro de la institución.

Igualmente, los resultados que se encontraron proceden a dar indicios al tercer objetivo particular el cual consiste en desarrollar estrategias para la gestión de seguridad de la información en la Universidad de Guanajuato. Se detectó que la planificación de seguridad de la información no es relevante, y por lo tanto no se considera dentro de la planificación organizacional, lo que origina poca efectividad al momento de realizar la incorporación de herramientas TIC en la Universidad. En este sentido, la Universidad de Guanajuato, debe desarrollar capacidades en el ámbito de seguridad de la información, que respondan a las nuevas demandas y que les apoye a la alineación institucional. Por eso, es importante que se

establezca un plan estratégico de seguridad de la información, donde estén las pautas para alcanzar los objetivos institucionales.

Debido a lo anterior, se debe establecer una estrategia de seguridad de la información que se adapte a las necesidades de la Institución, pero que esté regida bajo la influencia de las diferentes metodologías existentes como podría ser el caso de ISO 27001, para que de esta forma ayude a la institución a mejorar su gestión de seguridad de la información desde altos mandos en primera instancia y después hacia las diferentes áreas que integran a la Universidad. Sin embargo, como ya se mencionó, la sensibilización de la cultura en seguridad de la información hacia una visión estratégica de seguridad representa un factor clave para el desempeño en la Universidad y no sólo de ella sino de cualquier organización (pública o privada), por ello es indispensable aumentar la conciencia en los líderes de las diferentes áreas de la institución sobre los riesgos existentes y los cuidados que deben tener con la información que custodian.

Como resultado del diagnóstico de la situación de gestión de seguridad de la información y derivado de los instrumentos de investigación utilizados podemos confirmar el supuesto uno:

> *La alineación institucional contribuye a una mayor conciencia de los riesgos y controles de seguridad de la información.*

Nuestro estudio muestra que la alineación institucional tiene un significativo impacto en tres factores: conciencia de la organización, apoyo de la dirección y control de seguridad, esto concuerda con la revisión de la literatura que la conciencia del personal, la formación y el apoyo de la dirección se encuentran para ser los factores más importantes en la determinación del éxito en implementación de la Gestion de seguridad de la información y la importancia de los diferentes factores. El supuesto dos también se confirma:

> *El soporte de los altos directivos influye en el desempeño de la gestión de seguridad de la información.*

El estudio también proporciona evidencia empírica de que los factores humanos son más importantes que controles de seguridad para el éxito organizacional de la Gestion de

seguridad de la información. En comparación con la parte superior el apoyo de la alta dirección contribuye al éxito de la Gestion de seguridad de la información, ya que, sin el apoyo de ambos la dirección y los empleados, las medidas de seguridad, incluso perfectamente desarrolladas no pueden implementarse o realizarse correctamente.

Entonces al señalar que para la Gestión de seguridad de la información es importante la alineación estratégica, tomamos en cuenta las estrategias de SI frente a las necesidades institucionales, sin dejar de alinear los objetivos mutuos. Con esto se vinculan los proyectos generales de la institución con los específicos relacionados con la seguridad de la información y así obtener una relación positiva. Siguiendo la misma lógica en el contexto de Gestión de SI cuando la estrategia de seguridad de la información está alineada con la estrategia institucional, entonces damos más soporte organizativo a la Gestión de SI y se mejora el nivel operativo, tomando en cuenta la conciencia organizacional de seguridad de la información y los controles de seguridad que pueden ser mejor aprovechados y finalmente la Gestión de seguridad de la información será más exitosa.

Por otra parte, las limitaciones que se tuvieron en el desarrollo de este trabajo fueron las siguientes:

- La seguridad de la información en este tipo de instituciones es todavía un tema poco estudiado e implementado, por lo que consideramos importante conocer sobre la situación actual de esta disciplina en las IES para poder aportar estrategias que les pueden servir para mejorar su Gestión en seguridad de la información que se relaciona a la institución, así como aumentar su cultura organizacional en seguridad de la información.
- El número limitado de estudios de Gestión de seguridad de la información aplicado a las organizaciones en México dificultó conocer más sobre la situación, las herramientas o metodología que se utilizan en las instituciones de otras entidades federativas y posteriormente realizar estudios comparativos para llegar a un conocimiento más profundo del tema.

