REPÚBLICA DEL ECUADOR

UNIVERSIDAD TECNOLÓGICA
EMPRESARIAL DE GUAYAQUIL

TRABAJO DE TITULACIÓN
PARA LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN GESTIÓN DE TELECOMUNICACIONES MENCIÓN REDES DE ACCESO Y TELEFONÍA

TEMA:

METODOLOGÍA DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 APLICADA A ENTIDADES FINANCIERAS.

AUTOR:
JAVIER GEOVANNY MORALES GUIJARRO

GUAYAQUIL – ECUADOR
2018

AGRADECIMIENTO

Agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas.

A mis padres por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron en todo el camino, pero sobre todo agradezco a mi esposa por el apoyo incondicional brindado y por acompañarme en cada momento que pensaba en rendirme, y por saber usar las palabras exactas que despertaban el deseo de continuar.

A mis hijos por ayudarme con cada una de sus sonrisas a levantarme el ánimo y acompañarme en esas largas jornadas de estudios e investigaciones.

A todos docentes que con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional.

DEDICATORIA

Primeramente dedico este trabajo a Dios, por estar a mi lado y estar siempre conmigo, guiándome en mí camino.

A mi familia:

A mi esposa Lady Marisol Armijos Suarez; por estar conmigo siempre brindándome su compañía y apoyo incondicional, por cada una de sus palabras de aliento y sobre todo por ser mi compañera de vida. A mis hijos Jahir y Joshua que son el motor de mi vida que cada día me motivan a dar lo mejor de mí y por inyectarme esa energía que necesito con cada una de sus sonrisas.

A mis Padres por haberme educado con el amor necesario para lograr ser quien soy y haber cultivado en mí la virtud de la responsabilidad que son la base principal de todo, orgullosamente dedico este trabajo a ellos, mis padres Jorge Morales y Ana Guijarro.

La responsabilidad de este trabajo de Investigación, con sus resultados y conclusiones pertenece exclusivamente al autor.

……..
Javier Morales Guijarro

METODOLOGÍA DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 APLICADA A ENTIDADES FINANCIERAS.

Javier Geovanny Morales Guijarro
Universidad Tecnológica Empresarial de Guayaquil
Javier.morales2683@gmail.com

RESUMEN

Este artículo tiene como objetivo presentar una descripción de los puntos más importantes de la norma ISO 27001:2013 y su aplicación en instituciones financieras como bancos, cooperativas y empresas tanto públicas como privadas y donde para un mejor entendimiento se mencionara de una manera detallada el proceso de implementación y las fases que se deberán cubrir basado en algunas experiencias de implementaciones realizadas ya que esta norma puede ser implementada con objetivos de obtener una certificación o tan solo poner en marcha mejores prácticas que ayuden a perfeccionar las seguridades físicas y tecnológicas implementadas. Así también se hace referencias claras que ayudarán a mantener un orden interno sobre la gestión de sus activos de información mediante el levantamiento de políticas y procedimientos de las distintas áreas que intervengan dentro del alcance; donde durante todo el desarrollo de este artículo se podrá evidenciar el paso a paso de las actividades a realizar y de cómo estos puntos favorecerán a la institución.

INTRODUCCIÓN

En el transcurso de los últimos años instituciones financieras alrededor del mundo han sido víctimas de ciberataques y de robos millonarios según últimas encuestas realizadas por entidades internacionales como PCI COUNCIL encargada de generar normativas para entidades financieras que ayudan a cuidar datos de tarjetas de créditos. Ante esta realidad las entidades financieras se han visto en la necesidad de encontrar estrategias que ayuden a proteger la información de sus clientes y lograr la continuidad del negocio en caso de que sus seguridades fuesen vulneradas.

¿Cómo ayudaría la implementación de la norma ISO 27001:2013 a las entidades financieras? ISO 27001:2013 es un estándar que ayuda a identificar e implementar procedimientos y políticas orientadas a proteger la información logrando identificar sus riesgos internos y externos estableciendo una metodología y su correcta aplicación, identificando sus activos críticos, y los controles que intervendrán para protegerlos; a su vez al momento de implementar el sistema de gestión de seguridad de información se considerara una fase importante que es la de concientización al personal interno ya que es la parte más importante de las instituciones.

MARCO TEÓRICO

Para la construcción de este artículo hemos identificado a la información como el activo más importante que tienen todas las instituciones ya sean estas instituciones financieras y empresas públicas o privadas cuyo objetivo principal es brindar confianza a sus clientes mediante el resguardo de sus datos; lo que las lleva a buscar e implementar metodologías y herramientas tecnológicas que ayuden a brindar un tratamiento a los riesgos que se encuentran latentes como se menciona a continuación “En la actualidad a causa de la evolución de la tecnología y desconocimiento de la misma somos más vulnerables.” (AUTELSI, 2018)

La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros (ISO27001, 2016).

