ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"ESTUDIO DE LAS NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN DE INSTITUCIONES PÚBLICAS: PROPUESTA DE UNA NORMATIVA EN UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR"

LUCÍA VERÓNICA GUEVARA ESPINOSA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de MAGÍSTER EN SEGURIDAD TELEMÁTICA.

RIOBAMBA – ECUADOR

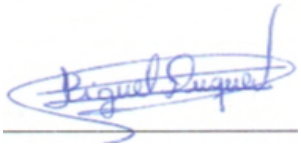
MARZO 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, "**ESTUDIO DE LAS NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN DE INSTITUCIONES PÚBLICAS: PROPUESTA DE UNA NORMATIVA EN UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR",** de responsabilidad de la Sra.: Lucía Verónica Guevara Espinosa ha sido prolijamente revisado y se autoriza su presentación. Tribunal:

Ing. Freddy Proaño. PhD.	_____
PRESIDENTE	FIRMA
Ing. Blanca Hidalgo Ponce. MsC.	_____
DIRECTOR	FIRMA
Dr. Julio Santillán MsC.	_____
MIEMBRO	FIRMA
Ing. Miguel Duque Vaca Mg.	
MIEMBRO	FIRMA

Riobamba, marzo 2018

DERECHOS INTELECTUALES

Yo, Lucía Verónica Guevara Espinosa, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

.

LUCÍA VERÓNICA GUEVARA ESPINOSA

No. Cédula 0603410515

DEDICATORIA

A mi padre, madre y mis hermanos que, sin su ayuda, su apoyo incondicional y su gran amor no podría alcanzar mis sueños.

Y sobre todo a mi hijo la razón de mi vida Luis Alejandro.

Lucy G.

AGRADECIMIENTO

Quiero agradecer primeramente a Dios por darme salud para poder seguir capacitándome y desarrollarme como profesional.

A mi tutora de tesis a la Ing. Blanca Hidalgo por sus sabias orientaciones y pautas, para poder realizar y desarrollar esta tesis y por su apoyo incondicional por último agradezco su confianza y apoyo incondicional al Ing. Miguel Duque y al Doc. Santillán por ser uno de los pilares fundamentales en cumplir con esta nueva etapa de mi vida.

Lucy G.

CONTENIDO

RESUMEN xiii

ABSTRACT xiv

CAPÍTULO I 1

1 INTRODUCCIÓN 1

1.1 Problema de Investigación 2

1.1.1 Planteamiento del problema 2

1.2 Formulación del problema 2

1.3 Sistematización del problema 3

1.4 Justificación de la investigación 3

1.4.1 Justificación teórica 3

1.4.2 Justificación metodológica 4

1.5 Objetivos 5

1.5.1 Objetivo general *5*

1.5.2 Objetivos específicos *5*

1.6 Hipótesis 5

CAPÍTULO II 6

2 MARCO REFERENCIAL 6

2.1 Antecedentes del problema 6

2.2 Bases Teóricas 8

2.3 Cuadro comparativo de la ISO 27001 respecto a las leyes y normativas ecuatorianas 24

2.4 Justificación del caso de estudio en el sector Público 28

CAPÍTULO III 34
3 METODOLOGÍA DE LA INVESTIGACIÓN 34
3.11.1. Indicadores de la variable independiente *39*
3.11.2. Indicadores de la variable dependiente *39*

CAPÍTULO IV 40
4. RESULTADOS Y DISCUSIÓN 40
4.3.5. Especificación del estadístico *42*
4.4.1 Indicadores de la variable independiente *42*
4.4.2 Indicadores de la Variable dependiente *42*
4.5 Comprobación de la Hipótesis General 49

CAPÍTULO V 52
5 PROPUESTA 52
5.1. Introducción 52
5.2 Objetivos 52
5.3 Descripción del escenario sin leyes y normativas 52
5.4. Descripción del escenario con la normativa 55
5.5. Definición del Método 62
5.6. Lineamientos 62
5.7 Estructura del Método 63
5.8 Ventajas y desventajas 64
5.9 Repositorio Digital 64
CONCLUSIONES 67
RECOMENDACIONES 68

ÍNDICE DE TABLAS

Tabla 2-1 Encuesta Latinoamérica de seguridad de información…… 14
Tabla 2-2 Sectores participantes en la iv encuesta latinoamericana de seguridad de información……... 15
Tabla 2-3 Sistematización de riesgo…….…….... 17
Tabla 2-4 Comparativa norma INEN ISO 27001 versus leyes y normas ecuatoriana……. 23
Tabla 2-5 FODA de la dirección de tecnología y comunicación de la ESPOCH……... 26
Tabla 3-1 Operacionalización conceptualización…….…….. 31
Tabla 3-2 Operacionalización metodológica…….…….…. 31
Tabla 4-1 Análisis descriptivo de la encuestas……..... 38
Tabla 4-2 Normas en vigencia……..... 39
Tabla 4-3 Recurso en vigencia…….… 40
Tabla 4-4 Confidencialidad……..... 41
Tabla 4-5 Integridad…….… 43
Tabla 4-6 Disponibilidad…….…….…. 44
Tabla 4-7 Valores porcentuales totales……..…….……..…. 45
Tabla 4-8 Tabla de contingencia…….…. 49
Tabla 5-1 Tabla de vulnerabilidades...…….…… 53
Tabla 5-2 Entregables de la planificación…… 56
Tabla 5-3 Formato propuesto……..…… 59
Tabla 5-4 Letras de identificación para los documentos..... 60
Tabla 5-5 Numeración para las áreas……... 60
Tabla 5-6 Ejemplo de una política…….…….. 62
Tabla 5-7 Ventajas y desventajas……..... 64

ÍNDICE DE FIGURAS

Figura 1-1 Modelo sistema de gestión de seguridad de la información……... 10

Figura 1-2 Modelo de gestión de servicio ITIL v3……..…… 11

Figura 1-3 Modelo buenas prácticas COBIT……..... 12

Figura 4-1 Gráfico estadístico v. independiente normas vigentes……... 39

Figura 4-2 Gráfico estadístico v. independiente recursos vigentes……. 41

Figura 4-3 Gráfico estadístico v. dependiente confidencialidad……. 42

Figura 4-4 Gráfico estadístico v. dependiente integridad…… 43

Figura 4-5 Gráfico estadístico v. dependiente disponibilidad……. 45

Figura 4-6 Valores porcentuales finales ……...….. 46

Figura 4-7 Campana de gauss…….. 51

Figura 5-1 Metodología ISO 27001…….. 55

Figura 5-2 Caracteres del serial propuesto……..... 59

Figura 5-3 Pantalla inicial de repositorio…….. 66

Figura 5-4 Menú de opción de las políticas del DTIC…….. 67

RESUMEN

El objetivo fue reconocer los cambios en el Departamento de Tecnología y Comunicación (DTIC) de la Escuela Superior Politécnica de Chimborazo. ante una propuesta de controles de seguridad de la información. Se realizó el estudio de una propuesta de estándares internacionales, las cuales pueden ser adaptadas a las leyes ecuatorianas vigentes en los últimos años en cuanto al ámbito de seguridad de información, con el objetivo de mejorar la integridad, disponibilidad y confidencialidad de los datos que maneja un centro de informática de una institución de educación superior. La propuesta está diseñada para ser aplicada al DTIC de la Escuela Superior Politécnica de Chimborazo. Al levantar la información inicial nos dio como resultado que su principal problema es el no posee un plan estratégico de seguridad de información, por lo tanto la dirección del departamento ve la necesidad de adoptar una propuesta con políticas y normativas vigentes en el Ecuador las cuales ayude a mejorar su nivel de seguridad de información basado en un estándar internacional ISO 27001 y sus 11 dominios que permiten levantar procesos de alto impacto en el DTIC, de esta manera se garantiza a los usuarios de la institución superior que sus datos están debidamente tratados bajo indicadores de calidad como integridad, confiabilidad y disponibilidad, la implementación de la propuesta en algunos de sus procesos más críticos da a conocer a la dirección del DTIC una mejora del 60% en la seguridad de la información. Se recomienda fomentar la investigación sobre estos temas para incentivar sobre el uso de las normativas y leyes vigentes en nuestro país en instituciones de educación superior.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <SEGURIDAD TELEMÁTICA>, <ISO 27001>, <LEYES DE SEGURIDAD DE LA INFORMACIÓN>, <INDICADORES DE CALIDAD>, <PROCESOS CRÍTICOS>-.

ABSTRACT

The objective was to recognize the changes in the Department of Technology and Communication (DTIC) of the Escuela Superior Politécnica de Chimborazo in the face of a proposal of information security controls. A study of a proposal of international standards was carried out, which can be adapted to the Ecuadorian laws in force in recent years in the field of information security with the aim of improving the integrity, availability and confidentiality of the data handled a computer center of a higher education institution. The proposal is designed to be applied to the DTIC of the Escuela Superior Politécnica de Chimborazo. When the initial information was collected, it turned out that its main problem is not having a strategic information security plan. Therefore, the department's management sees the need to adopt a proposal with policies and regulations in force in Ecuador that will help to improve its level of information security based on an international ISO 27001 standard and its 11 domains that allow high-impact processes to be created in the DTIC. Thus, guaranteeing the users of the higher institution that their data is duly treated under indicators of quality as integrity, reliability and availability. The implementation of the proposal in some of its most critical processes gives the DTIC management a 60% improvement in information security. It is recommended to promote research on these issues to encourage the use of regulations and laws in force in our country in institutions of higher education.

Key words: <TECHNOLOGY AND ENGINEERING SCIENCES>, <TELEMATIC SECURITY>, <ISO 27001>, <INFORMATION SECURITY LAWS>, <QUALITY INDICATORS>, <CRITICAL PROCESSES>.

CAPÍTULO I

1 INTRODUCCIÓN

En la actualidad, toda entidad privada y sobre todo pública deben regirse a las disposiciones gubernamentales las cuales buscan mantener una transparencia y seguridad en la información que manejan ante las autoridades y sobre todo ante los usuarios, de esta manera se garantizará la calidad de servicios que preste la entidad, sin importar su área, ya sea: educativa, salud, financiera, entre otros.

En la presente investigación, partiendo del estudio critico de las normativas vigentes en el Ecuador en torno a la seguridad de la información y con el análisis del comportamiento de las mismas en la Dirección de Tecnología de Información y Comunicación de la Escuela Superior Politécnica de Chimborazo, se pretende establecer las recomendaciones más óptimas para el logro de los lineamientos de políticas de seguridad que garanticen la calidad y transparencia de servicio en el departamento.

Es necesario recalcar lo importante de poseer una normativa de seguridad que contribuya a la calidad de la Información, ya que ayuda a mejorar su imagen, además ganará confianza de sus usuarios y público en general, al estar preparada para una auditoria sea interna o externa.

Para el alcance de los objetivos se consideró establecer las normas vigentes del Ecuador, estándares de seguridad de la información internacional, objetivos del Plan Nacional de Buen Vivir, leyes y acuerdos vigentes en la gestión de servicios del esquema gubernamental de seguridad de la Información.

1.1 Problema de Investigación

1.1.1 Planteamiento del problema

En la actualidad toda institución pública y/o privada (entre ellas la educativa) sustentan sus actividades de decisión y desarrollo en la información, la cual, por su validez y transparencia, requiere que todas y cada de las mismas incluyan normas y procedimientos necesarios que garanticen su calidad y seguridad.