- El tiempo limitado para la realización de la investigación dificultó conocer más a fondo casos particulares de la aplicación de estrategias de gestión de seguridad de la información en IES.
- La falta de aplicación de propuestas derivadas de esta investigación para poder medir el impacto que pudieran tener la implementación de la alineación de estrategias de seguridad de la información.

Como futuras líneas de investigación se espera:

- Realizar un enfoque más cuantitativo que determine la incidencia que tiene la gestión de seguridad de la información con un enfoque estratégico dentro de las instituciones educativas de nivel superior.
- Replicar el estudio en otra IES con el objetivo de realizar estudios comparativos.
- Profundizar en el conocimiento del tema.

REFERENCIAS

Ahimbisibwe, A., Daellenbach, U. y Cavana, R. Y. (2017). Empirical Comparison of Traditional Plan-Based y Agile Methodologies: Critical Success Factors for Outsourced Software Development Projectsfrom Vendors Perspective. *Journal of Enterprise Information Management*, 30 (3), 400-453.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, 26(4), 276-289.

Albrechtsen, E., y Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers y Security*, 28(6), 476-490.

Alcalá M., D. (2011). La hermenéutica Analógica como el límite de la interpretación. En N. Conde Gaxiola, *Hermenéutica, Analogía y Scociedad* (41-54). México: Torres Asociados.

Ashenden, D. (2008). Information Security management: A human challenge?. *Information security technical report,* 13(4), 195-201.

Baker, W. H., y Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy*, 5(1), 36-44

Banerjee, A., Dolado, J., y Mestre, R. (1998). Error-correction mechanism tests for cointegration in a single-equation framework. *Journal of time series analysis*, 19(3), 267-283.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys*, 25(4), 375-414.

BBC Mundo. (15 mayo 2018). *México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias*. Recuperado de https://www.bbc.com/mundo/noticias-america-latina-44130887

Beautement, A., Becker, I., Parkin, S., Krol, K., y Sasse, A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. In Twelfth Symposium on Usable Privacy and Security,253-270.

Beuchot, M. (2015). Elementos esenciales de una hermenéutica analógica. *Diánoia, 60* (74), 127-145.

Boockholdt, J. L. (1989). Implementing security and integrity in micro-mainframe networks. MIS Quarterly, 135-144.

Bremser, W. G. y Chung, Q. (2005). A Framework for Performance Measurement in the EBusiness Environment, Electronic Commerce Research and Application, 4, 395-412.

British Standards Institution. (1995). BSI catalogue. BSI Standards.

BS7799-1. (1999). Code of Practice for Information Security Management, Department of Trade and Industry.

Cazemier, J. A., Overbeek, P. L., y Peters, L. M. (2000). Security Management (IT Infrastructure Library Series). Stationery Office, UK.

Chang, S. E., Chen, S.-Y. y Chen, C.-Y. (2011). Exploring the Relationships between It Capabilities and Information Security Management. *International Journal of Technology Management*, 54 (2/3), 147-166.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014), Defining cybersecurity, *Technology Innovation Management Review*, 4 (10), 13-21.

Culnan, M. J., Foxman, E. R. y Ray, A. W. (2008). Why It Executives Should Help Employees Secure Their Home Computers. *MIS Quarterly Executive*, 7 (1), 49-56.

Cumps, B., Martens, D., De Backer, M., Haesen, R., Viaene, S., Dedene, G., Baesens, B. y Snoeck, M. (2009). Inferring Comprehensible Business/Ict Alignment Rules. *Information y Management*,46 (2), 116-124.

Davies, T. (2002). The 'Real' Success Factors on Projects, International Journal of Project Management, 20(3), 185-190.

Dhillon, G. y Backhouse, J. (2001). Current Directions in Is Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*. 11(2), 127-153.

Dhillon, G., y Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.

