UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS ECONOMICAS Y FINANCIERAS

CARRERA CONTADURIA PÚBLICA

INSTITUTO DE INVESTIGACIÓN DE CIENCIAS CONTABLES, FINANCIERAS Y AUDITORIA

UNIDAD DE POSTGRADO

TALLER DE INVESTIGACION I

PERFIL DE TESIS

PROPUESTA DE DISEÑO, IMPLANTACIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN TECNOLOGIA DE LA INFORMACIÓN PARA ENTIDADES GUBERNAMENTALES DE BOLIVIA BASADO EN LA NORMA NB/ISO/IEC 27001:2013

CASO: MINISTERIO DE EDUCACIÓN - UNIDAD DE AUDITORIA INTERNA - USO DEL WHATSAPP

Postulante: Noemi Abigail Laura Zurita
Docente: MMA. Ruth Benites Cuenta
La Paz, Bolivia

2017

INDICE

INDICE DE GRÁFICOS

ABREVIATURAS

CGEIT	Certificado en Gobierno de TI de la Empresa
CISA	Auditor Certificado de Sistemas de Información
CISM	Gerente Certificado de Seguridad de la Información
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas
CRISC	Certificado en Riesgos y Controles de los Sistemas de Información
EDP	Asociación de Auditores de Procesamiento Electrónico de Datos
IEC	Comisión Electrotécnica Internacional
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ISO	Organización Internacional de Normalización
ITGI	Instituto de Gobierno de TI
NTP	Norma Técnica Peruana
POI	Planes Operativos Informáticos
SGSI	Sistemas de Gestión de Seguridad de la Información
TI	Tecnología de la Información

INTRODUCCIÓN Y DESARROLLO DEL PROBLEMA

INTRODUCCIÓN

Este trabajo de investigación pretende implantar e implementar el sistema de gestión de seguridad de la información en tecnología de la información para entidades gubernamentales de Bolivia en base a la confidencialidad, integridad y disponibilidad de la información y una de las razones es por el uso excesivo del WhatsApp, que es una de las mayores herramientas de comunicación de hoy en día que influye en nuestras vidas, especialmente en el aspecto laboral.

Dentro de los aspectos que presentan mayores desafíos para las organizaciones en Latinoamérica se destaca la implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes y brechas de seguridad de la información. Esto resulta de relevancia considerando que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses. (Deloitte, 2016)[1]

En el entorno de negocios actual, la información que se maneja tanto al interior de una organización como hacia el exterior de la misma está expuesta a un gran número de riesgos, los cuales tienen un impacto variable en los atributos de seguridad de la información: confidencialidad, integridad y disponibilidad. En la actualidad, el principal reto está en entender los riesgos específicos para cada entorno de negocios en particular y también entender, o incluso medir, **el impacto que estos riesgos tienen sobre la seguridad de la información.** (DUXDILIGENS)[2]

[1] Deloitte. (2016). Deloitte. Obtenido de https://www2.deloitte.com/co/es/pages/risk/articles/la-evolucion-de-la-gestion-de-cyber-riesgos-y-seguridad.htm

[2] DUXDILIGENS. (s.f.). DUXDILIGENS. Obtenido de http://www.duxdiligens.com/seguridad-informacion.shtml

España es el país europeo con más uso del WhatsApp, los datos confirman ahora esta realidad: con una cuota de penetración del 70% entre los usuarios de telefonía móvil, España se ha convertido en el cuarto país del mundo en uso de WhatsApp.

Los españoles son además los europeos que más utilizan este popular servicio de mensajería instantánea, por detrás de países como Italia -62% de cuota de penetración, séptimo país del mundo y segundo de Europa-, Holanda -61% de cuota-, y Alemania -57% de cuota de penetración-, según el informe Telco Trends 2015 que elabora Strategy&, consultora estratégica de PwC que aprecia, sin embargo, que las operadoras no han podido rentabilizar este inmenso negocio. No en vano, durante el año 2014 se enviaron diariamente 30.000 millones de wasaps, lo que arroja un promedio de cuatro WhatsApp por cada habitante del planeta. (Cuiñas, 2015)[3]

En Inglaterra esta aplicación no tiene tanta acogida, de hecho tan solo un 39% de los móviles ingleses tienen instalado WhatsApp, mientras que en España el 97% lo tienen instalado. (Adrian, 2016)[4]

Estados Unidos es un país en el cual nacen las tendencias de Internet para los consumidores del mundo, popularizando páginas tales como Google y Facebook. Pero cuando se trata de la mensajería móvil, el país se queda muy atrás.

En Brasil, WhatsApp tiene una penetración estimada del 70% entre los propietarios de teléfonos inteligentes, que lo utilizan para vender productos, la promoción de los candidatos políticos, y para reemplazar el correo electrónico del trabajo. En la India, donde WhatsApp tiene más de 70 millones de usuarios activos mensuales, la aplicación

[3] Cuiñas, A. B. (25 de febrero de 2015). EL MUNDO. Obtenido de EL MUNDO: http://www.elmundo.es/economia/2015/02/25/54ece95cca47414b488b456f.html

[4] Adrian. (junio de 2016). Trucos Londes. Obtenido de Trucos Londes: https://trucoslondres.com/whatsapp-inglaterra/

se ha vuelto tan popular que los médicos lo utilizan para mantenerse en contacto con los pacientes.

Line cuenta con 53 millones de usuarios mensuales en Japón y 17 millones de usuarios mensuales en Taiwán (alrededor del 80% de la población total de este último), y recientemente ganó $ 234 millones en ingresos trimestrales, en gran parte gracias a los juegos virtuales. (HOT NEWS, 2015)[5]

De acuerdo al diagnóstico efectuado en Bolivia el 67.5 por ciento de la población boliviana, de 14 años o más, es internauta, es decir que en los últimos 30 días previos a la encuesta, han tenido acceso a internet al menos una vez.