A pesar de que el estado y gobierno ecuatoriano en los últimos años ha establecido y generado normativas y reglamentos que permiten que las instituciones públicas puedan gestionar de forma eficiente y eficaz la seguridad de la información, es frecuente y cotidiano conocer las más diversas manifestaciones de alteración y violación de la misma, así como sus efectos de orden social, económico y político.

Muchas son las causas para la presencia de este panorama de inseguridad e incerteza que sufre la información, el cual puede considerarse que se inicia desde el desconocimiento, incapacidad, errores y alteraciones en la aplicación, hasta una falta de motivación para la implementación de normas y procedimientos para la garantía y seguridad de la información

Por lo que sería de un aporte importante que una institución pública en este caso una institución de educación superior adopte las normativas vigentes en el Ecuador y de esta manera se evalué constantemente su cumplimiento.

1.2 Formulación del problema

El presente estudio pretende mostrar la influencia de las normativas de seguridad de la información y el control para garantizar la calidad de la información en la Dirección de Tecnología de Información y Comunicación de la Escuela Superior Politécnica de Chimborazo, durante el periodo 2016-2017

1.3 Sistematización del problema

La percepción del problema que en primera instancia implica la relación entre normativas y calidad de efectos esperados, requiere de un análisis y respuesta crítica, con el estudio d estas normativas se de una percepción de la validez y confiabilidad basados en los indicadores establecidos para la seguridad de la información como son: integridad, confidencialidad y disponibilidad para responder luego a la interrogante de:
¿Cómo contribuiría la existencia de una normativa de seguridad de la información adaptados a la legislación actual?

1.4 Justificación de la investigación

1.4.1 Justificación teórica

En la actualidad, la información demanda para su uso, así como para la provisión de servicios, procesos y uso de herramientas de tecnológicas, expone tanto a las entidades públicas como a sus funcionarios ya que las mismas herramientas han sido una arma para provocar actos fraudulentos o ilegales en la información y pone en riesgo la misma o inclusive la infraestructura de un institución.

La universidad ecuatoriana como parte de la sociedad en la que se encuentra inmersa en su condición de participante, constructora y testigo del auge tecnológico de las dos últimas décadas y específicamente en el área del procesamiento de datos tiene como responsabilidad la motivación a buscar soluciones, eficientes, y de gran impacto a través de la investigación.

Por estas amenazas que se enfrentan han llevado a que se desarrolle un *documento o normativa* que orientan como tratar en el caso de que se esté produciendo algún tipo de riesgo ya que puede ocasionar serios problemas a los activos que posee la Institución y sobre todo al departamento encargado de resguardar de la información.
La Secretaria de Administración Pública del Ecuador ha creado normativas de seguridad de la información basada en los Acuerdos Ministeriales Nº 804 y Nº 837, como en el plan de gobiernos electrónico las normativas de gestión de servicios y las normas ISO/27001

las cuales muestran el proceso que se llevará para asegurar la información de las entidades públicas.
Así como en el Plan Nacional del buen vivir nos indica que la Instituciones deben impulsar la calidad de seguridad y especialmente en áreas importantes como la producción, educación y salud.

En el área educativa en el Ecuador existes instituciones que manejan normativas de seguridad de la información como la Escuela Superior Policía Nacional quien tiene establecido su normativa sobre seguridad de la información y documentación.

En el esquema gubernamental de seguridad de la información en el artículo 14 y 15 considera la importancia de que exista una normativa que establezca políticas, metodologías de gestión e innovación institucional que mejore la eficiencia, calidad y transparencia en la gestión de seguridad de la Información.
En otros países como en España, en la Universidad de Málaga, posee una normativa en base al crecimiento que ha tenido la Universidad el cual ha mejorado el manejo de seguridad de la Información.

1.4.2 Justificación metodológica

A pesar que desde hace algún tiempo a nivel nacional y gubernamental se ha puesto en evidencia la necesidad de implementación, control y seguimiento de la seguridad de la información en entidades de la administración pública central e institucional, son muy pocas las estrategias para su implementación, es así, que en el año 2014, en el proyecto de su implementación se toman en cuenta únicamente en 88 instituciones gubernamentales de las cual son solo dos de ellas del ámbito educativo: Yachay y la misma Secretaria Superior , Ciencia , tecnología e Innovación

Es decir, que la propuesta por si misma encierra la justificación metodológica que el análisis e interpretación de la situación actual, así como de sus ventajas y limitaciones que serán el sustento para la reinterpretación y generación de los lineamientos de una propuesta que ayude a mejorar la calidad de la seguridad de la información en la Dirección de Tecnología de Información y Comunicación de la Escuela Superior Politécnica de Chimborazo.

1.5 Objetivos

1.5.1 *Objetivo general*

Reconocer los cambios en el DTIC ante una propuesta de controles de seguridad de la información.

1.5.2 *Objetivos específicos*

- Indagar sobre las normativas de seguridad de la información que existen en el Ecuador.
- Analizar dichas normativas de seguridad de la información y comparar con un estándar internacional.
- Proponer al Departamento de tecnología de información y comunicación de la Institución determinada para el estudio posibles normativas que sean adoptadas basándose en su situación actual.
- Presentar un informe de los aspectos encontrados al realizar la evaluación de la normativa en el DTIC.

1.6 Hipótesis

El uso de controles de seguridad de la información producirá mejora en la calidad de servicio en la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo.

CAPÍTULO II

2 MARCO REFERENCIAL

En toda institución el marco legar debe ser el más importante a desarrollar ya que en base a este debe regirse todo su funcionamiento.
Se considera también en el marco legal leyes que ayuden al mejoramiento de la seguridad de la información basados en una norma certificable.

2.1 Antecedentes del problema

2.1.1 Análisis de normativas vigentes en el Ecuador para el proceso de control de las instituciones públicas

Las Instituciones públicas o privadas en el Ecuador han registrado durante los últimos años incidentes de seguridad que afectan la información y que en forma resumida pueden ser: modificaciones no autorizadas de la información, de códigos, de aplicaciones y servicios, sustracción de información almacenada, ejecución de delitos por el mal uso de credenciales de acceso y aun suplementación de identidad vulnerando sistemas y causando graves problemas económicos y el más importante ha perjudicado en la imagen de las Instituciones que han sufrido dichos ataques. Se presenta algunos casos los más renombrados y que han llamado la atención de las autoridades legales y de la ciudadanía.

Delitos Informáticos en el Ecuador

"Las cifras de los ciberataques son alarmantes, según Daniel Molina, experto de la empresa Kaspersky, quien asegura que cerca del 16% de usuarios de la región son víctimas de fraudes informáticos, lo cual suma 60'090.173 detecciones de ataques en el 2014.
En el Ecuador, sostiene, las cifras podrían ir en aumento debido al crecimiento económico del país, que lo convierte en un blanco interesante para los ataques

cibernéticos. "Hay hackers que atacan desde Perú, Colombia o Europa occidental a los bancos ecuatorianos, lo que antes no sucedía, pues se trata es un delito importado". (Universo, 2014)

Caso Consejo Nacional Electoral

Durante el proceso de inscripciones de organización políticas para las elecciones generales del 2013, se dio lugar a varias sospechas que apuntaban a que los registros de afiliación no eran reales debido a que existían supuestamente personas afiliadas siendo que muchas de ellas decían no ser afiliadas al partido político, Este fraude se llevó a descubrir ya que la CNE (Corporación Nacional Electoral) implemento un link en su portal en cual se podía consultar a través de su cedula si se encontraban afiliado o no a algún partido o movimiento político.

"En las elecciones recibimos 1.400 intentos de sabotear el sistema, uno de ellos fue hecho por un gran centro con gran capacidad de procesamiento en el primer mundo (…) tenía una sofisticación tecnológica y tenía enmascaradas sus direcciones. No sabemos aún de dónde es, pero quisieron tumbar el sistema informático del Consejo Nacional Electoral (CNE)" (SurAmerica, 2013).

Caso Municipio de Riobamba

Las Irregularidades en el Municipio de Riobamba se fueron dando desde el 2012 pero el más relevante fue debido a que el alcalde de ese momento Juan Salazar realiza un desvío de 13.33 millones de dólares a cuentas de otras personas asociados con él en el delito, del dinero extraviado se logró recuperar 10 millones quedando el resto sin dar solución de mismo.

"Se incluyeron el informe de Contraloría, peritajes contables, reconocimiento de lugar, pericias a los sistemas informáticos del Banco Central del Ecuador y a los equipos informáticos incautados por la Fiscalía fueron elementos de convicción presentados en la audiencia realizada en la ciudad de Riobamba." (Estado F. G., 2013)

Las empresas o instituciones de cualquier sector (bancos, telecomunicaciones, gobiernos o educación, entre otros) del país sean estos públicas o privadas posee una Dirección de

Tecnología de la Información y Comunicación, las cuales son las designadas en la seguridad de la información que maneja la Institución.
Una vez analizado algunos antecedentes, Leyes a nivel Internacional y Nacional se puede apreciar que:

- El Ecuador es un país que ha dado la importancia a la seguridad de la información en las instituciones públicas y privadas, por los ataques que han sucedido en los últimos años.
- Las leyes que posee el Ecuador hacen referencia a la seguridad de la información en los últimos años sin embargo no se ha realizado una actualización de las mismas.

En el Ecuador en el año 2011 las Normas Técnicas Ecuatorianas INEN aprobadas por el Subcomité Técnico de Tecnologías de la Información – TIC regulariza el proceso de **seguridad** con la norma NTE INEN ISO IEC 27001.

2.2 Bases Teóricas

Norma ISO

Al tratar con la norma ISO (Organización Internacional de Estandarización) se recoge un extenso números de normas dentro de la familia ISO entre ella tenemos la familia de la 27000 dentro de la misma existen varias numeraciones las mismas que ayudan a definir algún cambio entre la una o la otra según las necesidades existentes.

ISO 27001

Es la norma principal de toda la serie ya que incluye todos los requisitos del Sistema de Gestión de Seguridad de la Información en las organizaciones. En el Anexo A se enumeran los objetivos de control y los análisis que desarrolla la norma ISO27001 para que se puedan seleccionar las empresas durante el progreso de sus Sistemas de Gestión de Seguridad de la Información. La empresa podrá argumentar el hecho de no aplicar los controles que no se encuentren implementados ya que no es obligatorio, además está

diseñada con un enfoque preciso: si desea crear la estructura de la seguridad de la información en su organización y definir su encuadre.

ISO 27002

En este caso la norma ISO 27002 establece un catálogo de buenas prácticas que determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en base a la situación actual de una empresa o institución.

Principal diferencia entre ISO 27001 y 27002

Ante todo, no es posible obtener la certificación ISO 27002 porque no es una norma de gestión. ¿Qué significa una norma de gestión? Significa que este tipo de norma se define cómo ejecutar un sistema; y en el caso de la ISO 27001, esta norma define el sistema de gestión de seguridad de la información des cual nace estos controles. Por lo tanto, la certificación en ISO 27001 sí es posible.