Doherty, N. F. y Fulford, H. (2006). Aligning the Information Security Policy with the Strategic Information Systems Plan. *Computers & Security*, 25 (1), 55-63.

Douglas, M., y Wildavsky, A. (1982). How can we know the risks we face? Why risk selection is a social process. *Risk analysis*, 2(2), 49-58.

Eccles, P. (1993). Planning for Improved Performance. *Management Accounting*. 53-54.

Erkan, K. (2005). *Evaluating It Security Performance with Quantifiable Metrics*, Recuperado de:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.4000&rep=rep1&type=pdf

ESET Security Report Latinoamérica (2017). Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Ferguson C. y Roger D. (1982). Critical Success Factors for Directors in the Eighties. *Business Horizons*, 14-18.

Foro económico mundial (2012). Global Risks Archivo. [online] disponible en: http://reports.weforum.org/global-risks-2012 /

Galindo C. (1998). Técnicas de investigación en sociedad, cultura y comunicación. México: Pearson Education

Gattiker, U. E., y Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information systems research*, 10(3), 233-254.

Gerow, J. E., Grover, V., Thatcher, J. y Roth, P. L. (2014). Looking toward the Future of It-Business Strategic Alignment through the Past: A Meta-Analysis. *MIS Quarterly*, 38 (4), 1159-1185.

Villegas, G. (1995). Gestión por factores críticos de éxito. *Revista Universidad Eafit, 9*.

Grupo del Banco Mundial. Indicadores de desarrollo mundial. *Publicaciones del Banco Mundial*. Recuperado de: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2016&locations=GW-VE&name_desc=true&start=1990&view=chart

Gupta, M., Charturvedi, A.R., Metha, S. y Valeri, L. (2001). The experimental analysis of information security management issues for online financial services, ICIS 2000, 667-75.

Hagen, J.M. y Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, 17 (5), 388-407.

Hagen, M. J., Albrechtsen, E. y Hovden, J. (2008). Implementation and Effectiveness of Organizational Information Security Measures. *Information Management & Computer Security*, 16 (4), 377-397.

Harrington, H. J., y Harrington, J. S. (1996). Administración total del mejoramiento continuo: la nueva generación. McGraw-Hill.

Hedström, K., Kolkowska, E., Karlsson, F., y Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384.

Herath, T., y Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Herath, T., Herath, H. y Bremser, W. G. (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for It Security Performance Management. *Information systems management*, 27 (1), 72-81.

Hofel, C. y Schendel E. (1978). Strategy Formulation: Analytical Concepts. St. Paul. Minn. West Publishing Company.

Höne, K., y Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & security*, 21(5), 402-409.

Hong, K. S., Chi, Y. P., Chao, L. R., y Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), 104-115.

Huang, S.-M., Lee, C.-L. y Kao, A.-C. (2006). Balancing Performance Measures for Information Security Management: A Balanced Scorecard Framework. *Industrial Management & Data Systems*, 106 (2), 242-255.

Humphreys, E. J., Moses, R. H., y Plate, A. E. (1998). Guide to risk assessment and risk management. British Standards Institution.

Hussain, S. J. y Siddiqui, M. S., (2005). *Quantified Model of COBIT for Corporate IT Governance, International Conference on Information and Communication Technologies, Karachi, Pakistan,*. Recuperado de: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1598575&isnumber=33619

ISACA,2016. *Fundamentos de seguridad cibernética CSAC de ISACA*, disponible en: www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIgnatuschtschenko_GCSCC_presentation_160112_0.pdf

ISO/IEC (2013). Iso/Iec 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements (Second Edition)." Geneva, Switzerland: ISO/IEC.

ISO/IEC 27000. (2016). *Information technology–Security techniques–Information security management systems–Overview and vocabulary*. Recuperado de: https://www.iso.org/standard/66435.html.

IT Governance Institute, (2000). COBIT Executive Summary, 3rd Edition, Released by COBIT Steering Committee, 3.

Jenster, V. (1987). Using Critical Success Factors in Planning. *Long Range Planning*, 20. (4),102-109.

Johnston, A. C., y Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, 52(1), 126-129.