De estos internautas el 94 por ciento utiliza la red social Facebook y el 91 por ciento WhatsApp. Le sigue youtube con un público del 40 por ciento de internautas y luego twitter con un 17 por ciento. (Lima, 2017)[6]

Hoy en día la forma en la que nos comunicamos está sufriendo un profundo cambio tras la aparición de los medios de comunicación y de las nuevas tecnologías. Entre ellas se ha de destacar el uso de los teléfonos móviles, que tras la aparición de los Smartphone son una herramienta indispensable en nuestro día a día. Se ha llegado a un punto en el que gran parte de nuestras interacciones sociales se dan por medio de los Smartphone, en concreto, por medio de aplicaciones como WhatsApp. La aparición de este tipo de mensajería ha supuesto asimismo un gran cambio en la forma en la que interactuamos con los demás.

[5] HOT NEWS. (25 de agosto de 2015). Obtenido de http://www.mundotkm.com/us/hot-news/18703/por-que-whatsapp-no-funciona-en-estados-unidos Juarez

[6] Lima, E. (17 de mayo de 2017). AGENCIA DE GOBIERNO ELECTRONICO Y TECNOLOGIAS DE COMUNICACION E INFORMACION. Obtenido de AGETIC: https://blog.agetic.gob.bo/2017/05/facebook-y-whatsapp-acaparan-el-uso-de-redes-sociales-en-bolivia/

La aparición de este tipo de mensajería ha supuesto asimismo un gran cambio en la forma en la que interactuamos con los demás. La aparición de tecnologías como intermediario del acto comunicativo puede suponer a su vez un obstáculo para el mismo o una vía más eficaz, pero ¿Afecta también en el aspecto laboral? Al ser la comunicación un aspecto tan propio de la naturaleza social del hombre, la aparición del WhatsApp interfiere, ya sea de forma negativa o positiva, en el aspecto social y laboral del hombre.

De esta manera podemos darnos cuenta de que el objetivo de WhatsApp es lograr adaptar las características de una comunicación oral a la escrita mediante los teléfonos móviles, de manera que sea instantánea, teniendo como consecuencia la falta de la información documentada en las entidades gubernamentales en base a evidencias como exige la norma internacional por el uso excesivo de este medio.

CAPÍTULO I:

DESARROLLO DEL PROBLEMA

1.1 IDENTIFICACIÓN DEL PROBLEMA

De acuerdo al estudio realizado se pudo identificar la falta de Seguridad de la Información por el uso del WhatsApp para las entidades Gubernamentales de Bolivia - Caso Ministerio de Educación.

El uso excesivo del WhatsApp ha afectado muchos aspectos de nuestras vidas, especialmente en el aspecto laboral. Todo lo que digamos y hagamos con el uso excesivo del WhatsApp puede perjudicar nuestra vida profesional ya que el uso de este medio nos consume tiempo de las horas de trabajo, dinero e ineficiencia en avance del trabajo lo que puede perjudicar la imagen de la empresa u organización en la que trabajamos e incluso puede llegar a costarnos el puesto.

1.2 PLANTEAMIENTO DEL PROBLEMA

La falta de seguridad de la información puede ocasionar el impacto potencial de una falla de seguridad de la información en las entidades Gubernamentales, teniendo en cuenta las potenciales consecuencias por la pérdida de la confidencialidad, integridad o disponibilidad de la información y de otros recursos.

Las Organizaciones en Latinoamérica se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales y de mayor exposición a las cyber amenazas inherentes a este nuevo contexto de negocios.

En los resultados obtenidos revelan que si bien hay una consolidación de la función de gestión de cyber riesgos y seguridad de la información, los ejecutivos responsables de administrar la seguridad de la información consideran que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer. (Deloitte, 2016)

El uso indebido del servicio de mensajes WhatsApp puede ser peligroso porque crea adicción en algunas personas y deja huellas difíciles de controlar y borrar. Este tipo de conducta, llevada a los extremos, puede provocar problemas de aprendizaje, reducción de la capacidad de retención y menor capacidad de dar la cara entre las personas, mencionan algunos expertos.

Riesgos provoca el uso excesivo de WhatsApp

El WhatsApp, es una de las apps más utilizadas en nuestros días, ya que es una herramienta muy útil que facilita la comunicación además no es costosa. Pero qué sucede cuándo se es adicto a este tipo de Apps, aunque no lo crean, utilizar WhatsApp por un tiempo prolongado puede ser riesgoso según expertos.

Aunque utilizar este tipo de aplicaciones adictivas parezca inofensivo, deja algunas consecuencias serias, a continuación se presentan las consecuencias de utilizar WhatsApp:

WhatsAppitis:

Sencillamente, se trata de la ansiedad que sufren las personas al olvidar su Smartphone, ya que se sienten totalmente incomunicados sin leer sus mensajes.

Tendinitis:

Esto es provocado por el uso excesivo de la escritura en el teclado del celular, lo que puede provocar es inflamación en un tendón por escribir de manera constante.

Phubbig:

Esto se trata de estar totalmente aislado de tus seres queridos, por estar en el celular o contestando mensajes en las Apps y redes sociales, es lo que más afecta al ser humano ya que se pierden de grandes momentos con sus familias por esta adicción. (Juarez, 2016)[7]

Si no se controla el uso del WhatsApp puede generar adicción, problemas en las relaciones interpersonales y alterar el orden vital de las personas, por el uso indebido del WhatsApp.

1.3 FORMULACION DEL PROBLEMA

¿Con este diseño de implantación e implementación de un sistema de gestión de seguridad de la información en tecnología de la información se lograra proteger la seguridad de la información en base a la confidencialidad, integridad y disponibilidad de la información en las Entidades Gubernamentales de Bolivia - Caso Ministerio de Educación: Unidad de Auditoria Interna?

[7] Juarez, T. (7 de noviembre de 2016). TELEVISA. Obtenido de http://www.televisajuarez.tv/15-estilo-de-vida/1877-que-riesgos-provoca-el-uso-excesivo-de-whatsapp

1.4 OBJETIVOS DE LA INVETIGACIÓN

1.4.1 OBJETIVO GENERAL

Proponer un diseño, implantación e implementación de un sistema de gestión de seguridad de la información en tecnología de la información para entidades Gubernamentales de Bolivia basado en la Norma NB/ISO/IEC 27001:2013 – Caso Ministerio de Educación: Unidad de Auditoria Interna: uso del WhatsApp".