Para la ISO 27001 están definidos dominios que abarcan los aspectos más importantes de seguridad de la información. (Darwin, 2015)

Para la norma ISO 27001 preservar la confidencialidad, integridad y disponibilidad en su información y que esta mejore su calidad es lo más importante, además su principal objetivo es la mejora continua. (www.ccia.es, 2012)

Se adopta el modelo Plan-Do-Check-Act para todos los procesos de la organización

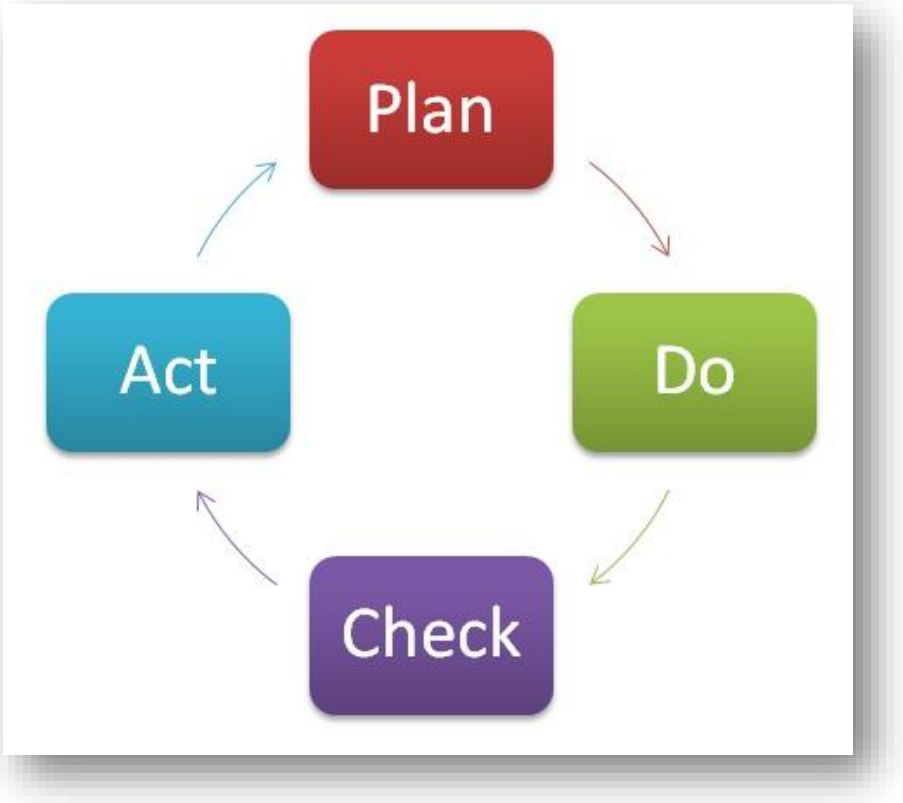


Figura 1-1 Modelo Sistema de Gestión de Seguridad de Información,
Fuente: (Jaramillo, 2014).

Ventajas de las normas ISO

En base a esta finalidad y objetivo inicial y debido al gran prestigio y enorme seguimiento alcanzado, las normas ISO suponen importantes beneficios para las empresas, compañías, instituciones y organizaciones en general (Freddy, 2015):

- Proporcionan elementos para que una organización puede alcanzar y mantener mayores niveles de calidad en el producto o servicio.
- Permite a las empresas reducir costos, conseguir más rentabilidad y aumentar los niveles de productividad.
- Constituye uno de los medios más eficaces para conseguir ventaja competitiva.
- Reducir rechazos o incidencias en la producción o en la prestación de servicios.
- Implementar procesos de mejora continua.
- Conseguir un mayor y mejor acceso a grandes clientes y administraciones y a los mercados internacionales.

Los beneficios sobrepasan el ámbito de las empresas y administraciones y sus clientes, que se ven favorecidos por un mejor servicio, alcanzando también a los gobiernos, que gracias a las normas ISO pueden:

- Asegurarse de que los bienes y servicios cumplen con los requisitos obligatorios relacionados con la calidad, la seguridad o el medio ambiente, entre otras cuestiones.
- Controlar el comercio exterior con otros países.

ITIL

Está destinado a las mejores prácticas sobre gestión de seguridad de información aunque ITIL se basa en la alta calidad de Servicio que puede proveer una institución, además esta consiente de las necesidades de la organización y de los usuarios, a través de las leyes y reglamentos en base a su eficacia y eficiencia, como son:

1. Calidad en los servicios
2. Aumentar la eficacia
3. Reducir los riesgos asociados a los servicios. (Van Bon, Jan, 2010)

La Norma ISO 27001 a diferencia de ITIL tiene un enfoque hacia la gestión de la seguridad a través de la implementación o mejorar de una normativa, sin embargo ambos marcos toman en cuenta la importancia que implica los riesgos para cumplir los objetivos que se desea alcanzar.

En la familia de la ISO 27001 cuenta con los controles A.10.2 Gestión de la presentación de servicios por terceras personas, A.10.2.1 Prestación de servicios, A.10.2.2 Supervisión de revisión de los servicios prestados por terceros, A.10.2.3 Gestión del cambio en los servicios prestados por terceros

Sin embargo estos controles hacen énfasis en la seguridad de la información respectos a la gestión de servicios.

Lo más importante para ITIL está enfocado en las fases de operación la misma que permite alcanzar el máximo en tiempo versus costo de esta manera los procesos sean eficaces y eficientes y que este siempre centralizada la información y que el servicio sea

fiable, consistente y de alta calidad y sobre todo de un costo aceptable. (ECONOCOM, 2012)

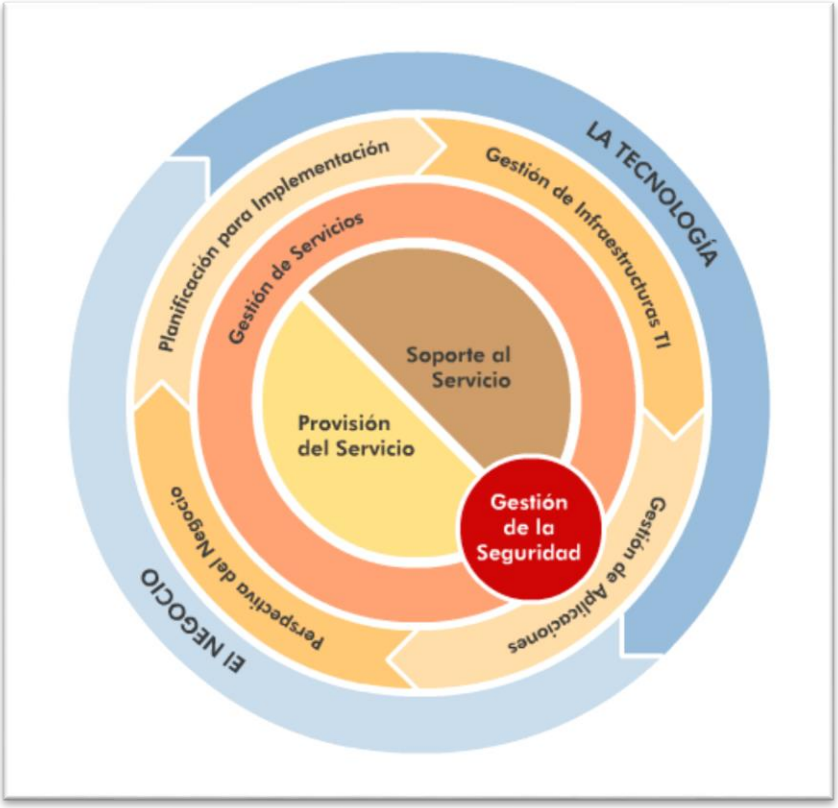


Figura 1-2 Modelo de gestión de servicios ITIL V3
Fuente: (ECONOCOM, 2012)

Una diferencia a resaltar entre ITIL e ISO 27001 consiste en el tratamiento de los incidentes. Para ITIL un incidente es: "cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o reducción de calidad del mismo" (OASIATIS, 2013).

Mientras que la norma ISO 27001 define un incidente de seguridad como: uno o varios eventos no deseados que ocurren en sistema, servicio o red que indican una violación de la política de la seguridad o falta de un control, llegado a esto a comprometer a la seguridad de la información (27001, 2014)

COBIT

Una de las principales características de COBIT es de entregar las responsabilidades a la gerencia para salvaguardar todos los activos de la institución de esta manera la gerencia mantendrá un control interno, por otro lado COBIT optimiza las inversiones que sean realizadas en TI para entregar un mejor servicio de manera que satisfaga los requerimientos de servicios. Teniendo como principales controles:

1. Orientado al negocio
2. Orientado a procesos.
3. Basado en Controles.
4. Impulsado por la mediación (Vargas, 2013).

COBIT tiene un gran beneficio en cuanto a buenas prácticas y a sus procesos ya que se encuentran enfocados en el control y no en la ejecución, es decir ayudan a optimizar las facilidades que posee las tecnologías de información y que sean aplicadas al negocio (BITCOMPANY, 2013)

Figura 1-3 Modelo buenas practicas COBIT.

Fuente: (BITCOMPANY, 2013)

Una vez estudiado el contenido de COBIT se puede emitir algunos criterios sobre las principales diferencias con la norma ISO 27001

- ENFOQUE: COBIT está orientado al negocio y al gobierno de TI, mientras que la ISO 27001 se centra en el establecimiento de controles se seguridad seleccionados a partir de un proceso de gestión de riesgos.
- OBJETIVO: COBIT busca una solución integrada que ayuda a las organizaciones a establecer un gobierno de TI. La ISO 27001 permite a las organizaciones la creación, mantenimiento y mejora de un sistema de gestión de seguridad de la información.
- ESTRUCTURA: COBIT posee 34 procesos agrupados en 4 dominios. La ISO 27001 posee 11 dominios de 39 objetivos de control y 133 controles.

La tabla 2.1 presenta un breve mapeo éntrelos objetivos de control definidos en los marcos investigados y la norma ISO 27001.

Tabla 2-1. Cuadro comparativo de los marcos internacionales de seguridad de información

	ITIL	COBIT	ISO 27001
Objetivos en la seguridad de la información	Mejores prácticas para la gestión y soporte de servicios de TI	Está orientado al negocio y al gobierno TI	Establece controles de seguridad seleccionados a partir de un proceso de gestión de riesgo
Numero de dominios para procesos de seguridad de información	No crea procesos	4	11
Ayuda a respaldar procesos del negocio de una organización	Si	Si	Si
Estandariza los procesos del negocio de una organización	No	Si	Si
Importancia a los riesgos de la organización para cumplir los objetivos deseados	Si	Si	Si
Seguridad de la información respecto a gestión, supervisión y revisión de servicios	No	Si	Si
Responsabilidades y procedimientos frente a	No	No	Si

incidentes de seguridad de información			
Comunica contantemente a la gerencia sobre los proceso realizados	No	No	Si
Posee gestión de calidad	No	Si	Si
Gestiona continuamente los cambios realizados en los procesos realizados	No	Si	Si
Gestiona servicios a terceras personas	No	No	Si
Monitorea y evalúa el control interno de la organización	No	No	Si
Proporciona gobiernos de TI	No	Si	Parcialmente
Gestiona los ambientes físicos como parte del riesgo existente	No	No	Si
Educa y entrena a los usuarios	No	Si	Si
Garantiza la continuidad del negocio mediante procesos o normativas	No	Si	Si
Gestiona Proyectos de la organización	No	Si	No

Fuente: Lucía Guevara, 2017

Una de las ventajas más notables de la norma ISO 27001 es certificable, lo que incrementa el prestigio y la confianza de usuarios y clientes.

Además, que la normas ISO 27001 define su propio proceso de gestión de riesgo y un conjunto de controles de seguridad.