Jourdan, Z., Rainer, R.K., Marshall, T.E. y Ford, F.N. (2010). An investigation of organizational information security risk analysis. *Journal of Service Science*, 3 (2), 33-42

Kabay, M.E., (1996). The NCSA Guide to Enterprise Security, McGraw-Hill, Nueva York, NY.

Kaplan, R. S. y Norton, D. P. (1992). The Balanced Scorecard-Measures That Drive Performance. *Harvard Business Review*, 70, 71-79.

Kaplan, R. S. y Norton, D. P. (1993). Putting the Balanced Scorecard to Work. *Harvard Business Review*, Sept–Oct, 134-147.

Kaplan, R. S. y Norton, D. P. (2004). The Strategy Map: Guide to Aligning Intangible Asset. *Strategy & Leadership*, 32 (5), 10-17.

Karlsson, F., Hedström, K., y Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, 67, 267-279.

Kayworth, T. y Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, 9 (3), 163-175.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., y Nelson Ford, F. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Knapp, K. J., Morris Jr., F., Marshall, T. E. y Byrd, T. A. (2009). Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, 28 (7), 493- 508.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. y Breitner, M. H. (2014). Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, 37 (12), 1049-1092.

Lee, S. y Ahn, H. (2008). Assessment of Process Improvement from Organizational Change. *Information & Management*, 45 (5), 270-280.

Leidecker K. y Bruno (1984). Identifying and using Critical Success Factors. *Long Range Planning*, 17 (1), 23-32.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, 173-186.

Ma, Q., Schmidt, M. B. y Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business*, 30 (1), 58-69.

Marr, B. y Schiuma, G. (2003). Business Performance Measurement - Past, Present and Future. *Management Decision*,41, 680-687.

Martin, C., Bulkan, A. y Klempt, P. (2011). Security Excellence from a Total Quality Management Approace. *Total Quality Management*, 22 (3), 345–371.

Martino, A. A. (2012). Asecho del derecho a la privacidad en América Latina.

Mohr, J. y Spekman, R. (1994). Characteristics of Partnership Success: Partnership Attributes, Communication Behavior, and Conflict Resolution Techniques. *Strategic Management Journal*, 15 (2), 135-152.

Narain S.A., Gupta, M. P., y Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, 27(5), 644-667.

Nazareth, D. L. y Choi, J. (2015). A System Dynamics Model for Information Security Management. *Information & Management*, 52, 123-134.

NIST Interagency Report (IR) 7298 Revision 2. (2013). *Glossary of key information security terms*. Recuperado de: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Nyanchama, M. (2005). Enterprise Vulnerability Management and Its Role in Information Security Management. *Information Systems Security*, 14 (3), 29-56.

Ortiz U., F. G. (2007). La entrevista de investigación en las ciencias sociales. México: Limusa.

Pipkin, D. L. (2000). Information Security: Protecting the Global Enterprise. Upper Saddle River, NJ: Prentice-Hall PTR.

Pizarro, A. (2000). El análisis de estudios cualitativos. Atención primaria, 25(1) disponible en http://ww25.atencionprimaria.com/revista/1A_oo/

Posthumus, S., y Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, 23(8), 638-646.

Psomas, E. (2016). The Underlying Factorial Structure and Significance of the Six Sigma Difficulties and Critical Success Factors: The Greek Case. *The TQM Journal*, 28 (4), 530-546.

Rainer Jr, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently?. *Information Systems Security*, 16(2), 100-108.

Reed, R. y Buckley R. (1988). Techniques for implementing Strategy. *Long Range Planning*, 21(3), 67-74.

Robert, N., Dearden E. y Vancil F. (1972). Key economic variables. *Management Control Systems*. *Homewood. Irwin*, 147.

Rockart, J. F. (1979). Chief Executives Define Their Own Data Needs. *Harvard Business Review*, 57 (2), 81-93.

Rockart, J. F. (1982). The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective. *Sloan Management Review*, 24 (1), 3-13.

Ronald, D. (1961). Management Information Crisis.. *Harvard Business Review*,111-121.