1.4.2 OBJETIVOS ESPECIFICOS

- Diseñar un Manual de un sistema de gestión de seguridad de la información en tecnología de la información para entidades Gubernamentales de Bolivia – Caso Ministerio de Educación: Unidad de Auditoria Interna: uso del WhatsApp
- Diseñar un control y planificación de la información documentada.
- Establecer una política de seguridad de la información documentada
- Definir un proceso de evaluación y tratamiento de riesgo de la seguridad de la información
- Mejorar el sistema de seguridad de la información dentro de la entidad

1.5 HIPOTESIS

El diseño, implantación e implementación de un sistema ayudara a mejorar de manera continua un sistema de gestión de la información - Ministerio de Educación: Unidad de Auditoria Interna: uso del WhatsApp en base a la confidencialidad, integridad y disponibilidad de la documentación, para evitar el riesgo de pérdidas de la información.

1.5.1 CAUSA

VARIABLE INDEPENDIENTE 1

Falta de diseño de seguridad de la información en tecnología de la información en base a la confidencialidad, integridad y disponibilidad.

1.5.2 EFECTO

VARIABLE DEPENDIENTE 2

Pérdida de información importante de la organización.

1.5.3 SOLUCIÓN

VARIABLE MODERANTE 3

Para entidades gubernamentales de Bolivia recomendadas por la NB/ISO/IEC 27001:2013

1.6 JUSTIFICACIÓN

La presente trabajo de investigación será preparada para proporcionar los requisitos para establecer, implementar mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.

1.6.1 Justificación teórica

El presente trabajo es una utilidad para la parte académica que beneficia a los estudiantes de la Unidad de Pregrado y Postgrado de la Universidad Mayor de San Andrés.

1.6.2 Justificación practica

El proyecto de investigación se orienta a conocer los factores que contribuyen a mejorar la falta de seguridad de la información de tecnologías de información:

- Asegurar la integración de los requisitos del sistema de la seguridad de la información a los procesos de las entidades gubernamentales.

- Asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles.

- Comunicar la importancia de la gestión de seguridad de la información efectiva y del cumplimiento de los requisitos del sistema de gestión de la seguridad de la información

- Asegurar que el sistema de gestión de la seguridad de la información logre sus resultados esperados.

MARCO TEORICO

CAPÍTULO II:

MARCO TEORICO O CONCEPTUAL

La Auditoría de Tecnologías de la Información y la Comunicación es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de Tecnologías de la Información y la Comunicación, para expresar una opinión independiente respecto:

i) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

ii) Al uso eficaz de los recursos tecnológicos.

iii) A la efectividad del sistema de control interno asociado a las Tecnologías de la Información y la Comunicación.

2.1 DISEÑO

ISO/9001[8]

Conjunto de procesos que transforma los requisitos en características especificadas o en la especificación de un producto, proceso o sistema.

NIA 402.8 (b)[9]

[8] ISO/IEC 17799 (2003): International: calidad: definición de términos
[9] NIA 402: "Consideraciones de auditoria relativa a una entidad que utiliza una organización de servicio"

Informe sobre la descripción y el diseño de los controles de una organización de servicios

(a) una descripción, preparada por la dirección de la organización de servicios, del sistema de la organización de servicios, de los objetivos de control y de otros controles relacionados que se han diseñado e implementado en una fecha determinada; y

(b) un informe elaborado por el auditor del servicio, con el objetivo de alcanzar una seguridad razonable, que incluya su opinión sobre la descripción del sistema de la organización de servicios, de los objetivos de control y otros controles relacionados, así como de la idoneidad del diseño de los controles para alcanzar los objetivos de control especificados.

2.2 SISTEMA

NB/ISO/IEC 17799 (2003)[10]

Sistemas electrónicos de oficina

Se debe preparar e implementar políticas y lineamientos para controlar las actividades de la empresa y riesgos de seguridad relacionados con los sistemas electrónicos de oficina. Estos proporcionan la difusión y distribución más rápida de la información de la empresa mediante una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz general, multimedia, servicios o instalaciones postales y máquinas de fax.

[10] NB/ISO/IEC 17799 (2003): International Organizacion For Standardization: "Seguridad de los sistemas electrónicos de oficina": Pág. 34

ISSAI/ES/1003 (2013)[11]

Sistema de información relevante para la información financiera

Elemento del control interno que incluye el sistema de información financiera, consistente en los procedimientos y registros establecidos para iniciar, registrar, procesar e informar sobre las transacciones de una entidad (así como hechos y circunstancias) y para rendir cuentas sobre los activos, pasivos y patrimonio neto relacionados.

http://www.contraloria.gob.bo: NAG 270 y correlativa[12]

Sistema de información (SI)

Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

2.3 GESTIÓN

NB/ISO/IEC 17799 (2003)[13]

El proceso de identificación, control y minimización o eliminación a un costo aceptable de los riesgos de seguridad que podrían afectar a los sistemas de información.

[11] ISSAI/ES/1003 (2013) Glosario de términos de las Directrices de auditoría financiera Pág. 34
[12] http://www.contraloria.gob.bo/Auditorias TIC: Fuente: Normas de Auditoría Gubernamental NAG 270 y correlativa
[13] NB/ISO/IEC 17799 (2003): International Organizacion For Standardization: Gestión de Riesgos Pág. 5

2.4 SEGURIDAD DE LA INFORMACIÓN

NB/ISO/IEC 17799 (2003)[14]

La preservación de la confidencialidad, integridad y disponibilidad de la información:

- Confidencialidad: garantía de que acceden a la información, solo aquellas personas autorizadas a hacerlo.

- Integridad: Salvaguardar de la exactitud y totalidad de la información y los métodos de procesamiento.

- Disponibilidad: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieren.

NB/ISO/IEC 17799 (2005)[15]

Preservación de confidencialidad, integración y disponibilidad de la información, además también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad.