Seguridad de información en Latinoamérica

Latinoamérica por la creciente delincuencia a nivel informático y siendo que aún posee desventaja sobre seguridad de la información por el nivel de conocimiento, busca la manera de ir dando a conocer los tipos de ataques que en la actualidad se van dando para ellos existen algunas organizaciones o empresas que han unido su conocimiento con el objetivo de fortalecer el conocimiento de seguridad de la información en América Latina y el Caribe.

Organización de estados americanos (OEA)

En el 2004 todos los países miembros de la OEA fortalecieron el dominio informático sea más estable seguro, con el objetivo de combatir los delitos cibernéticos de esta manera resguardar el desarrollo económico y social.

Por unanimidad de los estados miembros promovieron la cooperación entre el sector público y privado y el sector académico ya que la información que se maneja en estos sectores afecta a la mayor parte de los usuarios. (Symantec, 2014)

Equipo de respuestas a incidentes de seguridad (CSIRT)

Una vez que los estados miembros de la OEA analizaron la necesidad urgente de fortalecer la seguridad de la información por los repetidos ataques cibernéticos se crea para cada país el CSIRT el cual posee políticas y técnicas para dar respuesta a casos emergente ante la delincuencia cibernética.

La OEA indica que se deben crear redes y software que faciliten el intercambio de prácticas óptimas y un alto conocimiento profesional dentro de los estados miembros por lo que es necesario que tengan CSIRT robustos y que desarrollen la capacidad de generar seguridad en recursos financieros, salud y académicos. (Trendmicro, 2012).

VI Encuesta latinoamericana de seguridad de la información

Como objetivo es entender cuanto es el aporte que brindan los países participantes par que a través de su experiencia se pueda dar un mejoramiento al ejercicio de proteger los activos de información más críticos de las organizaciones o instituciones.

Los resultados de estas encuestas que aportaron países como Argentina, Colombia, Perú, Uruguay entre otros, permiten tener una visión más clara acerca de la seguridad de la información, a continuación, se muestra la tabla de comparación de las encuestas realizadas desde el año 2009 hasta el 2014 realizadas por expertos en seguridad de la información en América Latina, con el fin de apreciar el porcentaje de los países en cuanto acaso reportados de seguridad de la información.

Tabla 2-2: IV Encuesta Latinoamericana de Seguridad de Información

PAISES PARTICIPANTES	2009	2010	2011	2012	2013	2014
Argentina	6,50%	12,76%	17%	23.33%	20.4%	3,7%
Chile	8,80%	0%	2%	2,50%	0%	2,6%
Colombia	65,40%	58,90%	60%	42,22%	67,5%	69,7%
Costa Rica	0%	0%	0%	7,50%	1,7%	1,1%
México	12,20%	10,30%	5%	5%	1,3%	2,2%
Uruguay	7,10%	6,07%	3%	1,39%	0,8%	0,4%
Paraguay	0%	6,38%	0%	2,80%	1,3%	1,1%
Perú	0%	0%	0%	15%	1,7%	4,1%
Otros países: Aruba, Bolivia, Brasil, Ecuador, El Salvador, España, Honduras, Panamá, República Dominicana, Venezuela	0%	5,50%	13%	2,78%	5,40%	15,1%

Fuente: (Jeimy J. Cano, 2014).

En base a la tabla anterior podemos dar algunas conclusiones sobre la seguridad de la información en Latinoamérica.

- El país con más participación es Colombia.
- El Ecuador tienen un mayor interés en el año 2011 y el año 2014 en donde su participación incrementa considerablemente con respecto a los otros años, ya sea que a partir de estos años se han producido mayores ataques a la información de entidades públicas y privadas, por lo que más profesionales son participes.

En la siguiente tabla se presentan en las encuestas los sectores participantes en las VI encuestas de seguridad de la información.

Tabla 2-2: Sectores participantes en la IV encuesta latinoamericana de seguridad de información

SECTORES PARTICPANTES	2011	2012	2013	2014
Bancos	6,76	5,26	7,80	19,22
Telecomunicaciones	4,34	3,64	2,22	1,94
Salud	3,20	3,34	3,33	3,99
Educación, Gobierno/Sector Público	13,60	12,76	16,2	10,00

Otros Sectores: Agropecuario, Logísticos, Farmacéutico, Transporte	0	18,25	16,95	17,49

Fuente: (Jeimy J. Cano, 2014).

En base a la tabla anterior podemos dar algunas conclusiones sobre los sectores que participan.

- Se puede visualizar que la mayor participación es en el sector público y dentro de esta la educación, pudiendo asumir que los gobiernos poseen mayor cantidad de ataques a las entidades públicas o que se encuentren relacionadas, por lo que los gobiernos obligan a implementar leyes y normativas de controles de seguridad de información las cuales se encuentran basadas en las normas internacionales como ISO, COBIT, ITIL entre otros, además se dan a conocer herramientas y nuevas prácticas para la seguridad de la información además de la concientización de la importancia de la misma en todas los sectores en empresas u organizaciones públicas y privadas.
- La VI encuestas de seguridad de la información muestra la importancia de identificar las vulnerabilidades de todas las empresas y por consiguiente deduce que a nivel de Latinoamérica están aceptando de manera más consiente de los riesgos que puede conducir el no tener normas y leyes que respalden la información.

Seguridad de la información y el marco legal en el Ecuador

El Ecuador ha visualizado a través del tiempo claros ejemplos de ataques a la seguridad de la información Instituciones como: bancos, ministerios e incluso el gobierno por lo se han creado diferentes leyes y reglamentos que aseguran la información.

Constitución política del Ecuador

En la Constitución del Ecuador no existe claramente un tema que detalle a profundidad de la seguridad de información, pero existen dos Artículos que son importantes mencionar ya que abordan la temática.

"*Art. 18. Todas las personas, e forma individual o colectiva, tiene derecho a:*

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en caso expresamente establecidos por la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información". (Ecuador, 2008).

"*Art. 389. El estado garantizará el derecho de las personas, las colectividades y la naturaleza a la protección frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objeto de minimizar la condición de vulnerabilidad"* (Ecuador, 2008).

Aclarando que los desastres de *origen antrópico* hacen referencia a aquellos incidentes de seguridad que puedan ser ocasionados por personas.

Normas de control interno de la Contraloría General del Estado

Para que la seguridad de información se gestione con transparencia y consistencia en cualquier Institución, es importante siempre considerar los riesgos que se puede generar en cualquier Institución y en sentido establece las *"Normas de control interno para las entidades, organismos del sector público y de derecho privado."*

Las mismas que en lo referente a seguridad de información se detallan el riesgo y se sistematiza a continuación:

Tabla 2-3: Sistematización de riesgo.

Código	Título de la norma	Concepción
300	Evaluación de Riesgos	*La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a*

		los que está expuesta la organización para el logro de sus objetivos" (Estado C. G., 2011).
300-01	Identificación de riesgos	*Los directivos de la entidad del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizará, el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos"* (Estado C. G., 2011)
300-02	Plan de mitigación de riesgos	*Los directivos de la entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos"* (Estado C. G., 2011).
300-03	Valoración de riesgos	*La valoración del riesgo estará ligada a obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, este análisis le permitirá a las servidoras y servidores reflexionar sobre cómo los riesgos pueden afectar el logro de sus objetivos, realizando un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar..."* (Estado C. G., 2011).
300-04	Respuesta de riesgo	*Los directivos de la entidad identificarán las opciones de respuestas al riesgo, considerando la probabilidad y el impacto en relación con la tolerancia al riesgo y su relación costo/beneficio.."* (Estado C. G., 2011).

Fuente: (Estado C. G., 2011).

Es claro que se podría relacionar con la ISO 27001, debido a que ambas abarcan la gestión de riesgos.

Las Normas de control interno también hacer referencia explícita a la seguridad de información en el siguiente artículo.

"*Art. 410-10 Seguridad de tecnología de Información.- La Unidad de tecnología de información, establecerá mecanismos que protejan en salvaguarden contra perdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medida:*

1. *Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de información y en especial a las áreas de: servicios, desarrollo y bibliotecas".*
2. *Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.*
3. *En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.*
4. *Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.*
5. *Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.*
6. *Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada , entre otros;*
7. *Consideración y disposición de sitios de procesamiento alternativos.*
8. *Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.* (Estado C. G., 2011) .

Ley de comercio electrónico, firmas electrónicas y mensajes de datos

La ley de comercio electrónico regula el uso de sistemas de información y redes electrónicas, como en el internet, desarrollo de comercio tanto en el sector público y privado los puntos más importantes en estas leyes son:

1. Titulo 1: De los mensajes

2. Titulo 2: De las firmas electrónicas, certificados de firma electrónica, entidades de certificación de información, de regulación de entidades de certificación debidamente acreditadas.
3. Titulo 3: De los servicios electrónicos, la contratación electrónica y telemática.
4. Titulo 4: de la prueba y notificación electrónica.
5. Título 5: De las infracciones informáticas (Congreso Nacional, 2002)

Ley orgánica de transparencia y acceso a la información pública

El objetivo principal de esta norma es el derecho de las personas a estar informados sobre los procesos de gestión que mantenga cualquier Institución pública ecuatoriana y además de asegurar la información para que no sea mal utilizada, a través de sus artículos.

"*Art. 10. Custodia de la información.- Es responsabilidad de las instituciones públicas y demás entes señalados en el artículo 1 de la Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción."* (Nacional C. , 2013).

"Art. 5. Información Pública.- Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de la instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren baso su responsabilidad o se haya producido con recursos del Estado." (Nacional C. , 2013).

"Art. 6. Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimo y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de las Constitución de Política de la Republica" (Nacional C. , 2013)

Indicando en el artículo 23 y 24 sobre el derecho a las personas de mantener su vida privada y no atentar a la integridad de la persona.

Ley del sistema nacional de registros de datos públicos.

Esta ley considera como principal objetivo garantizar que la información se maneje de forma eficiente y eficazmente de la Instituciones Públicas que manejen recursos públicos como indica en uno de sus artículos.

"Art. 26. Seguridad.- Toda Base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impida la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar l información pública" (Nacional A. , 2010).

Este artículo hace referencia a la seguridad de la información, gestión de respaldos, planes de contingencia y la protección para robos o alteración de información.

Ley de protección a la intimidad y a los datos personales.

El propósito de esta ley es complementar a la ley anteriormente explicada ya que los datos personales busca la protección a la intimidad que se encuentren almacenados en lugares físicos y digitales.

En esta ley se estipulan los siguientes aspectos los cuales deben estar debidamente justificados.

- Se permitirá la recolección de información personal siempre y cuando estén claramente especificadas las razones de su uso.
- Se prevé una organización como órgano de control de datos personales de esta manera será únicamente el que controles toda la información personal para que no exista abuso de la misma.

Los datos Públicos necesita ser complementada con algún a normativa que considere la protección de datos personales, como se mencionó, la norma ISO 27001 establece un control denominado A.15.1.4 protección de datos y privacidad de la información de carácter personal, que podría ser considerado en la elaboración de una futura ley de protección de datos personales.

Una vez analizado la leyes y normativas del Ecuador citadas anteriormente en sus artículos la mayoría de estas obligan a implementar controles de seguridad de información en base a sus criterios de calidad, los mismo que darán como resultado que las instituciones públicas con sus propias normativas en base a su realidad las mismas que podrán ser presentadas de forma transparente ante la ciudadanía.

La ISO 27001 posee controles de seguridad de información internacionales y nacionales los cuales se han compaginado con las normas Ecuatorianas citadas anteriormente, a continuación se muestra una tabla comparativa de la norma con respecto a dichas leyes.