Singh, A. N., Gupta, M. P. y Ojha, A. (2014). Identifying Factors of "Organizational Information Security Management". *Journal of Enterprise Information Management*, 27 (5), 1-24.

Smith, S. y Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information systems management*, 23 (2), 23-32.

Solano, L.J., Ardila, H., y Ardila, L.E. (2016). *Gestión De Seguridad De La Información: Revisión Bibliográfica. El Profesional de La Información*, 25(6), 931–948. Recuperado de: https://doi-org.e-revistas.ugto.mx/10.3145/epi.2016.nov.10

Soomro, Z. A., Shah, M. H. y Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36, 215-225.

Spears, J. L. y Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, 34 (3), 503-522.

Srinivas, J.,Kumar D. y Kumar, N.,(2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-188, ISSN 0167-739X.

Stoll, M. (2014). An Information Security Model for Implementing the New ISO 27001, Handb. Res. Emerg. Dev. Data Priv., 216

Straub Jr, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Straub Jr, D. W., y Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS quarterly*, 45-60.

Straub, D. W., y Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.

Symantec, (2014). Recuperado de: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Taylor, S.J., y Bogdan, R. (1992). Intrucción a los métodos cualitaivos de investigación. Barcelona:Paidos.

Taylor, S., Lloyd, V., y Rudd,C.,(2011). ITIL Version 3 Service Design, The Office of Government Commerce.

Tsohou, A., Karyda, M., y Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security*, 52, 128-141.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., y Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*,18 (5),350-36 5.

Tu, C., Yuan, Y., Archer, N., y Connelly, C. (2018). Strategic value alignment for information security management: a critical success factor analysis. *Information & Computer Security*, 26(2), 150-170.

Tudor, J.K. (2001). Information Security Architecture, CRC Press, Boca Raton, FL.

Valle, M. S. (2007). *Técnicas cualitativas de investigación social.* Madrid: Sintesis Sociología.

Van B., (2007). Foundations of IT Service Management based on ITIL V3, ITIL, 1, 234.

Velázquez, F., & Nava, N. (2014). La hermenéutica analógica en el análisis organizacional. *Telos. Revista de Estudios Interdisciplinarios en Ciencias Sociales*, *16*(2), 195-206. Recuperado el 09 de diciembre de 2019, de http://publicaciones.urbe.edu/index.php/telos/article/view/3399.

Vermeulen, C., y Von Solms, R. (2002). The information security management toolbox–taking the pain out of security management. *Information management & computer security*, 10(3), 119-125.

Von Solms R. y Von Solms, B., (2004). From policies to culture, *Comput Secur*, 23, 275-279.

Von Solms, R. (1999). Information Security Management: Why Standards Are Important. *Information Management & Computer Security*, 7 (1), 50-58.

Von Solms, R. y Von Solms, SB. (2006). Gobierno de la seguridad de la información: un modelo basado en el ciclo de control directo. *Computer and Security*, 25 (6), 408-412.

Von Solms, R., Thomson, K. L., y Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. Information Security for South Africa (pp. 1-6). IEEE.H.S. Venter, M. Coetzee, M. Loock(Eds.). *Information security South Africa* (ISSA) (2011),1-6.

Vormayr G., Zseby T. y Fabini J., (2017). Botnet Communication Patterns, in IEEE Communications Surveys & Tutorials,19(4), 2768-2796. Recuperado de: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8026031&isnumber=8115327

Warkentin, M. y Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems*, 18 (2), 101–105.

Webb, J., Maynard, S., Ahmad, A. y Shanks, G. (2014). Information Security Risk Management: An Intelligence-Driven Approach. *Australasian Journal of Information Systems,*18 (3), 391-404.

Werlinger, R., Hawkey, K. y Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*,17 (1), 4-19.