2.5 TECNOLOGIA DE LA INFORMACIÓN

ISSAI/ES/1003 (2013)[16]

Procedimientos manuales o automatizados que operan habitualmente en relación con la gestión de procesos. Los controles de aplicación pueden ser de naturaleza preventiva o

[14] NB/ISO/IEC 17799 (2003): International Organizacion For Standardization
[15] NB/ISO/IEC 17799 (2005): International Organizacion For Standardization
[16] ISSAI/ES/1003 (2013) Glosario de términos de las Directrices de auditoría financiera: Controles de aplicación en las tecnologías de la información (TI) Pág. 11

de detección y se diseñan para asegurar la integridad de los registros contables. Por consiguiente, los controles de aplicación están relacionados con los procedimientos que se usan para iniciar, registrar, procesar e informar sobre transacciones u otros datos financieros.

http://www.contraloria.gob.bo: NAG 270 y correlativa[17]

Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Se refiere al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información.

https://delgadocaramutti.wordpress.com/[18]

La Auditoria de Tecnologías de Información (T.I.), como se le conoce actualmente, (Auditoria informática o Auditoria de sistemas en nuestro medio), se ha consolidado en el mundo entero como cuerpo de conocimientos cierto y consistente, respondiendo a la acelerada evolución de la tecnología informática de los últimos 10 años. En algunos países altamente desarrollados es catalogada como una actividad de apoyo vital para el mantenimiento de la infraestructura crítica de una nación, tanto en el sector público como privado, en la medida en que la Información es considerada un activo tan o más importante que cualquier otro en una organización. Existe un cuerpo de conocimientos, normas, técnicas y buenas prácticas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la Información tratada y

[17] http://www.contraloria.gob.bo/Auditorias TIC: Fuente: Normas de Auditoría Gubernamental NAG 270 y correlativa
[18] https://delgadocaramutti.wordpress.com/

almacenada a través del computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de un ente están manejando dicha Información y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoría de general aceptación y conocimiento técnico específico.

También desde el punto de vista en cuanto a Especialidad profesional se refiera, es apoyada por un conjunto de conocimientos profundos acerca de la tecnología informática, de técnicas y procedimientos de auditoría y de conocimientos contables suficientes, para evaluar la calidad, fiabilidad y seguridad de un entorno informático dado, así como brindar seguridad razonable acerca de la utilidad de la información almacenada y procesada en ellos, con el fin de emitir un juicio al respecto. ENTIDAD PÚBLICA

ISSAI/ES/1003 (2013)[19]

Oficina, unidad, agencia, servicio o ministerio público, o un grupo consolidado de estas entidades.

[19] ISSAI/ES/1003 (2013) Glosario de términos de las Directrices de auditoría financiera Pág. 5

MARCO HISTORICO

CAPÍTULO III:

MARCO HISTORICO

3.1 TECNOLOGIAS DE INFORMACIÓN

Las tecnologías de información (TI) constituyen uno de los principales instrumentos que apoyan la gestión de las organizaciones mediante el manejo de grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Su uso ha implicado, al menos, tres situaciones relevantes: la dedicación de porciones importantes del presupuesto de las organizaciones, con el costo de oportunidad que ello conlleva, principalmente en organizaciones con recursos limitados y actividades sustantivas esenciales para la sociedad; un marco jurídico cambiante tendente a buscar su paralelismo con las nuevas relaciones que se dan a raíz del uso de esas TI; y una presión importante de proveedores y consumidores por la implementación de más y mejores servicios apoyados en estas tecnologías.

Dado el impacto de dichas situaciones, las TI deben gestionarse dentro de un marco de control que procure el logro de los objetivos que se pretende con ellas y que dichos objetivos estén debidamente alineados con la estrategia de la organización.

Con el propósito de coadyuvar con ese marco de control y procurar una mejor gestión de dichas tecnologías por parte de las organizaciones, esta Contraloría General sustituye el “Manual sobre normas técnicas de control interno relativas a los sistemas de información automatizados”, mediante la promulgación de las presentes “Normas técnicas para la gestión y el control de las tecnologías de información”, que se

constituyen en una normativa más ajustada a la realidad y necesidad de nuestro ámbito tecnológico actual.

En razón de que dicha normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, el jerarca y los titulares subordinados, como responsables de esa gestión, deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292. Asimismo, la Función de TI debe contribuir con ello cumpliendo con dicho marco de control y facilitando la labor estratégica del jerarca.

Esta normativa es de acatamiento obligatorio para la Contraloría General del Estado y las instituciones y órganos sujetos a su fiscalización, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable. (Normas Gestión Control TI-CGE)

3.2 HISTORIA DE WHATSAPP

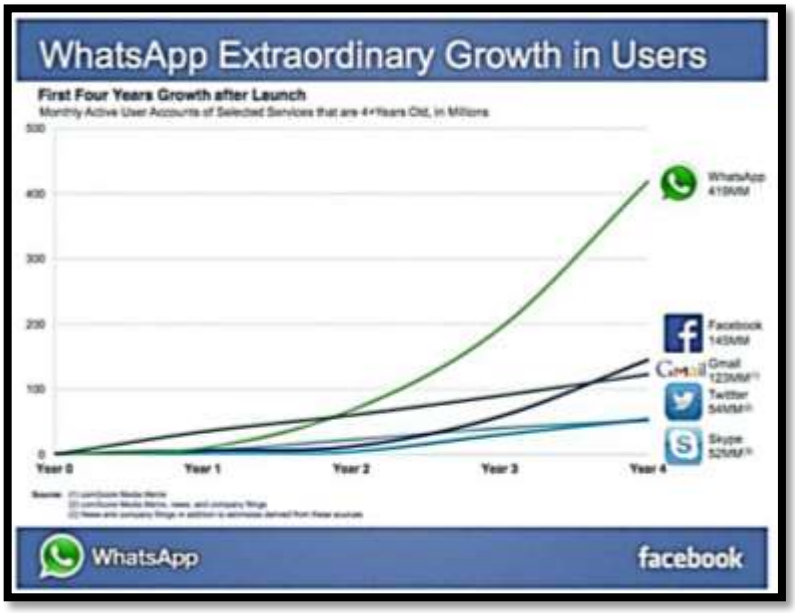
Hasta ahora, se había investigado sobre la historia de WhatsApp y su evolución (Catalina Larrondo G., 2014), su papel en las prácticas de intimidad familiar (Lucía Jiménez Iglesias, 2014) y el WhatsApp como complemento de aprendizaje (Ana Morató Payá, 2014) por eso nos ha parecido interesante investigar sobre este tema porque creemos que es necesario contrastar, si los hubiera, los beneficios y los peligros que puede suponer el uso de una aplicación la cual su uso está tan extendido hoy en día.