La norma NTE INEN-ISO/IEC 27001

Esta norma habla sobre sistemas de gestión que proveen un modelo, además incorpora las características sobre las cuales los expertos en el campo han llegado a un consenso de que se trata tecnología de punta internacional. “La norma cuenta con un comité experto dedicado al desarrollo de normas sobre sistema de gestión para la seguridad de la información, también conocidas como familia de normas del sistema de gestión de la seguridad de la información (SGSI)” según (INEN, 2016). Mediante el uso de la familia de normas SGSI, las organizaciones pueden desarrollar e implementar un marco de referencia para gestionar la seguridad de sus activos de la información y preparar una evaluación independiente de su SGSI, aplicada a la protección de la información tales como información financiera, propiedad intelectual y detalle de empleados o información confiada a ellos por clientes o por terceros.

2.3 Cuadro comparativo de la ISO 27001 respecto a las leyes y normativas ecuatorianas

Tabla 2-4: Tabla comparativa norma ISO 27001 versus leyes y normas Ecuatorianas

Ley o Normativa Ecuatoriana	Articulo	Controles de la norma ISO 27001	Posibles controles para complementar la ley o normativa
Constitución política del Ecuador	Articulo 389	A.14.1.2 Continuidad del negocio y evaluación de riesgos.	
Normas de Control Interno de La Contraloría General del Estado	Articulo 300 Evaluación del Riesgo identificación de riesgos, Plan de mitigación de riesgos Valoración de riesgos Respuestas de riesgos	A.14.1.2 Continuidad del negocio y evaluación de riesgos.	
	Artículo 410-10 Seguridad de tecnología de información	A.8.2.2 Educación, formación y concienciación sobre la seguridad de la información. A.9.1.1 Perímetro de seguridad física A.9.1.2 Controles de acceso físico A.9.1.3 Seguridad de oficinas, recintos e instalaciones A.9.1.4 Protección contra amenazas externas y ambientales A.9.1.5 Trabajo en áreas seguras A.9.2.2 Servicios de suministro A.10.5.1 Respaldo de la información A.10.8.3 Medios físicos de transporte	A.7.1 Responsabilidad por los activos A.7.1.1 Inventario de activos A.8.2.3 Proceso disciplinario A.8.3.3 Retiro de los derechos de acceso A.10.1.1 Documentación de los procedimientos de operación A.10.1.2 Gestión del cambio A.10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación A.11.4.5 Separación en las redes A.12.6 Gestión de la vulnerabilidad técnica

Ley o Normativa Ecuatoriana	Articulo	Controles de la norma ISO 27001	Posibles controles para complementar la ley o normativa y propuesta del proyecto de tesis
		A.12.5.1 Procedimientos de control de cambios. A.12.6.1 Control de la vulnerabilidades técnicas A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.	A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información A.15.1.3 Protección de los registros de la organización.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos.	Titulo 1,2,3,4	A.10.9.1 Comercio Electrónico A.10.9.2 Transacciones en línea A.10.9.3 Información públicamente disponible	A.11.4.6. Control de conexión a las redes A.12.3 Controles criptográficos. A.15.1 Cumplimientos de los requisitos legales. A.15.1.4 protección de los datos y privacidad de la información personal. A.15.1.6 Reglamentación de los controles criptográficos.
	Titulo 5	A.8.2.3 proceso Disciplinario	A.13.2.3 Recolección de evidencias.

Ley o Normativa Ecuatoriana	Articulo	Controles de la norma ISO 27001	Posibles controles para complementar la ley o normativa y propuesta del proyecto de tesis
Ley orgánica de transparencia y Acceso a la información Pública.	Articulo 5 Información Pública Articulo 6 Información confidencial Articulo 10 Custodia de la información	Se direcciona a la aplicación de una norma técnica para la protección de información.	A.15.1.4 Protección de datos y privacidad de la información de carácter personal
Ley del Sistema Nacional de Registros de datos Públicos	Articulo 26 Seguridad	A.10.5.1 Respaldo de la información A.14.1.2 Continuidad del negocio y evaluación de riesgos. A.5.1.1 Documento de la política de la seguridad de la información	A.9 Seguridad física y del entorno A.14 Gestión de la continuidad del negocio A.15.1.13 Protección de los registros de la organización

Fuente: Lucía Guevara, 2017

2.4 Justificación del caso de estudio en el sector Público

En base al análisis realizado anteriormente podemos evidenciar que las instituciones públicas en el Ecuador han registrado una serie de incidentes de seguridad de la información en los últimos años, que ha causado graves perjuicios económicos además que han perdido la confianza de la ciudadanía en el manejo de recursos y la protección de los datos personales de los ciudadanos, por esta razón se menciona casos anteriormente de los casos ocurrido durante los últimos años los cuales se muestra como se ha perdido la imagen de estas instituciones públicas.

Por tal motivo es importante que los departamentos de tecnología de las instituciones públicas adopten las leyes y normativas vigentes que crean en los gobiernos para que de esta manera respalden este activo que es la información, además que la pertenecer al estado están en la obligación de cumplir con lo solicitado por el mismo.

En el Ecuador existen instituciones con la certificación ISO 27001 como lo son: la Corporación Nacional de telecomunicaciones desde el 2015 (CNT, 2015), La Secretaria Nacional de la Administración Pública desde 2014 (SNAP, 2014), Escuela Superior Politécnica del Litoral trabaja en su departamento de tecnología con controles de seguridad de la información bajo la norma ISO 27001 (ESPOL, 2015)

2.4.1 *Justificación de la selección de la Dirección de tecnología y comunicación de la Escuela Superior Politécnica De Chimborazo*

La dirección de tecnología de información y comunicación de la Escuela Superior Politécnica de Chimborazo la misma que se encuentra administrada actualmente por su director el Ing. Gustavo Hidalgo ha brindado las facilidades necesarias para la realización ante el presente proyecto de investigación además de demostrar un importante interés en el misma ya que el DTIC no cuenta con ningún tipo de control de seguridad de la información estandarizado en ninguna ley vigente en el Ecuador, únicamente de ciertos requerimiento que solicita la ESPOCH para auditorias administrativas más no técnicas. Por lo que considera muy importante el planteamiento de una propuesta que le permita

dar un punto de inicio a la seguridad de la información, y el cumplimiento de las leyes ecuatorianas.

La situación actual del DTIC se verá reflejada en el análisis FODA ya que esta herramienta permitirá identificar las fortalezas, oportunidad, debilidades y amenazas que afectan al departamento y de esta se obtendrá una visión más clara de la situación actual del objeto de estudio, para alcanzar los objetivos planteados.

Tabla 2-5. FODA de la Dirección de Tecnología y Comunicación de la ESPOCH.

FODA de seguridad de la Información de la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo	
Fortalezas	**Oportunidades**
• El Director del DTIC no depende de otras direcciones para la toma de decisiones, es decir las iniciativas con respecto a la infraestructura tecnológica dependerá de un previo análisis de requerimientos los cuales garantizan el mejoramiento de dicha infraestructura. • Toda información se encuentra centralizada en el DTIC por lo cual resulta más sencillo protegerla mediante el uso de controles de seguridad. • En la actualidad están establecidos algunos controles de seguridad física.	• Capacitación al personal sobre la seguridad de información • Cumplir con las normativas y leyes establecidas para la protección de la información. • Definición de procedimientos formales los cuales garanticen la seguridad de la información en el DTIC.
Debilidades	**Amenazas**
• Falta de capacitación actualizada del personal con respecto a seguridad de información. • Falta de controles de seguridad en la información que se maneja.	• Ataques internos y externos a la institución que afecten a la integridad, disponibilidad y confidencialidad de la información.

• Falta de procesos de documentación de los sistemas.	• Daños provocados por actividades de terceros • Fuga o revelación de información • Incumplimiento de leyes.

Fuente: Lucía Guevara, 2017

2.4.2 Conclusión del FODA

En el Ecuador existen una gran variedad de instituciones públicas las mismas que están expuestas a amenazas de seguridad que a lo largo de estos años se han visto afectadas económicamente y en la imagen de la empresa por esta razón el gobierno ha implementado leyes y normativas las cuales ayudan a estas empresas a mejorar su nivel de seguridad de información la ESPOCH siendo una institución pública está obligada a cumplir con dichas normativas para su servicio y transparencia de la información.

Las debilidades identificadas pueden ser cubiertas mediante el uso de controles basados en la norma ISO 27001

En la siguiente tabla se muestra que controles que deberían ser usados para solventar las debilidades encontradas en el departamento.

Tabla 2-6 Comparación de las debilidades encontradas en base a controles de la ISO 27001

Debilidades	Controles
Falta de capacitación de los funcionarios del DTIC en los aspectos relacionados con seguridad de la información.	A.5.2.2 Concientización, formación y capacitación
Falta de políticas	A.5.1.1 Documento de política de seguridad de la información
Falta de controles de seguridad que se maneja	A.5.1.2 Revisión de la política de seguridad de la información
Falta de compromiso de la dirección para la seguridad de la información	A.6.1.1. La dirección debe apoyar activamente el uso de la seguridad de información mediante el uso de las políticas.

Determinar un proceso de respaldo de información	A.10.5.1 Respaldo de la información A.15.1.3 Protección de los registros de la organización
Falta de una documentación estandarizada de los sistemas y actualizaciones	A.7.1.1 Inventario de activos A.12.4.1 Control de software operativo A.12.5.1Procedimiento de control de cambio

Fuente: Lucía Guevara, 2017

De igual manera para las amenazas identificadas se puede implementar los controles específicos tales como se muestra en la tabla.

Tabla 2-7 Comparación de las amenazas encontradas en base a controles de la ISO 27001

Amenazas	Controles
Ataques internos y externos a la Institución que afecten a la integridad disponibilidad y confiabilidad de la información	A.5.2.2 Concientización, formación y capacitación A.5.1.1 Documento de política de seguridad de la información A.5.1.2 revisión de la política de seguridad de la información A.10.4.1 Controles contra códigos maliciosos A.12.2.1. Validación de los datos de entrada A.12.2.2. Control de procesamiento interno A.12.6.1. Control de la vulnerabilidades técnicas
Acceso físico no autorizado a las instalaciones de la institución	A.9.1.1 Perímetro de la seguridad física A.9.1.3 Seguridad de oficinas, recintos e instalaciones.
Daños provocados por actividad de terceros	A.10.2.1 Prestación de servicio A.10.2.2 Monitoreo y revisión de los servicios por terceros.
Falla en los equipos	A.9.2.2 Servicios de suministro A.9.2.3 Seguridad del cableado A.9.2.4 Mantenimiento de los equipos
Fuga o revelación de Información	A.9.2.1 Ubicación y protección de los equipos A.12.5.4 Fuga de información
Incumplimiento de leyes	A.15.1.1. Identificación de la ley aplicable

	A.15.1.2 derechos de propiedad intelectual A.15.1.4 Protección de los datos y privacidad de la información personal.

Fuente: Lucía Guevara, 2017

El análisis FODA permitió identificar de manera general algunas oportunidades que pueden ser explotadas mediante la implementación de una Normativa claramente establecida que permitirán a la dirección de tecnología de la información y comunicación implementar, mantener y mejorar la seguridad de la información.

2.4.3 Análisis de vulnerabilidades

Una vez analizado el FODA del departamento para determinar la situación actual del mismo es importante considerar las vulnerabilidades lógicas y físicas del DTIC de la Escuela Superior Politécnica de Chimborazo.