Whitman, M.E, Mattord H.J. (2009). Principles of information security (3rd ed.), Thompson Course Technology

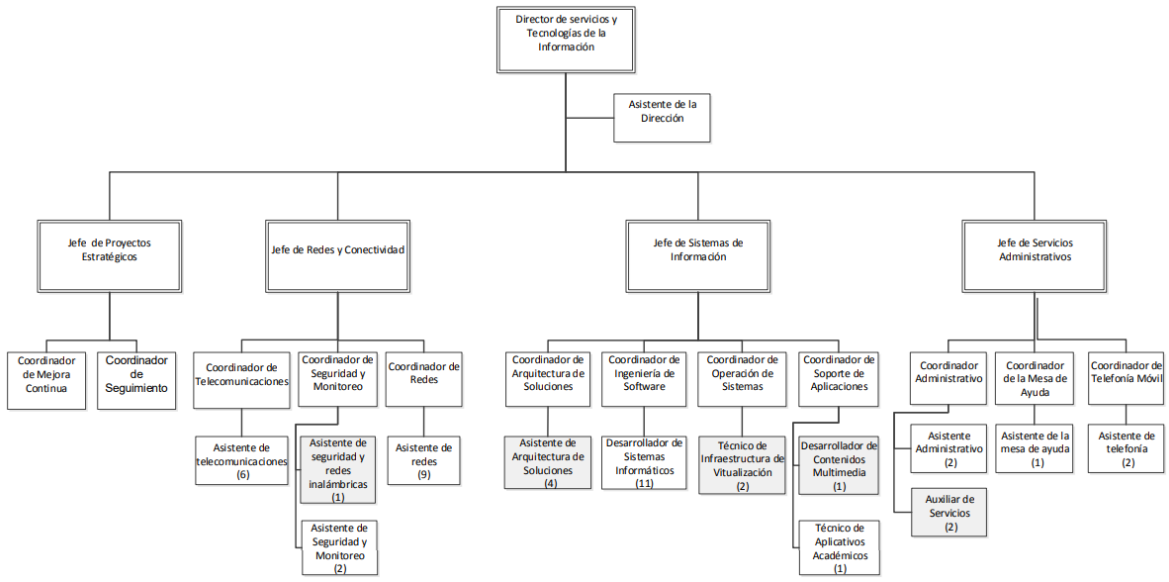
Whitworth, B., y Whitworth, E. (2014). Spam and the social-technical gap. *Computer,* 37(10), 38-45.

Yeoh, W. y Popovič, A. (2016). Extending the Understanding of Critical Success Factors for Implementing Business Intelligence Systems. *Journal of the Association for Information Science and Technology*, 67 (1), 134-147.

APENDICES

ANEXO 1

Organigrama de la DSTI



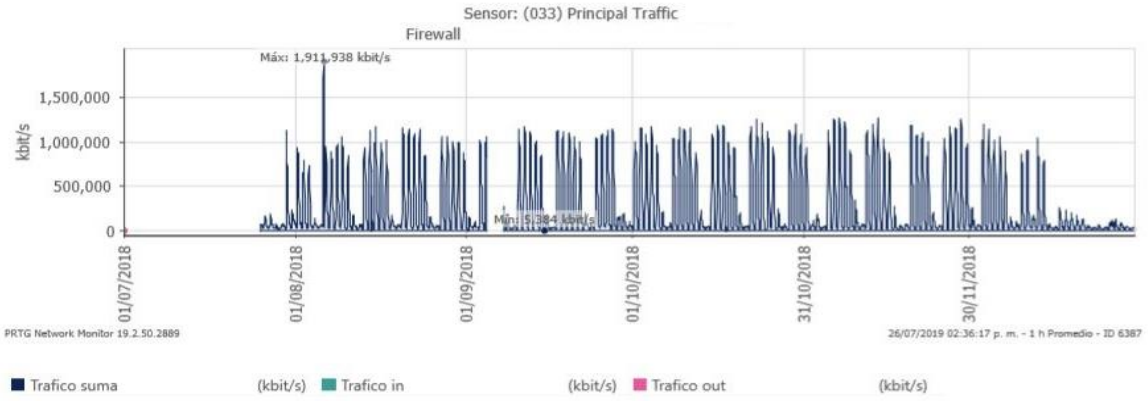
Organigrama de la DSTI, MO-DSTI -01, 2019