WhatsApp propone un tipo de comunicación que nunca había tenido lugar a lo largo de la historia, ya que es una aplicación de mensajería ‘’de pago’’ (con un coste de 0,99€/año) que permite enviar y recibir mensajes mediante Internet (de modo instantáneo). Además los usuarios pueden crear grupos y enviarse mutuamente

imágenes, vídeos y grabaciones de audio. La aplicación fue creada en enero de 2009 principalmente por Jan Koum, y el 19 de febrero de 2014 fue comprada por la empresa Facebook por 19 millones de dólares (Catalina Larrondo G.). Consta con más de 600 millones de usuarios en todo el mundo ya que ha tenido mucho éxito por ser de gran utilidad. Esto es fácilmente apreciable en el gráfico 1.

En un principio, se utilizaba para añadir un estado, como en el gimnasio, poca batería, disponible...visible a tus contactos. Más tarde fue añadiendo distintas funciones hasta llegar a la aplicación de la que disponemos hoy en día. Lo que distinguía a WhatsApp de BlackBerry Messenger (otra aplicación que cubría la mayoría de las funciones actuales de WhatsApp) era que el método de registro no era sólo mediante un código asociado a un teléfono móvil de la marca, sino que se realizaba a través de los números de teléfono haciéndolo accesible a todo tipo de terminales móviles.

GRÁFICO 1: Extraordinario aumento de usuarios de WhatsApp



Fuente: móvil zona

Como podemos apreciar en la gráfica 1, WhatsApp tuvo un gran éxito, y el número de usuarios aumentó masivamente hasta llegar a los 400 millones en sus primeros cuatro años de actividad. Quienes se ven más afectados, positiva o negativamente, por los cambios que conllevan los nuevos medios de comunicación son aquellos que han nacido, o están desarrollando su personalidad, al mismo tiempo de su implementación en la sociedad. Por eso hemos querido investigar el impacto de WhatsApp, en el aspecto laboral de las entidades gubernamentales de Bolivia.

MARCO REFERENCIAL

CAPÍTULO IV:

MARCO REFERENCIAL

4.1 ANTECEDENTES DE LA ISO/IEC 27001

La norma ISO 27001, creada por la International Organization for Standardization (ISO), tiene por objeto proporcionar una metodología universal para la implementación, administración y mantenimiento de la seguridad de la información dentro de una organización.

- Una auditoría ISO 27001 demuestra la conformidad de su Sistema de Gestión de la Seguridad de la Información (SGSI) con los estándares documentados.
- Por lo general es utilizada por organizaciones que quieren demostrar la madurez de su seguridad de la información.
- Satisface las obligaciones contractuales y puede ayudar a obtener una exclusividad competitiva frente a su competencia.[20]

4.1.1 QUE ES LA ISO/IEC 27001

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

[20] http://www.a-lign.com/iso27001-espanol

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

La norma ISO 27001 es un instrumento base para la gestión de la seguridad de la información, estructurándose en un conjunto de controles y de recomendaciones dirigido a los responsables de promover, implantar y mantener la seguridad en las entidades. Mediante ella las empresas pueden certificar sus Sistemas de gestión de Seguridad de la Información (SGSI). Un SGSI es un sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en función de los requisitos técnicos, legales y organizativos identificados en la organización.[21]

4.1.2 EVOLUCIÓN

En el año 2004 se publicó la UNE 71502 titulada Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002.

Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001.

[21] https://delgadocaramutti.wordpress.com/

4.1.3 CAMBIOS DE LA ISO 27001:2013

Existen varios cambios con respecto a la versión 2005 en esta versión 2013. Entre ellos destacan:

- Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades.

4.1.4 PROCESO DE AUDITORÍA ISO 27001

El proceso de auditoría ISO 27001 de A-LIGN consta de las siguientes fases:

- Determinación del Ámbito
- Pre-evaluación (opcional)
- Etapa 1 – revisión de la documentación

- Etapa 2 – pruebas detalladas

4.1.5 IMPLANTACIÓN

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).

4.1.6 CERTIFICACIÓN

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2.

Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación trienal, puesto que la certificación BS 7799-2 ha quedado reemplazada.

El Anexo C de la norma muestra las correspondencias del Sistema de Gestión de la Seguridad de la Información (SGSI) con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004 (ver ISO 14000), hasta el punto de poder llegar a certificar una organización en varias normas y con base en un sistema de gestión común.

4.1.7 EVOLUCIÓN

La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC:

4.2 ISO 27000

Publicada en mayo de 2009, contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

4.2.1 UNE-ISO/IEC 27001:2007

"Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la de la versión española 29 noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799).

4.2.2 ISO/IEC 27002: (anteriormente denominada ISO 17799)

Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.

4.2.3 ISO/IEC 27003: En fase de desarrollo; probable publicación en 2009

Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

4.2.4 ISO 27004: Publicada en diciembre de 2009

Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.

4.2.5 ISO 27005: Publicada en junio de 2008

Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

4.2.6 ISO 27006: Publicada en febrero de 2007

Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

4.3 ANTECEDENTES DE LA ISO/IEC 17799

ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos internacionales miembros de ISO e IEC participan en el desarrollo de Estándares Internacionales a través de los comités establecidos por la organización respectiva para lidiar con áreas particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, junto con ISO e IEC, también participan en el trabajo. En el campo de la tecnología de la información. ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Los Estándares Internacionales son diseñados en concordancia con las reglas dadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico son presentados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere de la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

Se presta atención a la posibilidad que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no debieran ser responsables de identificar todos o alguno de dichos de derechos de patente.