Actualmente muchas de estas instituciones utilizan las redes sociales para darse a conocer sin tomar las debidas precauciones sobre las seguridades que las plataformas en la nube puedan ofrecer, generando innumerables amenazas, dejando a las instituciones totalmente vulnerables a la materialización de Riesgos presentes sobre la seguridad de su información logrando tener impactos negativos para la institución a nivel de imagen y económico logrando a su vez comprometer los tres factores importante sobre la seguridad de información como son la disponibilidad, confidencialidad e integridad, como podemos apreciar en el siguiente enunciado: “Tenemos que considerar que la seguridad de la información no se lo gestiona adquiriendo herramientas de software o hardware. Cada organización debe

establecer su normativa de seguridad que contiene políticas, procedimientos y roles los mismo que deben estar definidos en la organización” (ZAPATA, 2014)

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) tendrá como propósito garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, así como lo menciona el siguiente enunciado “Se deben establecer controles para minimizar los riesgos significativos y de alto impacto para la institución, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial” (ROBIN, 2014)

El SGSI ayudara a las instituciones a establecer políticas y procedimientos en relación a los objetivos de las instituciones, con objeto de mantener un nivel de exposición siempre menor de riesgo decidido asumir, considerando el siguiente concepto de riesgo:

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia. Existe 3 naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales. (MOSQUERA, 2017)

Dentro de los puntos importantes considerados por la norma ISO 27001 al momento de implementar toda institución deberá tener claros los siguientes significados mencionados a continuación: confidencialidad “Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas” (Celestino, 2017); Disponibilidad “Condición que garantiza que los usuarios

autorizados tengan acceso a la información institucional y a los recursos relacionados" (MORALES, 2014); Integridad: "Característica de los activos, los mismos no pueden ser modificados sin autorización o personal no autorizado" (Muñoz, 2015), Vulnerabilidad: "Deficiencias que se pueden convertir en amenazas", Amenazas: "cualquier acción o evento que puede ocasionar consecuencias adversas", Riesgo Residual: "Riesgo que permanece después de que se han implementado medidas y controles" (VARGAS, 2014); Política de Seguridad: "Normativa interna de seguridad que regula las líneas sobre la forma en que trabajará la organización en el tema de seguridad de la información" (Ronderos, 2016); Análisis de riesgo: "Es el proceso cuantitativo o cualitativo que permite evaluar los riesgos" (NIEVES, 2017).

La seguridad de la información da lineamientos claros de cómo se podrá implementar buenas prácticas mientras que las instituciones deberán considerar identificar la infraestructura tecnológica que soportan, almacenan y transmiten la información por lo que las obliga a establecer y clasificar estos activos que puede ser una tarea de grandes proporciones, sobre todo en aquellas grandes instituciones, ya que es probable que existan terabytes de datos electrónicos, almacenes de documentos y miles de personas y dispositivos que hacen parte de los activos tecnológico. (Gallardo, 2013, pág. 12). Debemos dejar claro que las instituciones podrán crear sus propias metodologías que les ayuden a evaluar los riesgos y como base para la creación podrán tomar como referente distintas normas; para lo cual mencionamos los siguientes conceptos como son:

La norma ISO 31000:2009: “Establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz; recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo” (Novoa, 2015).

Metodología Octave: Se centra en el estudio de riesgos Organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia partiendo de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa. (Carmona, 2013)

Metodología Magerit**:** “Esta metodología implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información”. (Candau, 2014)

Metodología ISO 27005: “Esta metodología muestra un enfoque directamente centrado en Risk Management para Tecnologías de la Información”. (GARCÍA, 2017)

La metodología ayudara a identificar la importancia que soportan los activos mediante la ejecución de talleres logrando evaluar los riesgos y que como paso siguiente ayudara a definir estrategias de control, y recomendaciones enfocadas a cumplimiento de un Sistema de gestión de seguridad de Información, cumpliéndose con la normas de seguridad de información la empresa deberá proceder a crear un