En la siguiente tabla se determina que vulnerabilidades lógicas que fueron encontradas:

Tabla 2-8 Vulnerabilidades lógicas encontradas en el DTIC.

Proceso realizado	Vulnerabilidad
Recopilación de la información	Información desactualizada
	Nombres de dominios relacionados con IP´s Publicas
	Nombres de dominios relacionados con IP´s privadas
Mapeo de la red	Información visible de puertos abiertos
	Información de los servicios
	Información de los sistemas operativos
	Direcciones IP visibles durante traceroute
	Se muestra información en el switch capa 3
Seguridad de las contraseñas	No existe asignación de contraseñas a nivel BIOS
	Única contraseña para sistemas y servicios
	Falta de control en las contraseñas para los accesos
	Contraseñas permanentes en equipos de comunicación
Seguridad del Router	Se muestran puertos abiertos
	Servicio http permanentemente habilitados

Fuente: Lucía Guevara. 2017

En la siguiente tabla se muestra las vulnerabilidades físicas encontradas

Tabla 2-9 Vulnerabilidades físicas encontradas en el DTIC.

Proceso realizado	Vulnerabilidad
Seguridad Física	Espacio insuficiente en el interior y exterior dela sala de los servidores
	La ubicación física de los servidores debería ser diferente
	No existe un plan de continuidad en caso de que exista un desastre.

Fuente: Lucía Guevara, 2017

CAPÍTULO III

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño de estudio

La presente investigación es cuasi experimental, ya que se pretende dar a conocer las normativas y leyes vigentes en el Ecuador, las cuales permitan mejorar la seguridad de la información en el DTIC de la Escuela Superior Politécnica de Chimborazo. Para la investigación las muestras serán consideradas el personal que trabaja en el DTIC.

La muestra se tomará con el objetivo de conocer la realidad de la seguridad de información con la Dirección de Tecnología y Comunicación de la Institución, así de esta manera se podrá entregar un informe de los aspectos encontrados al realizar la evaluación de las normativas y leyes del Ecuador para la seguridad de la información.

3.2. **Tipo de estudio**

El siguiente trabajo es de tipo exploratorio, ya que pretende incluir controles de seguridad de la información para mejorar la calidad de la Dirección de Tecnología y Comunicación.

Además, no se pretende cuestionar el manejo de la Dirección de Tecnología si no de conocer su estado actual y proponer una mejora.

3.3. **Población**

La población de la investigación está constituida por las personas que trabajan en la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo, ya que son quienes manejan directamente los procesos de información.

3.4. **Muestra**

La muestra para la investigación será nuestra misma población

3.5. **Métodos**

Para la investigación se ha utilizado el método científico – modelo general, que incluye el planteamiento del problema, la formulación de la hipótesis, el levantamiento de la información, el análisis e interpretación de datos, la comprobación de la hipótesis y la difusión de los resultados de la investigación.

También ha sido utilizado el método deductivo, para la evaluación inicial del DTIC y evaluar si posee alguna normativa o ley o carece de las mismas.

Adicionalmente el método inductivo ha sido utilizado para desarrollar las conclusiones generales presentadas en este proyecto de investigación, basadas en los resultados específicos de las muestras.

3.6. Técnicas

Por el ámbito de la experimentación, la observación es la técnica principal utilizada en esta investigación. La misma ha permitido la ponderación de cada uno de los indicadores que se muestra la calidad en la seguridad de información.

Para la comprobación de la hipótesis se ha utilizado el análisis estadístico y la estadística inferencial.

3.7. **Instrumentos de evaluación**

La validación de los instrumentos utilizados en una investigación tiene por objetivo medir el dominio especifico de las variables que se han considerado. Las encuestas elaboradas fueron avaladas por el tutor y los miembros de la tesis, quienes han utilizado diferentes metodologías en campo de gestión de TI.

3.8. **Aplicación del método**

Dentro de los sectores de seguridad de información uno de los más vulnerables es la Educación por es que el DTIC de la Escuela Superior Politécnica de Chimborazo es viable para la aplicación de la propuesta.

La propuesta de normativa necesita como requisito el conocimiento o la investigación previa de las normas y leyes vigentes en el Ecuador además de las políticas implementadas por el gobierno de turno.

La normativa propuesta tiene como objetivo ser un documento de apoyo para mejorar la calidad de la información de la Dirección de Tecnología y Comunicación de la ESPOCH.

3.9. **Procedimientos**

Como primer punto debemos conocer las normativas y leyes vigentes en el Ecuador en cuanto a seguridad de información.

Por otro lado en base a los resultados obtenidos en las encuestas podremos determinar el estado actual en cuanto a normativas y leyes que posea el DTIC en seguridad de información.

Y de esta manera proponer una normativa en base a una norma ISO que ayude a mejorar la calidad de seguridad de información del DTIC.

3.10. **Variables e indicadores**

Estará basada en la hipótesis de la investigación planteada en el trabajo de investigación que indica lo siguiente: *La aplicación de las normativas de seguridad de información mejorará la calidad de información en los Departamentos de tecnología y comunicación,* se determina las siguientes variables:

Variable Independiente*:* normativa de seguridad de la información.

Variable dependiente: calidad de información en los departamentos de tecnología y comunicación

El uso de controles de seguridad de la información producirá cambios en la calidad de servicio de la Dirección de Tecnología información y Comunicación de la Escuela Superior Politécnica de Chimborazo.

Operacionalización Conceptual

Tabla 3-1: Operacionalización conceptualización,

VARIABLE	TIPO	CONCEPTO
Normativas de seguridad de la información	v. independiente	Procedimientos adecuados en el tratamiento de la información de una organización[8]
Calidad	v. dependiente	Conjunto de propiedades y de características de un producto o servicio, que le confieren aptitud para satisfacer unas necesidad es explícitas o implícitas[9]

Fuente: Lucía Guevara, 2017

Operacionalización Metodológica

Tabla 3-2: Operacionalización metodológica

VARIABLE	INDICADOR	TECNICA	INSTRUMENTO /FUENTE
Normativas de seguridad de la información	• Normas en vigencia. • Recursos en vigencia	• Búsqueda de información • Observaciones • Análisis	Articulo Ministerial 277 Acuerdo 266
Calidad	• Confiabilidad • Integridad • Disponibilidad	• Observación • Análisis	Plan de desarrollo informático

		• Búsqueda de información	

Fuente: Lucía Guevara, 2017

Tabla 3-3. Variables independientes y dependientes

VARIABLES	INDICADORES	INDICES
V. Independiente: Normativas de seguridad de información	Normas en vigencia.	• Conocimiento por parte de los directivos y trabajadores.
	Recursos en vigencia	• Conocer los recursos y procesos que maneja el DTIC para seguridad de información.
V. Dependiente Calidad	Confidencialidad	• La información que maneja el DTIC en cuanto a sus principales activos. • En el DTIC se maneja políticas de confidencialidad.
	Integridad sustenta	• El ingreso de la información es avalado. • Procesos que permita en control periódico de la información almacenada.
	Disponibilidad	• La utilización y acceso de la información por parte de las personas que involucran (estudiantes, docentes y trabajadores) la ESPOCH.

Fuente: Lucía Guevara, 2017

3.11. **Análisis de las variables**

El presente trabajo investigativo plantea un análisis estadístico descriptivo que relaciona las variables de estudio de forma dicotómica y con tablas de doble entrada que sustentan el análisis estadístico inferencial que justifica la vigencia de una normativa que permitirá mejorar la calidad en la seguridad de información el cual será aplicado al DTIC de la ESPOCH el cual beneficie a la institución de educación superior.

3.11.1. ***Indicadores de la variable independiente***

Para la comprobación de la hipótesis en primer lugar determinaremos si el DTIC posee leyes o normativas de seguridad de información vigentes en el Ecuador.

3.11.2. Indicadores de la variable dependiente

Para determinar si mejora la calidad de la seguridad de la información con la que trabaja el DTIC será propondrá controles de la ISO 27001, y se determinará si existe un cambio en la seguridad de la información.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Procedimiento general

El presenta trabajo de investigación tiene como objetivo dar a conocer las leyes y normativas de seguridad de información vigentes en el Ecuador, para indicar la propuesta de una metodología que abarque estas leyes y puedan ser aplicadas a Instituciones de Educación Superior.

Se pretende demostrar que esta metodología puede ser utilizada en cualquier institución o empresa sea pública o privada y además que abarque las leyes y normas del Ecuador, para su correcto funcionamiento.

Para lograr esto, se estudia las normativas, estándares mundiales, para seguidamente revisar las que posee el Ecuador para de allí partir en saber cuál de estas sería la mejor opción y si abarca las leyes y normativas vigentes del país.

Para la demostración de la propuesta de metodología primeramente se debe conocer la situación actual mediante una encuesta en la cual nos proveerá de la información necesaria del DTIC.

4.2. Presentación de resultados

Los resultados obtenidos muestran de manera directa que el uso de la propuesta ayudaría a mejorar la calidad de la seguridad de la información basándonos en los parámetros que utiliza la norma ISO 27001 que son confiabilidad, disponibilidad e integridad.

4.3. **Demostración de la hipótesis**

A continuación, se presenta de una manera sistematizada la demostración de la hipótesis

4.3.1. ***Planteamiento***

La puesta en vigencia de controles de seguridad de la información producirá cambios en la calidad de la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo

4.3.2. ***Población***

La población que se ha utilizado para el presente estudio son los trabajadores de la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo, que son las personas que evidencian en su trabajo diario.

4.3.3. ***Selección del nivel de significación***

Se ha utilizado de un nivel de significación de ∞=0.05, considerando un 95% de confiabilidad de los resultados y un 5% de error.

4.3.4. ***Descripción de la muestra***

Para el estudio se ha tomado que el universo será la misma cantidad que nuestra población ya que no sobrepasa las 30 personas, en el caso de estudio el DTIC se encontraba laborando en este periodo de encuestas 12 personas, por lo que se consideró a estas personas como muestra.

En el caso de la presente investigación, se desarrolló un cuasi experimento ya que se trabajó en grupos ya definido previamente al conocer las personas que integran la dirección de tecnología y comunicación de la ESPOCH, por otra parte cumple el trabajo

con características experimentales al presentar la variable independiente (normativas de seguridad de información) y una variable dependiente (calidad) y el efecto que produce la variable dependiente sobre la independiente(mejorará la calidad de seguridad de la información).

El trabajo se realizó al mismo grupo sin la existencia y conocimiento de las leyes y normas vigentes del Ecuador en cuanto a seguridad de la información, y posteriormente una vez establecido propuestas de políticas al Director y una divulgación del tema propuesto y con el análisis del esto actual del DTIC se presenta el segundo escenario, para ello se observó se estableció la encuesta propuesta observar Anexo B.

4.3.5. *Especificación del estadístico*

Se supone la distribución para la población como una distribución de chi cuadrado en el cual determinamos si la observación o la situación del escenario antes de la propuesta e igual o cambia después de entrega de la propuesta. Con un nivel de significancia del 5%, para ellos se crea una tabla con los resultados obtenidos en las encuestas aplicadas al grupo determinado.

4.4. **Comprobación**

A continuación, se presenta una tabla donde se resume de una manera más clara los resultados obtenidos en las encuestas realizadas al personal del DTIC.

Se realizará una tabulación e interpretación de las preguntas de acuerdo a los indicadores planteados para la calidad de la información.