ANEXO 2

Uso de Internet, dentro de la Universidad de Guanajuato

Informe para (033) Principal Traffic

Plazo de tiempo de informe:	01/07/2018 12:00:00 a. m. - 31/12/2018 12:00:00 a. m.					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, dispositivo:	Sonda de clúster > Firewall					
Nodo de clúster:	(MONITOREO1					
Estadísticas de tiempo disponible:	Disponible:	100 %	[153d 09h 32m 48s]	Fallo:	0 %	[00s]
Estadísticas de petición:	Bueno:	99.995 %	[220885]	Fallo:	0.005 %	[10]
Promedio (Trafico suma):	262,421 kbit/s					
Total (Trafico suma):	424,680,135,619 KByte					



Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Tiempo de inactividad	Cobertura
Sumas (de 3712 valores)	424,680,135,619 KByte		354,076,188,578 KByte		70,603,947,042 KByte			
Promedios (de 3712 valores)	114,407,364 KByte	262,421 kbit/s	95,386,904 KByte	218,793 kbit/s	19,020,460 KByte	43,628 kbit/s	0 %	84 %

Dirección de Servicios de Tecnologías de la Información (DSTI) UG, 2019

ANEXO 3

GUIA DE ENTREVISTA

OBJETIVO:

Conocer los factores críticos que contribuyen al éxito de la seguridad de la información dentro de la institución.

Fecha de la entrevista: / / Hora:

Lugar:

Nombre:

Sitio de trabajo:

Cargo:

Unidad Administrativa a la que pertenece:

1. Sensibilización de la organización

¿Qué es la seguridad de la información?

¿Cuáles considera que son los factores críticos de éxito que hacen eficaz la seguridad de la información dentro de la institución?

¿Cuál es la política actual sobre seguridad de la información dentro de la institución?

¿Cómo se establecen los planes de continuidad?

¿Cuáles considera son los incidentes de seguridad de la información más importantes que se presentan en la institución?

2. Alineación del negocio

¿Cuenta con un portafolio de proyectos de seguridad de la información? ¿Como son alineados a los objetivos de la institución?

¿Cuándo la Alta Dirección (Rector o Secretarías) participa en la priorización de los proyectos del portafolio de seguridad de la información?

¿Cuáles fueron los proyectos con los que contó el Portafolio el año pasado?

3. Apoyo de la dirección

¿Cómo los servicios prestados son aprobados por su usuario líder?

¿Cuándo se presentan informes a la Alta Dirección (Rector o Secretarías) del desempeño de los Servicios que presta a los usuarios?

¿Cuáles son los procedimientos formales para la administración de las operaciones?

¿Cuándo se realizan auditorias para verificar la efectividad y la eficiencia de los servicios? ¿Como se realizan?

Tipo de Auditorias en Seguridad Informática que se realizan:

Dentro de la planeación anual, ¿se tiene destinado un presupuesto específico para la seguridad de la información?

4. Controles de seguridad

¿Ha firmado un acuerdo de confidencialidad con la institución?

¿Qué metodología de administración de proyectos tiene implementada?

¿Cuál es el marco de referencia en seguridad de la información que aplica?

¿Cómo utiliza la gestión de riesgos dentro sus procesos?

¿Qué metodologías o estándares utiliza para el análisis de riesgos?

¿Cuál es el proceso para la respuesta a incidentes de seguridad de la información que aplica?

¿Cuáles son las herramientas de seguridad de la información implementadas?

¿Qué factores impactan en la efectividad de las medidas de seguridad?

5. Rendimiento de gestión de seguridad de la información

¿Cuáles son los valores que se fomentan en su área de trabajo?

¿Cómo se establecen las metas de trabajo dentro de su departamento?

¿Cómo se atienden las quejas o sugerencias de los usuarios?

¿Cuáles son sus actividades establecidas dentro de la institución?

¿Cuáles certificaciones o capacitación a recibido sobre seguridad de la Información?

¿Como se informa o capacita a la comunidad sobre amenazas y medidas preventivas de seguridad de la información?

AGRADECIMIENTO: Agradecimientos por la participación, atención, tiempo que me ha dedicado y aporte en este proceso de formación.