documento de aplicabilidad, tomando como referencia el siguiente contexto: “SOA se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad)” (Mendoza, 2015). Tenemos que considerar que los ataques que pueden sufrir las instituciones son ataques externos que al materializarse con éxito tendría como afectación un impacto reputacional ya que no se pueden prevenir por tratarse de eventos fortuitos; sin embargo también se tendrá que considerar los ataques internos a los que están expuestos las instituciones y que muchas veces son ejecutados por el personal contratado; los mismos que pueden ser controladas por capacitaciones, concientizaciones constantes al personal para lograr disminuir la fuga de información que cada uno de los colaboradores manejan internamente, tal como se menciona en las siguiente referencia: “El éxito de la sensibilización es la practicidad y la simplicidad en que esta información es entregada, para captar la atención del aprendiz” (Mintic, 2016). Una vez que la institución tiene un personal comprometido y sensibilizado debe de monitorear y evaluar constantemente el cumplimiento de las políticas mediante auditorias, tal como lo específica a continuación en la siguiente referencia “La norma ISO 27001 establece que el propósito de la auditoría interna es verificar el cumplimiento tanto de los requisitos propios de la empresa**,** como los requisitos de la norma ISO 27001”. (ISO, 2017). Terminando así gran parte de implementación y teniendo como buena práctica la mejora continua del proceso interno de mantenimiento del sistema de Gestión adoptado y pueden ser tomado como referente la ISO 9001 “La ISO 9001:2015 establece los requisitos básicos que debe lograr una organización para administrar

su calidad. Es un modelo certificable cuya aplicación tiene alcance a nivel mundial, lo que representa una ventaja competitiva para aquellas entidades que opten por ella". (Guerra, 2016)

METODOLOGÍA

Para este artículo se consideró explicar la metodología de implementación utilizada por la empresa MA Solutions Group S.A., la misma que está basada en principios del ciclo de Deming que mantiene el concepto de mejora continua y que se encuentra alineada en buenas prácticas de estándares internacionales de direccionamiento de proyectos como es PMP (Project Managment Profesional); quienes cuenta con 7 años de experiencia en servicios de consultoría empresarial en implementaciones de la Normativa ISO 27001:2013 en el mercado Ecuatoriano, hemos podido recabar datos relevantes en base a su experiencia obtenida en trabajos ejecutados en implementaciones realizadas de Sistemas de Gestión de Seguridad de Información. Como se mencionó anteriormente la Norma ISO 27001:2013 es un estándar internacional certificable y auditable; por lo que puede ser implementado para prevenir y resguardar la seguridad de la información de las instituciones o para lograr imagen reputacional guardando los lineamientos de las cláusulas que conforman la norma. A continuación se muestra las 5 fases que las instituciones deben considerar al momento de implementar la norma ISO27001:

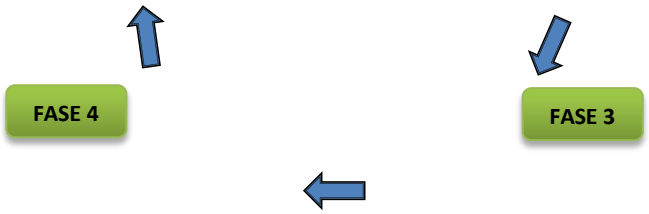


Figura 1. Fases de metodología de implementación SGSI
Fuente: Elaboración propia

FASE 1.- PLANIFICACIÓN Y CONOCIMIENTO.-

Esta fase tiene como propósito establecer el esfuerzo requerido para lograr una correcta implementación. Debemos recalcar que al iniciar un proyecto de implementación, como buena práctica se iniciara con una acta de compromiso firmada por alta gerencia; posterior se procede a la identificación de los roles internos responsables, aprobadores, consultados e informados que participaran dentro del proyecto basado en criterios de la matriz RACI como se muestra en el siguiente cuadro

Rol		Descripción	Niveles de Cargos
R	Responsable	Este rol corresponde a quien se encargara de realizar la tarea.	Jefe departamental
A	Aprobador	Este rol se encargara de que las diferentes tareas del proyecto se realicen y es el responsable de su ejecución	Gerente departamental
C	Consultado	Este rol es el que posee la información importante y relevante para el desenvolvimiento del proyecto.	Dueños de los procesos seleccionados
I	Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución del proyecto.	Directores Departamentales

basados en términos de una correcta gestión de proyectos:

Tabla 1.- Roles RACI
Fuente.- Elaboración Propia

Una vez que se tiene claro los roles internos y las responsabilidades asignadas a cada uno, las entidades deberán iniciar con la identificación de la realidad interna a nivel institucional y departamental basándose en información existente mediante la revisión de documentos existente y entrevistas al personal. Se comenzara con la revisión de los siguientes puntos: Misión, visión, objetivos estratégicos de la institución, normas regulatorios, Identificación de información, modelo operación de TI, análisis de riesgos realizados previamente; donde se preparara un check list que identifique todos requisitos existentes y faltantes logrando tener después de un análisis consensuado de toda la documentación y los resultados de las entrevistas un informe que reflejara el estado de cumplimiento con las cláusulas de la normativa ISO 27001:2013 que mencionamos a continuación en el siguiente gráfico:

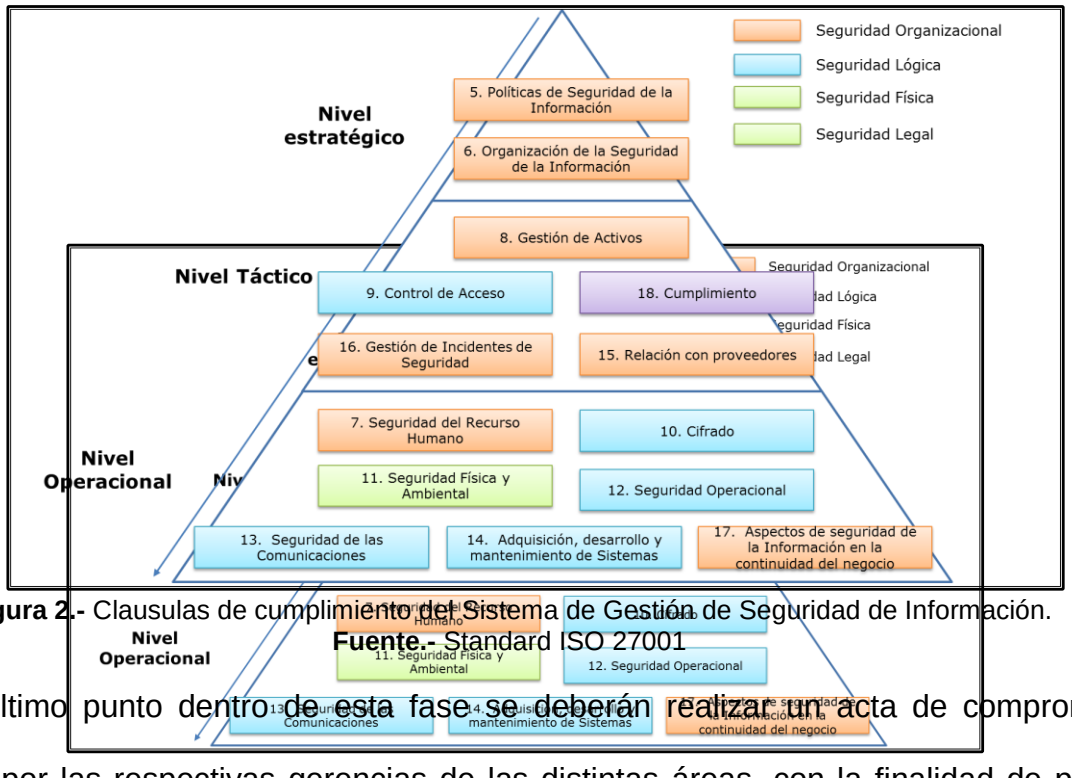


Figura 2.- Clausulas de cumplimiento del Sistema de Gestión de Seguridad de Información.
Fuente.- Standard ISO 27001

Como último punto dentro de esta fase se deberán realizar un acta de compromiso firmado por las respectivas gerencias de las distintas áreas, con la finalidad de poder contar con la disponibilidad de su personal a cargo en el transcurso de todo el proyecto.

FASE 2.- DOCUMENTACIÓN DEL ALCANCE

Esta fase comprende con las documentación de los siguientes puntos: alcance de la implementación; donde para caso práctico identificaremos al proceso de facturación del macro proceso de Financiero como referente siendo uno de los procesos importantes de toda institución, política del sistema de gestión, procedimientos expuestos por la ISO 27002:2013 basado en los controles, definición de indicadores de gestión basada en los criterios de SLA definidos internamente por la institución. Para poder levantar toda esta información las instituciones pueden redactarlas o a su vez adquirir plantillas que se encuentran a disposición en el portal web por medio de un valor a pagar en caso de considerar aprovechar el conocimiento de su personal interno o podrían realizarlo en conjunto con una empresa que brinde servicios de asesoría y acompañamiento metodológico y como resultado entregue las respectivas plantillas.