4.4.1 *Indicadores de la variable independiente*

Los indicadores para la variable independiente son las normas en vigencia y los recursos en vigencia los mismos que medirán la existencia de políticas o controles que ayude a la seguridad de la información.

4.4.2 *Indicadores de la Variable dependiente*

Los indicadores para la variable dependiente son integridad, disponibilidad y confidencialidad los mismos que ayudan a medir la calidad en la seguridad de la información.

Para poder demostrar si la propuesta genera algún cambio y sobre todo mejora la calidad en base a la seguridad de la información se propone implementar la política de control de acceso una vez determinada las vulnerabilidades del DTIC.

Tabla 3-4 Encuesta realizada para la implementación de la política propuesta.

	ISO 27001 Control de Acceso	SI CUMPLE	NO CUMPLE	PARCIALMENTE
1	Posee una política de control de acceso establecido por la Dirección?			
2	Existen perfiles de usuario definidos para accesos aplicaciones informáticas?			
3	Se encuentra establecido los derechos de acceso de usuarios a las aplicaciones informáticas?			
4	Se encuentra establecido la cancelación o ajuste de los derechos de accesos?			
5	Se comunica por escrito que los usuarios mantenga la autenticación de manera secreta?			
6	Se restringe el acceso a las funciones de los sistemas?			
7	Se establece una conexión segura de acceso a las aplicaciones informáticas?			

8	Se utiliza contraseñas interactivas y de calidad?			
9	Se restringe y controla el uso de programas utilitarios que afecten al funcionamiento de la aplicaciones informáticas?			
10	Se restringe el acceso a códigos fuente de sistemas de las aplicaciones informáticas?			

Fuente: Lucía Guevara, 2017

El primer escenario planteado es el DTIC sin el uso de la política de control de acceso a la información y sistemas. La misma que nos da lo siguientes resultados.

Los requisitos de seguridad para las aplicaciones de la Institución son documentados, por ejemplo: Toda aplicación deberá contar con un usuario y clave de acceso, no se permitirá sesiones concurrentes.

- La primera información entregada por la dirección del departamento nos indica que se han realizado proyectos en cuanto a las aplicaciones para acceder con su propio usuario, actualmente se encuentra en proceso de integración de aplicaciones a este proyecto.

¿Existen perfiles de usuario definidos para accesos aplicaciones informáticas?

- La Institución no posee una política que permita mantener los perfiles de usuario, pero tiene establecido los roles de acceso.

  Para la integración de las aplicaciones se están creando perfiles de usuarios según sus funciones y responsabilidades.

¿Se encuentra establecido la cancelación o ajuste de los derechos de accesos?

- Al no estar estandarizado en la actualidad ninguna ley en las aplicaciones no se cuenta con segregación de tareas un mismo usuario puede solicitar, aprobar y autorizar una transacción. Esto se considera de riesgo alto.

¿Se restringe el acceso a códigos fuente de sistemas de las aplicaciones informáticas?

- Se revisa que las aplicaciones existentes muestran que los códigos fuentes pertenecen algunos de los compañeros que trabajan en la misma área es decir que otro usuario puede acceder a la aplicación porque conoce su código fuente. Dando como único inconveniente el hecho de los trabajadores llevan el código fuente creado.

Los valores obtenidos son transformados en porcentaje con el objetivo de presentar una tabla los valores obtenidos en los dos momentos trabajados, sin el uso de normativas o controles y con el uso de la misma.

- ✓ El número de encuestados está representado por N: **N=12**
- ✓ El valor que en nuestras filas será un total de 11 ya que las preguntas pueden tener un valor de 12 como máximo y se pueden distribuir entre las 3 opciones:

12 100%|

x ? = (X * 100)/12 =

- ✓ Por lo tanto, la fórmula porcentual de las columnas para cada pregunta será la sumatoria de las preguntas, ya que el máximo de cada pregunta es 12 la sumatoria es de 36 y la formula será:

36 100%

∑(X) ? = **(∑(X) * 100)/36 =**

- ✓ Y por último para encontrar el valor porcentual general del total será de 36 por las 3 opciones de respuesta que es 108.

108 100%

∑ (X, Y, Z) ? = **(∑ (X, Y, Z) * 100)/108**

Tabla 3-5 Valores porcentuales de cada indicador sin la aplicación de la política

Indicador / Pregunta		Sin Aplicación de política			%
		Si(X)	No(Y)	Par(Z)	
NORMAS EN VIGENCIA	1	0	100	0	100
	2	16,16	58,33	25	100
	3	0	66,67	33,33	100
Total Normas vigencia		5,55	75	19,45	100
RECURSOS EN VIGENCIA	4	0	100	0	100
	5	0	100	0	100
Total Recursos vigencia		0	100	0	100
CONFIDENCIALIDAD	7	66,66	9	33,34	100
	9	0	58,33	41,66	100
	12	83,33	0	16,66	100
Total Confidencialidad		50	19,44	30,56	100

INTEGRIDAD	6	0	100	0	100
	8	0	83,33	16,67	100
	11	58,33	0	41,47	100
Total Integridad		19,44	61,11	19,45	100
DISPONIBILIDAD	10	0	66,66	33,34	100
	13	0	75	25	100
	14	0	100	0	100
Total Disponibilidad		0	80,60	19,40	100
TOTAL		**14,99**	**67,23**	**17,78**	**100**

Fuente: Lucía Guevara. 2017

APLICACIÓN DE LA POLÍTICA DE CONTROL DE ACCESO

Tabla 3-5 Propuesta de política de control de acceso de la dirección de tecnología y comunicación

Dirección TIC	**POLÍTICA DE** CO**NTROL DE ACCESO DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN**		
SERIAL: P00004	FECHA DE EMISIÓN:24/10/2016	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Maestrante	REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo		NÚMERO DE PÁGINA:1 de 2

Proceso de información sobre nueva política que adopta el DTIC

ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.

VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión

POLÍTICA:

ACCESO A INFORMACIÓN DEL DEPARTAMENTO:

La información estará en potestad del Director del DTIC con el fin de asegurar la confidencialidad, disponibilidad e integridad del mismo.

ACCESO A SISTEMAS:

Se crea un documento exclusivo del trabajador responsable donde no se podrá permitir el acceso a terceras personas sin previa autorización del Director, con el fin de resguardar la integridad, confidencialidad de la información del sistema.

Establecer una campaña de concientización sobre el control de acceso a los sistemas.

Propiciar una clave interactiva de calidad se deberá realizar el cambio de la misma cada 72 horas con 10 caracteres mínimos incluidos letras mayúsculas minúsculas, números símbolos que no haga referencia a nombres personales o de familiares o fecha de nacimiento propio o de familiares.

Es completa responsabilidad del trabajador el uso de su contraseña.

Creación obligatoria de perfiles de usuario con las funciones establecidas.

Será obligatorio para el director del departamento o la secretaria la constante información indicando que trabajadores salen de forma temporal o definitiva.

Será exclusivo el uso del código fuente para la Institución donde fue elaborado y no se podrá usar en otra institución fuera de la misma.

Fuente: Lucía Guevara, 2017

Para la verificación de que las actividades sean ejecutadas en cumplimiento con la política de control de acceso se trabajó directamente con las personas en los tiempos que podían dedicarle para comprobar si la política mejora su proceso de trabajo en el acceso a los sistemas. Estableciendo lo siguiente:

- Campaña personalizada de concientización del manejo de claves como medida de seguridad de la información que maneja ese sistema
- Singles sing on
- Perfiles de usuarios
- Para acceso a bases de datos serán a través de las interfaces aplicativas
- El token o ticket de sesión

- Clara identificación única de la sesión del usuario

La existencia de una política que posea controles de acceso de seguridad de la información da como resultado la siguiente tabla, basada nuevamente en el uso de la misma encuesta.

Tabla 4-6 Valores porcentuales de la encuesta aplicada con la política propuesta.

Indicador / Pregunta		Con la aplicación de política			%
		Si(X)	No(Y)	Par(Z)	
NORMAS EN VIGENCIA	1	100	0	0	100
	2	66,67	8,33	25	100
	3	80,56	8,33	16,66	100
Total Normas vigencia		5,55	80,56	5,56	13,88
RECURSOS EN VIGENCIA	4	100	0	0	100
	5	100	0	0	100
Total Recursos vigencia		0	100	0	0
CONFIDENCIALIDAD	7	66,66	0	33,34	100
	9	66,66	8,33	25	100
	12	100	0	0	100
Total Confidencialidad		50	77,77	2,77	19,44
INTEGRIDAD	6	58,33	16,66	25	100
	8	83,33	0	16,67	100
	11	83,33	16,67	0	100
Total Integridad		19,44	74,99	11,10	13,90
DISPONIBILIDAD	10	66,66	16,66	16,66	100
	13	58,33	8,33	33,33	100
	14	58,34	8,33	33,33	100
Total Disponibilidad		0	61,10	11,10	27,78
TOTAL		**14,99**	**78,88**	**6,10**	**100**

Fuente: Lucía Guevara, 2017

En la siguiente tabla muestra

Tabla 4-7: Valores porcentuales totales.

MOMENTOS	OPCIONES		
	SI **%**	**NO** **%**	**PARCIAL** **%**
Sin la Política	14,99	67,23	76,10
Con la Política	76,1	0,00	23,89

Fuente: Lucía Guevara, 2017

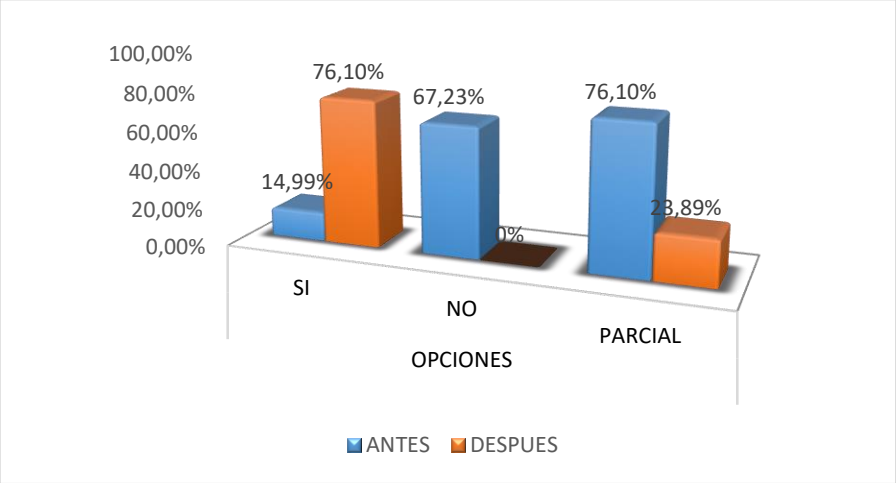


Gráfico 4-6: Grafico de barras de los valores porcentuales finales

Fuente: Lucía Guevara, 2017

Al obtener los resultados que nos muestra la tabla general mediante el gráfico podemos observar un incremento del 60% en la **mejora** de la calidad de la seguridad de la información con el uso de la propuesta presentada.

4.5 Comprobación de la Hipótesis General

A continuación, se presentará el sistema de hipótesis comenzando con la especificación de hipótesis nula y la hipótesis de la investigación.

Hipótesis Nula H_0: *Las normativas de seguridad de información* ***no*** *mejorará la calidad de información en los Departamentos de Tecnología y Comunicación.*

Hipótesis de investigación H_a: Las normativas de seguridad de información mejorará la calidad de información en los departamentos de tecnología y comunicación.