ISO/IEC 17799 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

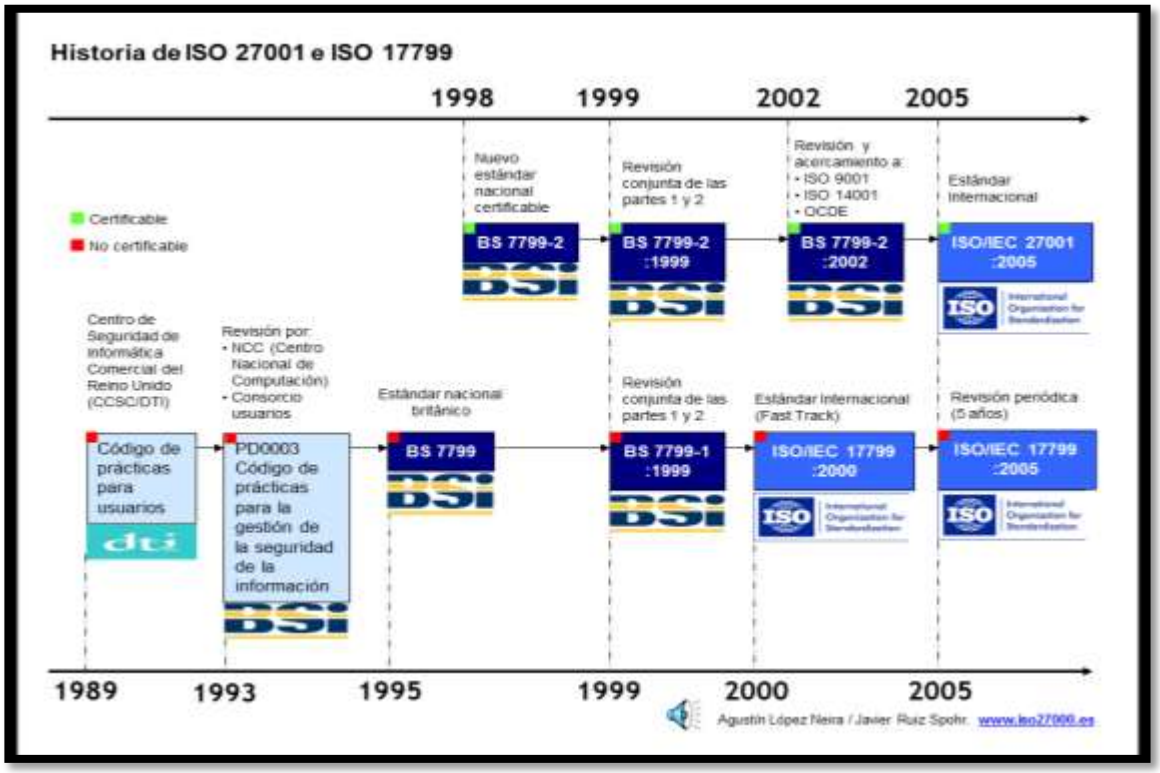
La segunda edición cancela y reemplaza la primera edición (ISO/IEC 17799:2000), la cual ha sido revisada técnicamente.

El ISO/IEC JTC 1/SC 27 viene desarrollando una familia de Estándares Internacionales para el Sistema de Gestión de Seguridad de la Información (ISMS). La familia incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. La familia adoptará el esquema de numeración utilizando las series del número 27000 en secuencia.

A partir del 2007, se propone incorporar una edición nueva del ISO/IEC 17799 en este nuevo esquema de numeración con el nombre ISO/IEC 27002.[22]

[22] ISO/IEC 17799 (2015) Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información Pág. 7

GRÁFICO 2: Historia de la ISO 27001 e ISO 17799



Fuente: http://www.iso27000.es/download/HistoriaISO27001.pps

4.3.1 POLÍTICA DE SEGURIDAD DE LA ISO/IEC 17799

Los riesgos tecnológicos actuales, al cual están expuestos los activos de información de las diferentes organizaciones del sector público, el 25 de Agosto del 2007 emitió a través de la **Resolución Ministerial 246-2007-PCM**, el uso obligatorio de la NTP-ISO/IEC 17799: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

Toda norma que regule la materia de seguridad de la información, tiene como finalidad asegurar los tres requisitos básicos:

- **Confidencialidad.** Exclusivamente las personas autorizadas a disponer de la información pueden acceder a ella.

- **Integridad.** La información ha de encontrarse operativa tal y como se encuentra en los sistemas de información. No ha de ser manipulada ni en su origen, ni en su destino, salvo por aquellas personas autorizadas.

- **Disponibilidad.** El acceso continúo a la información, en cualquier momento, por aquellas personas autorizadas a tratar y disponer de aquella.

Los tres requisitos precedentes son los pilares para asegurar la información y cualquier proceso que haga uso de esta como por ejemplo, la normativa de firma electrónica, el funcionamiento del D.N.I. electrónico, las medidas de seguridad en materia de protección de datos de carácter personal, etc.

La NTP contempla diferentes aspectos a ser considerados en la elaboración de los planes de seguridad de la información:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio

- Conformidad

Puedes encontrar mayor información en la NTP publicada en el banco de normas de la ONGEI

4.3.2 ALCANCES

Todas las instituciones públicas del Estado Peruano deberán considerar en materia de seguridad de la información lo siguiente:

- Las instituciones deberán implementar sus planes de seguridad en base a la NTP-ISO/IEC 17799.

- Las máximas autoridades de las instituciones deberán conformar un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes de la institución.

- Las máximas autoridades de las instituciones deberán asignar las responsabilidades en materia de seguridad de la información a funcionarios de su planta.

- Los planes de seguridad se reflejarán en los planes operativos informáticos de las instituciones (POI).

4.3.3 ÁMBITO DE APLICACIÓN DE LA NORMA

Según Decreto Supremo **N° 063-2007-PCM** y Decreto Legislativo **N° 604**, la ONGEI es el órgano especializado que depende jerárquicamente del Presidente del consejo de Ministros encargada de dirigir, como ente rector, el Sistema Nacional de Informática y de implementar la política nacional de Gobierno Electrónico e Informático.