FASE 3.- IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS DE SEGURIDAD

Esta fase consistirá en identificar y documentar los siguientes puntos que son importantes para el alcance definido: inventario de activos de información, riesgos de seguridad de la información, Definición del Plan de Tratamiento de Riesgos. Para poder dar inicio al levantamiento del inventario de activos la institución deberá elaborar una plantilla que contenga los siguientes campos: nombre de la institución, departamento al que pertenece, nombre del activo, descripción, propietario, responsable; posterior se identificará campos para clasificarlos por su tipo y el nivel de confidencialidad, confidencialidad y disponibilidad que estos deben tener para la institución, como se muestra a continuación ya que no en todos los tipos de activos se calificaran los tres criterios emitidos por la norma ISO 27001:2013 como se muestra en la siguiente tabla:

Tipos de Activos	Disponibilidad	Confidencialidad	Integridad
Informacion	✓	✓	✓
Software	✓	×	×
Activos Físicos	✓	×	×
Servicios	✓	✓	×

Tabla 2.- Activos vs criterios ISO 27001
Fuente.- Elaboración Propia

Para realizarla la calificación las instituciones definirán una tabla de criterios de

Valor	Niveles	Disponibilidad	Confidencialidad	integridad
1	**Bajo**	La disponibilidad del activo no paraliza los procesos de la organización	La divulgación de la información no afecta a la imagen institucional	La información incompleta o errada no afecta la continuidad de los procesos
2	**Medio**	La disponibilidad del activo paraliza los procesos internos de la organización parcialmente 1 hora	La divulgación de la información afecta a la imagen institucional generando perdida de clientes	La información incompleta o errada afecta la continuidad de los procesos generando inconsistencia en los sistemas
3	**Alto**	La disponibilidad del activo paraliza los procesos de la organización mas de una hora generando perdidas	La divulgación de la información afecta a la imagen institucional generando perdida de dinero y demandas	La información incompleta o errada afecta la continuidad de los procesos generando inconvenientes con clientes

ponderación considerando el nivel de importancia para la institución:

Tabla 3.- Niveles de calificación de la disponibilidad, confidencialidad e integridad
Fuente.- Elaboración Propia

Terminado la calificación se procederá a identificar el lugar donde reposan dichos activos dando por cerrada la etapa de inventario de activos. Como paso siguiente se realizara la identificación de los riesgos, como primer paso se procederá a realizar una identificación de los criterios con los cuales se calificaran la probabilidad e impacto

Valor	Niveles	Probabilidad	Impacto
1	**Bajo**	La probabilidad de ocurrencia en la institución es menor.	La institución no sufre afectación en sus procesos internos
2	**Medio**	La probabilidad de ocurrencia en la institucia es de un 50%	La institución sufre una paralización de sus procesos internos de 1hora
3	**Alto**	La probabilidad de ocurrencia en la institucia es de un 100%	La institución sufre una paralización total de sus procesos internos

como lo vemos a continuación:

Tabla 4.- Criterios de Probabilidad e Impacto

Fuente.- Elaboración Propia

Definidos los criterios de evaluación de la probabilidad y el impacto se deberá preparar la matriz para evaluar los riesgos cuidando los lineamientos de la ISO 31000:2018 donde para caso práctico evaluaremos un riesgos del activo laptop del proceso de facturación, donde podremos ir viendo la evaluación de los riesgos absolutos y donde se identificaran los eventos de riesgos, las amenazas y el tipo de amenazas que

MATRIZ DE RIESGOS Y CONTROLES

Nombre del Activo : **Laptop**

Fecha de Identificación de Riesgos: 15/11/2018

I. RIESGOS DE ACTIVOS DE TI									
No.	1. IDENTIFICAR AMENAZAS		2. IMPACTO DE LA AMENAZA SOBRE LOS ATRIBUTOS DE SEGURIDAD DE LA INFORMACIÓN			3. EVENTO DE RIESGO	7. RIESGO ABSOLUTO		
	CATEGORIA AMENAZA	TIPO AMENAZA	CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD		Probabilidad	Impacto	Nivel
1	Ataques intencionados	Difusión de software dañino	NO	SI	SI	Perdida de información por virus alojado en el equipo	3	2	M

pueden afectar a la confidencialidad, disponibilidad e integridad consecuencia de su materialización y posterior proceder a valorar la probabilidad e impacto usando los criterios ya identificados anteriormente, obteniendo así el nivel de exposición del riesgo absoluto como se muestra en la siguiente imagen adjunta donde se evalúa el activo laptop que pertenece al proceso de facturación identificado como el alcance de implementación:

Figura 4.- Análisis de Riesgos Absoluto
Fuente.- Elaboración Propia

Como segunda parte se evaluará los riesgos residuales, los mismos que consistirán en evaluar los controles aplicados sobre los riesgos identificados en la primera etapa de

evaluación de Riesgos, para esta evaluación la matriz deberá considerar los siguientes campos: existe o no un control, el efecto del control implementado si se lo quiere aceptar, transferir, compartir, o evitar el riesgo; luego se deberá definir el campo donde se llevara la descripción del control implementado y los campos que ayuden a identificar el control como si automático o manual, la frecuencia se lo utiliza, si esta formalizado, quien lo ejecuta y supervisa; luego proceder a la valoración según probabilidad e impacto como lo mostramos a continuación:

II. IDENTIFICACION Y EVALUACION DE CONTROLES																	
7. RIESGO ABSOLUTO			8. RESPUESTA AL RIESGO	9. RIESGO SE INCLUYE EN EL ANÁLISIS? (S/N)	10. EXISTE CONTROL	No. Control	11. ACTIVIDADES DE CONTROLES ESPECÍFICAS	12. TIPO DE CONTROL		13. SITUA	14. EJECUTADO POR	15. SUPERVISADO POR:	16. RIESGO RESIDUAL		
Probabilidad	Impacto	Nivel						Frecuencia	Manual/ Aplicación	Formalizado			Probabilidad	Impacto	Nivel
3	2	M	Reducir	SI	SI	1	Antivirus implementado y actualizado	C	A	Si	Jefe de Infraestructura	Oficial de Seguridad de Información	2	2	B

Figura 5.- Análisis de Riesgo Residual
Fuente.- Elaboración Propia

Realizado el análisis de Riesgos Residual se procederá a designación de controles en caso de no tener ninguno o a la identificar las brechas sobre los ya existentes, generando como resultado un plan de acción el cual deberá tener en cuenta un responsable de ejecución con sus respectivas fechas de inicio y fin. Como próximo pasos se deberá crear un documento denominado SOA o acta de compromiso de aplicabilidad de los nuevos controles a implementar determinados en el plan de acción. Con esta etapa finalizada se ha logrado gran parte de la implementación, pero se deberá considerar como un proyecto independiente y no menos importante la implementación de buenas prácticas basadas en la ISO 22301:2013 (business

continuity management), como el mantener un Plan de Continuidad de Negocio también conocido como (BCP); actualizado que ayude a identificar los pasos que la institución deberá seguir en caso de un evento de catástrofe que comprometan al desarrollo de la institución, así como también su departamento de infraestructura deberá poseer un Plan de recuperación de Desastre (DRP) con la finalidad de poder tener identificado los sistemas, servidores y equipos de comunicación claves que soportan la información. Estos documentos deberán ser actualizado cada año dependiendo del crecimiento interno de la institución tiempo y puestos a prueba.

FASE DE DIVULGACIÓN SGSI

Una vez elaborados y aprobados las políticas y procedimientos se realizará la divulgación de los mismos a los responsables de la ejecución de las actividades, con el fin que se proceda a su implementación y generación de evidencias que permitan sustentar el cumplimiento de los requisitos impuestos por el sistema de gestión de Seguridad de información. La divulgación del SGSI se la deberá realizar a través de presentaciones (presenciales y/o virtuales) según público objetivo: Usuarios final, Alta Dirección, Tecnología; de toda la institución.

RESULTADOS

Dentro de este artículo podemos identificar a la última fase de la metodología como una herramienta clave que ayudara a medir el resultado de la implementación mediante un proceso de auditoría interna, que adicionalmente ayudara a tener una clara visión del estado actual de la implementación y poder dar un mantenimiento al sistema de Gestión, en esta fase se deberá trabajar en conjunto con la área de auditoría definiendo como periodos de 3 meses realizar un seguimiento de los cumplimientos de las cláusulas exigidas por la norma ISO 27001.2013.

El proceso de revisión contemplara inspección documental y de registros que serán considerados como evidencia objetiva y que soportan la implementación de las cláusulas de obligatorio cumplimiento como son:

- Alcance del sistema de gestión.
- Política de seguridad de la información.
- Procedimientos para la gestión del SGSI: Control de la Información Documentada, Auditorías Internas, Acciones Correctivas y Oportunidades de

Mejora y Revisión del Sistema de Gestión por parte de la Dirección de la Institución.

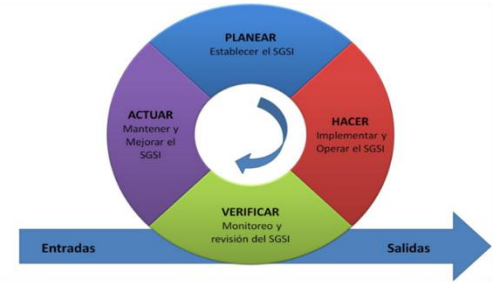
- Metodología de análisis de riesgos.
- Procedimiento de gestión de incidentes de seguridad.
- Declaración de Aplicabilidad.
- Aspectos legales y reglamentarios relacionados con las actividades incluidas en el alcance del sistema de gestión.