En este sentido el ámbito de aplicación incluye a todas las entidades del Gobierno Central, Organismos Públicos Descentralizados, Gobiernos Regionales, Direcciones Regionales y cualquier organización estatal no empresarial con:

- Autonomía financiera
- Personalidad jurídica
- Patrimonio propio

Donde el Estado Nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones.

4.3.4 PLAZOS

La implementación de la Norma se dará de manera progresiva y teniendo como plazos los estipulados en la RM 244-2004-PCM el haber preparado su plan de implementación.

4.3.5 MODELO SIMPLIFICADO DE IMPLEMENTACIÓN

La aplicación de la Norma Técnica Peruana de Seguridad de la Información tiene que estar alineada a la misión, visión, y objetivos que persigue la organización. A partir de este análisis se tiene que aplicar un esquema de gestión de la seguridad de la información. Para lo cual se detalla a continuación un esquema simplificado de cómo debería de aplicarse la NTP-ISO/IEC 17799:2004 dentro de cualquier organización pública.

a) ETAPA I

Esta primera etapa consiste en analizar la misión, visión y objetivos de la organización.

Misión y Visión y Objetivos de la Organización.

La misión y visión dan el enfoque claro de lo que la organización debería plantearse en términos de seguridad de la información de manera general.

Identificación de los recursos dentro de los procesos de la organización

El análisis de las principales funciones dentro de los procesos de la organización nos permitirá identificar todos los recursos que interactúan en estos procesos, los cuales podemos clasificarlos de la siguiente manera:

Materiales y Tecnológicos

Los recursos materiales y tecnológicos involucrados.

Recursos Humanos

Los recursos humanos involucrados.

Como resultado de esta etapa se tiene que tener una matriz con las funciones y todos los recursos o activos de información involucrados dentro del proceso analizado.

b) ETAPA II

En esta etapa debemos de usar la información obtenida de la Etapa I, para implementar lo que se recomienda dentro de la NTP-ISO/IEC 17799.

Establecimiento de la Política de Seguridad de la organización.

Se establecerá la política general a nivel de toda la organización, a partir de esta política se desarrollarán las normativas internas y procedimientos específicos, para cada área dentro de la empresa con el fin de cumplir con la política general.

Efectuar un análisis de riesgos.

En base a los activos identificados en la Etapa I, se comenzará a elaborar un análisis de riesgos, con la finalidad de poder identificar las vulnerabilidades, amenazas e impacto de estos sobre los activos identificados.

En base a los controles establecidos para cada dominio de la Norma que permita establecer la Brecha

El análisis de riesgos nos permitirá priorizar cuales son los activos prioritarios a proteger, y en base a esto realizar una comparación de lo que ya se tiene implementado versus lo que falta implementar, como medidas de seguridad.

c) ETAPA III

En esta etapa se tiene que proyectar la implementación de lo que se necesita en términos de seguridad.

Documentación del Plan de Seguridad de la Información

Establecimiento del documento del plan a 1, 2 o 3 años.

Implementación del Plan de Seguridad dentro del POI

Lo que se tiene en el plan tiene que estar reflejado como un proyecto de TI adicional dentro del Plan Operativo Informático.

d) ETAPA IV

Una vez elaborados los pasos anteriores se definen como entregables los siguientes documentos:

- Política de Seguridad
- Análisis de riesgos

- Brecha de lo implementado y lo que falta por implementar
- Plan de Seguridad de la Información (reflejado en el POI)[23]

4.4 HISTORIA DE LA NORMA ISACA

ISACA fue conformada por personas que reconocieron la necesidad de contar con una fuente centralizada de información y guías en el creciente campo de la auditoría a los controles de los sistemas computacionales. Hoy, ISACA tiene más de 115,000 miembros en todo el mundo.

4.4.1 VISIÓN GENERAL

ISACA comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones—se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI. **Conocida previamente como la Information Systems Audit and Control Association** (Asociación de Auditoría y Control en Sistemas de Información), ISACA ahora es solo un acrónimo, que refleja la amplia gama de profesionales en gobierno de TI a los que sirve.

Hoy, los integrantes de ISACA – más de 115,000 en todo el mundo – se caracterizan por su diversidad. Los integrantes viven y trabajan en más de 180 países y cubren una

[23] https://delgadocaramutti.wordpress.com/

variedad de puestos profesionales relacionados con TI – sólo por nombrar algunos ejemplos, auditor de SI, consultor, profesional de la educación, profesional de seguridad de SI, regulador, director ejecutivo de información (CIO) y auditor interno. Algunos son nuevos en el campo, otros están en niveles medios de la gerencia y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, contabilidad pública, gobierno y sector público, servicios y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista muy diferentes sobre una variedad de tópicos profesionales. Esta ha sido considerada durante mucho tiempo como una de las fortalezas de ISACA.

4.4.2 RED GLOBAL

Otra de las fortalezas de ISACA es su red de capítulos. ISACA tiene más de 200 capítulos en más de 80 países de todo el mundo, y dichos capítulos brindan a sus miembros educación, recursos compartidos, asesoría, red de contactos profesionales y una amplia gama de beneficios adicionales a nivel local. Descubra si hay un capítulo cerca de usted.

Desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales en gobierno, control, seguridad y auditoría de la información. Sus estándares de auditoría y control de SI son seguidos por profesionales de todo el mundo. Sus investigaciones abordan temas profesionales que son desafíos para sus miembros.

Su certificación *Certified Information Systems Auditor* "Auditor Certificado de Sistemas de Información", (CISA) es reconocida globalmente y ha sido obtenida por más de 109,000 profesionales desde su creación. La certificación *Certified Information*

Security Manager "Gerente Certificado de Seguridad de la Información", (CISM) se concentra exclusivamente en el sector de gerencia de seguridad de la información y ha sido obtenida por más de 25,000 profesionales. La certificación *Certified in the Governance of Enterprise IT* "Certificado en Gobierno de TI de la Empresa" (CGEIT)" promueve el avance de profesionales que desean ser reconocidos por su experiencia y conocimiento relacionados con el Gobierno de las TI y ha sido obtenida por más de 6,000 profesionales. La certificación *Certified in Risk and Information Systems Control* "Certificado en Riesgos y Controles de los Sistemas de Información" (CRISC) está designada para profesionales de TI que identifican y gestionan los riesgos a través del desarrollo, implementación y mantenimiento de controles de SI ha sido obtenida por más de 17,000 profesionales.