Una vez realizada la revisión documental se procederá a evaluar la implementación así como el nivel de cumplimiento de los controles aplicados. En esta etapa se deberá evaluar, los siguientes aspectos:

- Desarrollo y cumplimiento del plan de acción identificado.
- Evidencias obtenidas durante los últimos 6 meses, como registros, documentos y o manifiestos de proyectos en ejecución y culminados.
- Desempeño del sistema de gestión de la Institución mediante el cumplimiento de sus indicadores de gestión establecidos.
- Controles implementados de los procesos del sistema de gestión de la Institución.

Durante el transcurso de la implementación se fueron levantando gran parte de documentos que serán un input para el desarrollo de auditorías y que deben ser actualizados según el crecimiento de la institución ayudando a mantener un sistema de gestión actualizado bajo las diferencias de la nueva versión de la norma vs la anterior como lo podemos ver en el siguiente cuadro comparativo:

ISO/IEC 27001:2005



El proceso que se utiliza para la implementación del SGSI se basa en el modelo de proceso "PDCA" o también conocido como el "Ciclo de Deming", adoptado por el estándar internacional ISO/IEC 27001:2005.

ISO/IEC 27001:2005

ISO/IEC 27001:2013

Esta versión se adapta a la nueva estructura de alto nivel utilizado en todas las normas de Sistemas de Gestión y refleja una mayor flexibilidad para su implementación dentro de las empresas, sin importar su tamaño. **Su flexibilidad en gestión de riesgos permite alinearla al enfoque ERM**

Figura 6.- ISO 27001: 2013 **VS** ISO 27001:2005
Fuente.- Creación Propia

A su vez podemos evidenciar que durante años empresas a nivel mundial han ido sumándose a esta decisión de implementar la norma ISO 27001, tal como lo podemos identificar en los siguientes cuadro que nos refleja un crecimiento considerable hasta los años 2015 y 2016:

Figura 7 .- Implementación de ISO 27001
Fuente.- http://ingertec.com/iso-27001/

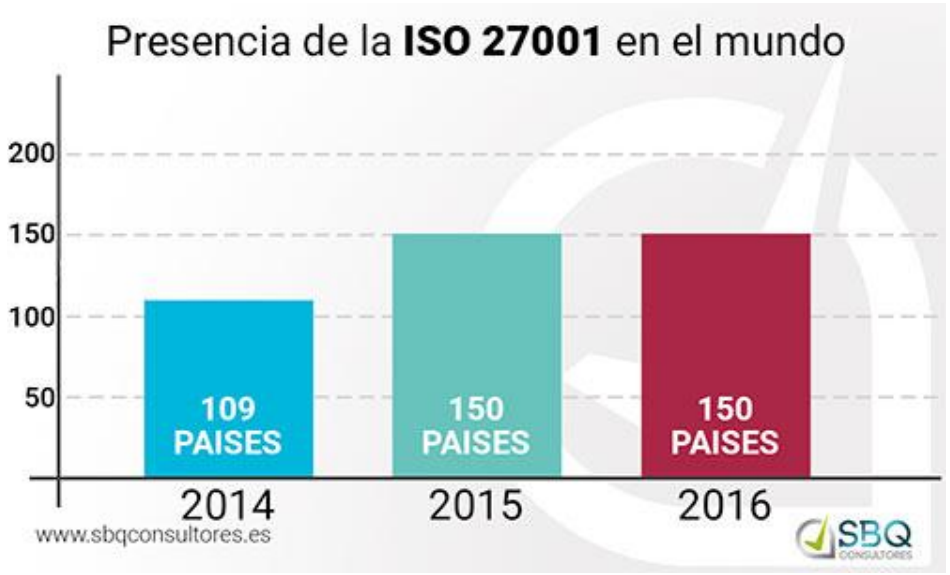


Figura 8.- crecimiento en países de ISO 27001
Fuente.- https://www.sbqconsultores.es/top-10-certificados-normas-iso-nivel-mundial/

CONCLUSIONES

- Como conclusiones para este artículo podemos acotar que las instituciones financieras deberán contar con el apoyo total de alta gerencia con la finalidad de poder lograr los objetivos establecidos al inicio del proyecto; así como también sus funcionarios deberán poner a disposición a su personal quienes serán los dueños y conocedores de los procesos internos críticos donde se maneja información crítica de clientes y que la institución deber resguardar bajo el concepto de tener un impacto reputación y Económico en caso de que esto se materialice.
- Como conclusión para iniciar el proceso de implementación la empresa iniciara por sus procesos críticos identificados así como un inventario de la información clasificada que se maneja en dichos procesos, logrando obtener un enfoque de toda la información que se deberá proteger dentro del alcance establecido para la implementación del SGSI.
- Como conclusión se debe poner a disposición al personal interno para el acompañamiento y realización de talleres de riesgos con la finalidad de evaluar los riesgos absoluto y Residual de sus procesos identificados, logrando identificar los controles que actualmente están mitigando esos riesgos; procediendo a analizar su nivel de efectividad y a su vez un plan de acción que ayudaran a reforzar esos controles aplicados.
- Como conclusión la institución creara un área de seguridad de información, la misma que trabajara en conjunto con el área de auditoría; con la finalidad de hacer cumplir todas las políticas, procesos y procedimientos documentados en el transcurso de la implementación.

BIBLIOGRAFÍA

ACIS.ORG. (2015). *www.acis.org.co*. Obtenido de http://www.acis.org.co/fileadmin/Revista_101/investigaci on.pdf .

Albeiro, J. (2015). http://www.acis.org.co/fileadmin/Revista_110/05inves.

AMBITO, R. (s.f.). *WWW.AUTELSI.COM*. Obtenido de WWW.AUTELSI.COM: https://www.autelsi.es/cms/index.php?option=com_autelsi&pagina=rambito.htm

Candau, J. (2014). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de fefensa frente a las ciberamenazas: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Carmona, E. J. (23 de septiembre de 2013). *Dirección de comunicación Universitaria veracruz.* Obtenido de Revista tecnológica universidad veracruzana: http: //www.uv.mx/universo/535/infgral/infgral_08.html

Celestino, E. (2017). DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS. *Revista de Tecnología Huanco Perú*, pág. 34.

Constante, G. R. (2012). Politica y Seguimiento de la seguridad de la Gestion de segurida de la Información. pág. 22.

Gallardo, S. (2013). Monitoreo y cumplimiento en la seguridad de la información. *ACIS.ORG*.

GARCÍA, D. (07 de SEPTIEMBRE de 2017). *Gestión de Riesgos de Tecnologías de la Información*. Obtenido de EALDE BUSSINESS SCHOOL: http://www.ealde.es/iso-27005-gestion-de-riesgos/

Guerra, Y. P. (2016). La mejora continua de los procesos en una organización. *Revista Empresarial, ICE-FEE-UCSG*, 2.

ISO. (7 de septiembre de 2017). *ISO TOOLS*. Obtenido de Blog especializado en Sistemas de Gestión: https://www.pmg-ssi.com/2017/09/iso-27001-mejorar-las-auditorias-internas-sgssi/

ISO27001. (2016). *https://www.isotools.org/*. Obtenido de ISOTOOLS.

José Gregorio Arévalo Ascanio, R. A. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información.* Revista Tecnura - Universidad Distrital Francisco José de Caldas, Colombia.

LADINO A., M. I., VILLA S., P. A., & LÓPEZ E., A. M. (abril de 2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. *Scientia Et Technica, vol. XVII*, págs. 334-339 .

Mendoza, M. A. (1 de abril de 2015). *¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?* Obtenido de Revista tecnológica ESET: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

Mintic. (2016). articles-5482_G14_Plan de Capacitación, y sensibilización de Seguridad de la Información. *Revista tecnológica vive digital colombia*, 11.

MORALES, J. T. (2014). IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION. *Revista Scielo* , pág. 113.

MOSQUERA, V. (2017). DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA GEOSURVEY DE LA CIUDAD DE LIMA. *Revista de tecnologías de UNIVERSIDAD DE HUÁNUCO*, pág. 13.

Muñoz, R. R. (10 de junio de 2015). IMPLEMENTACIÓN DE SGSI EN LA EMPRESA POLLOS PANCHITO S.A. *REVISTA DE TECNOLOGÍA Y CIENCIA*, pág. 25.

NIEVES, A. C. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001:2013. *REPOSITORIO TECNOLÓGICO DE LA UNIVERSIDAD POLITECNICA GRAN COLOMBIANO*, pág. 12.

Novoa, H. A. (2015). *Metodologías Para el Análisis de Riesgos en los SGSI*. Obtenido de Revista especializada en Ingeniería UNAD V.9: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ROBIN. (19 de 12 de 2014). PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013. *REVISTA UNIVERSIDAD OBERTA CATALUNYA*, pág. 20.

Ronderos, M. F. (6 de junio de 2016). ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE ISO 27001. *Revista tecnica Universitat Oberta de Catalunya*, pág. 19.

Urizarri. (2006). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana*, 12.

VARGAS, C. A. (Abril de 2014). Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. *Revista de tecnologias USCG*, pág. 41.

ZAPATA, F. X. (2014). “IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICANDO ISO 27000". *REVISTA UNIVERSIDAD CENTRAL DEL ECUADOR*.