ISACA publica el *ISACA Journal*, una revista técnica líder en el campo de control de la información. Organiza una serie de conferencias internacionales que se concentran en tópicos técnicos y gerenciales pertinentes a las profesiones de aseguramiento, control, seguridad de SI y gobierno de las TI. Juntos, ISACA y su afiliado el *IT Governance Institute* "Instituto de Gobierno de TI" (ITGI) lideran la comunidad de control de tecnología de la información y sirven a sus asociados brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente.[24]

4.4.3 ¿QUE ES ISACA?

ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

[24] http://www.isaca.org/about-isaca/history/espanol/pages/default.aspx

4.4.4 HISTORIA ISACA

Fue fundada en el año 1967. Fue incorporado por las personas que reconocieron la necesidad de una fuente centralizada de información y orientación en el creciente campo de los controles de auditoría para los sistemas informáticos. . Fue en 1969 que el grupo se formalizó a asociación, originalmente incorporada como EDP Auditors Association. En 1976 el nombre pasó a ser ISACA, por el que es actualmente conocida, y se estableció la primera certificación profesional de auditoría de sistemas de información, o CISA. Hoy en día, ISACA sirve 140.000 profesionales en 180 países.

4.4.5 OBJETIVOS

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

4.4.6 HECHOS SOBRE ISACA

Son los custodios del framework COBIT;

Son los creadores del ITGI (IT Governance Institute);

Desarrollaron cuatro certificaciones profesionales:

- CISA - Certified Information Systems Auditor, certificación de auditores de sistemas de información. Existen cerca de 90.000 personas certificadas (2012);

- CISM - Certified Information Security Manager, certificación de gestores de seguridad. Existen cerca de 16.000 personas certificadas;

- CGEIT - Certified in the Governance of Enterprise IT, certificación de gestores de la gobernanza empresarial TI. Existen cerca de 4.600 personas certificadas (2007);

- CRISC - Certified in Risk and Information Systems Control, certificación de gestores de control de riesgos en sistemas de información. Existen cerca de 15.000 personas certificadas (2010).

4.4.7 ¿QUÉ ES COBIT?

Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

4.4.8 RED GLOBAL

Otra de las fortalezas de ISACA es su red de capítulos. ISACA tiene más de 200 capítulos en más de 80 países de todo el mundo, y dichos capítulos brindan a sus miembros educación, recursos compartidos, asesoría, red de contactos profesionales y una amplia gama de beneficios adicionales a nivel local. Descubra si hay un capítulo

cerca de usted. Desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales en gobierno, control, seguridad y auditoría de la información. Sus estándares de auditoría y control de SI son seguidos por profesionales de todo el mundo. Sus investigaciones abordan temas profesionales que son desafíos para sus miembros.[25]

[25] https://es.slideshare.net/ElvinHernandez2/normas-y-estndares-aplicables-a-la-auditoria-informtica

BIBLIOGRAFIA

- NB/ISO/IEC 27001:2013: Tecnología de la información, técnica de seguridad, sistemas de gestión de seguridad
- NB/ISO/IEC 17799 (2005): Tecnología de la información, código de practica para la gestión de la seguridad de la información
- NB/ISO/IEC 17799:2003: Tecnología de la información, código de practica para la gestión de la seguridad de la información
- NB/ISO/90003: 2005: Ingeniería del Software
- NIA 402: "Consideraciones de auditoria relativa a una entidad que utiliza una organización de servicio"
- ISSAI/ES/1003 (2013) Glosario de términos de las Directrices de auditoría financiera
- http://www.contraloria.gob.bo/Auditorias TIC: Fuente: Normas de Auditoría Gubernamental NAG 270 y correlativa
- Normas Gestión Control TI-CGE
- http://www.contraloria.gob.bo/Auditorias TIC: Fuente: Normas de Auditoría Gubernamental NAG 270 y correlativa
- https://es.wikipedia.org/wiki/ISO/IEC_27001#ISO_27001:2013
- **http://www.iso9001calidad.com/definicion-de-terminos-586.html**
- https://es.slideshare.net/ElvinHernandez2/normas-y-estndares-aplicables-a-la-auditoria-informtica

REFERENCIAS

- Barredo, A. (06 de 06 de 2016). *Hipertextual.* Obtenido de Hipertextual: https://hipertextual.com/2016/06/whatsapp-espana-sms
- Cuiñas, A. B. (25 de febrero de 2015). *EL MUNDO.* Obtenido de EL MUNDO: http://www.elmundo.es/economia/2015/02/25/54ece95cca47414b488b456f.html

- Deloitte. (2016). *Deloitte.* Obtenido de https://www2.deloitte.com/co/es/pages/risk/articles/la-evolucion-de-la-gestion-de-cyber-riesgos-y-seguridad.html
- DUXDILIGENS. (s.f.). *DUXDILIGENS.* Obtenido de http://www.duxdiligens.com/seguridad-informacion.shtml
- *HOT NEWS.* (25 de agosto de 2015). Obtenido de http://www.mundotkm.com/us/hot-news/18703/por-que-whatsapp-no-funciona-en-estados-unidos
- Juarez, T. (7 de noviembre de 2016). *TELEVISA.* Obtenido de http://www.televisajuarez.tv/15-estilo-de-vida/1877-que-riesgos-provoca-el-uso-excesivo-de-whatsapp
- Lima, E. (17 de mayo de 2017). *AGENCIA DE GOBIERNO ELECTRONICO Y TECNOLOGIAS DE COMUNICACION E INFORMACION* . Obtenido de AGETIC: https://blog.agetic.gob.bo/2017/05/facebook-y-whatsapp-acaparan-el-uso-de-redes-sociales-en-bolivia