La representación estadística de la hipótesis nula y la de la alternativa o de investigación sería el de un caso unilateral, tal como sigue:

$$H_0: \mu_2 \leq \mu_1$$

$$H_a: \mu_2 > \mu_1$$

Fórmula para el Chi-Cuadrado muestra:

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 / D_J$$

Donde:

X^2 = ji cuadrado la cual agrupa en categorías las observaciones.

A = porcentaje antes de la aplicación de nuestra propuesta

D = porcentaje después de la aplicación de la propuesta

J= el *número* de opciones que se tiene dependerá la cantidad de frecuencias que se repite las variables.

La distribución chi-cuadrado depende de desviaciones independientes, grados de libertad y no puede ser negativa.

$$\sum_{J=1}^{K} (A_J - D_J)^2 / D_J$$

= 170.32

- Nivel de Significación

  95% de confianza = 5% de error ⇒ 0,05

- Grados de libertar mediante la fórmula:

  Gl = (r-1)

Gl_V = N – 1 => 12 – 1 = 11

$$\sigma = \sqrt{\frac{\sum_{J=1}^{K} (A_J - D_J)^2 / D_J}{k - 1}} = \sqrt{170,3/11} = 3.93$$

Valor crítico $X^2_{.99}$ = 3.36

Para el valor de crítico de ji – cuadrado de X^2 =3,36 es mayor 2.76 y menor a 4,13 con un novel de confianza de 95% s por lo tanto **rechazamos H_0 y aceptamos H_a**

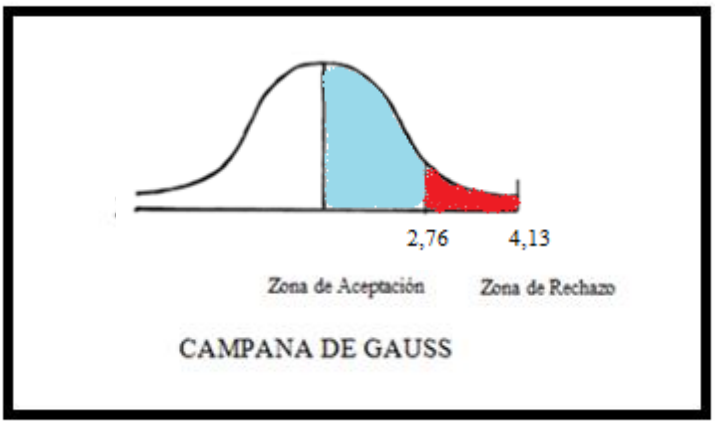


Gráfico 4-7 Campana de Gauss
Fuente: Lucía Guevara, 2017

CAPÍTULO V

5 PROPUESTA

5.1. Introducción

En este capítulo se presenta la propuesta de una normativa que abarque las leyes vigentes y que esté basada en un sistema de calidad que permita mejorar la seguridad de la información en la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo y al estar basado en una norma ISO conllevará el mejoramiento de la calidad, la comprobación de la misma se podrá visualizar al implementar una de las políticas en el departamento.

5.2 Objetivos

Con la propuesta de la normativa se pretende:

- Adoptar las leyes vigentes en el Ecuador, ya que es se obliga a las Instituciones sean estas públicas o privadas a asegurar sus activos y su información a través del uso de una norma de calidad y seguridad.
- Garantizar que la información de las Institución sea disponible, integra y confiable, para el personal y los usuarios.

5.3 Descripción del escenario sin leyes y normativas

El DTIC en la ESPOCH será abordado mediante la utilización de una encuesta inicial la cual nos proveerá de la información de la situación actual de la dirección teniendo en cuenta en esta encuesta los principales indicadores de mi propuesta como son la integridad, disponibilidad y confiabilidad para conocer la calidad de información que se maneja.

Una vez realizada la encuesta inicial el Director a cargo nos da a conocer lo siguiente:

- El DTIC no posee un plan estratégico para seguridad de información
- El conocimiento sobre las leyes y normativas vigentes en el Ecuador no son de su dominio más por conocimiento general sabe que existe pero detalladamente.
- Indica que los trabajadores manejan sus propios conocimientos de seguridad pero en seguridad física cumple con los requisitos necesarios.
- No se firma ningún acuerdo de confidencialidad pero solicita de manera verbal que no exista divulgación.
- No existe ningún tipo de sanción frente a la divulgación.
- La información es tomada de los servidores los cuales si poseen un backup pero los encargados de los servidores son quienes se encargan de ese tema.
- No poseen una bitácora se realiza un informe de lo sucedido pero no todas a personas tienen acceso a esa información.
- Que no tiene conocimiento de esta ley que el DTIC trabaja autónomamente y el conocimiento ayuda superar dichos obstáculos.
- Que no existe un proyecto de seguridad a su cargo o a toma de algún sucesor conoce de la importancia del mismo pero no se ha trabajado en ello.

Indica que el tema propuesto permitirá dar conocer al directivo como a los trabajadores su situación actual en cuanto a seguridad de información.

De esta manera ayudara a la Institución a cumplir con las leyes vigentes y a mejorar la calidad de su información la cual tendrá un efecto positivo ya que estará guiada bajo una normativa de calidad.

Además como parte del análisis inicial se realizó la observación y detección de vulnerabilidades encontradas en la dirección y de donde partiremos también para la propuesta de normativas basadas en la Norma NTE INEN-ISO/IEC 27001.

Tabla 5-1: Tabla de vulnerabilidades

Detección de vulnerabilidades	Vulnerabilidad
Acceso no autorizado a la red	Información visible de los servicios
	Direcciones visibles durante escaneo de red
	Información visible de los sistemas operativos.
Acceso no autorizado al sistema de información	Poca fortaleza en el estándar de contraseñas
	Única contraseña para los sistemas y servicios
	Información visible de los servicios
Repositorio de documento	No existe un repositorio virtual o digital de uso exclusivo del DTIC
	Cada persona no posee un registro de incidentes ni tampoco lo socializa.
	Si el trabajador sale del DTIC no entrega estos registros.
Claves de acceso	Las claves de acceso son entregadas al trabajador y no existe registro de cambios de contraseñas cada periodo de tiempo
	Los usuarios no son eliminados inmediatamente después de su salida.
Control de acceso a la información	No está establecido quien puede acceder o no dentro del DTIC a la información.
	Al salir del departamento sea temporal o definitivamente no existe un control de usuarios.
Intercambio de información	Al salir el trabajador del DTIC no firma un acuerdo no divulgar la información.
	Información visible de los servicios
	Información visible de los sistemas operativos.

Escritorio y pantalla limpia	Al dejar temporalmente su puesto de trabajo se deja bloqueada la pantalla
	Impresiones de código en el escritorio
	Anotaciones de información en el escritorio
Controles criptográficos	No existe política de manejo de control criptográfico en la implementación de software o intercambio de información entre sistemas.
Seguridad Física	Espacio insuficiente en el interior y exterior de la sala de servidores

Fuente: Lucía Guevara, 2017

5.4. Descripción del escenario con la normativa

Con la aplicación de la propuesta de implementación de la leyes y normativas de seguridad de información que rigen en el país y basándose en una norma de calidad como lo es la ISO 27001 se logrará primeramente ser una Institución reconocida no solo por sus logros académicos, sino ante sus principales usuarios como son estudiantes, docentes, administrativos y trabajadores mostrar que la información que maneja la Dirección de tecnología de la información y comunicación de la ESPOCH cumple con proceso de calidad en todas las áreas que existen, luego a nivel nacional dar a conocer que como institución pública cumple con las leyes y normas vigentes basándose en una norma Internacional de calidad información.

Para la elaboración de la propuesta se utiliza un modelo de implementación y mejora denominado PHVA (Planear-Hacer-Verificar-Actuar), este modelo se basa en la mejora continua.

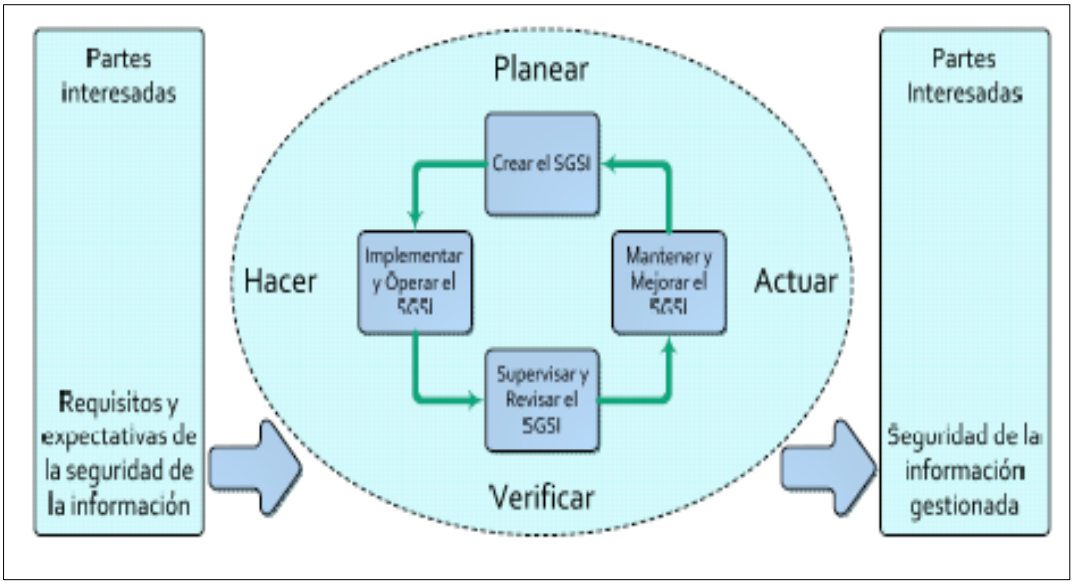


Gráfico 5-1 Metodología ISO 27001.
Fuente: (Ofiseg, 2014)

Breve indicación de las cuatro fases:

- Planificar: realiza un estudio la situación actual y se establece los objetivos y alcances generales.
- Hacer: Lograr lo planificado o la implementación del mismo
- Verificar: Analizar que los objetivos y metas se logren
- Actuar: Lograr corregir los error encontrados.

El presente proyecto se ubica en la fase de planificación, ya que el estudio realizado abarca la situación actual y establece a través de su propuesta los objetivos y alcances generales que debería poseer el departamento..

Como se indica anteriormente la fase de planificación aborda las políticas, objetivos, procesos y procedimientos para mejorar la calidad en la seguridad de la información.

A continuación se detalla en la siguiente tabla los objetivos que abordan esta fase y los cuales son entregables:

Tabla 5-2: Entregables de la planificación

	Entregables de la Norma ISO 27001	Entregable del Estudio de las normativas de seguridad de la información de instituciones públicas: Propuesta de una normativa en una Institución de Educación Superior
Obtención de la aprobación del director para iniciar el proyecto	Aprobación de la dirección para la iniciación del proyecto	Solicitud de permiso para la ejecución de encuestas, entrevista y observación en el Departamento de Tecnología y Comunicación de la ESPOCH
		Firma de Aceptación a la Solicitud
Definición de alcance y Políticas	Alcance	Propuesta de una normativa Proyecto de titulación.
	Política de seguridad	Política de seguridad del Departamento de Tecnología y Comunicación de la ESPOCH.

Fuente: Lucía Guevara, 2017

Una vez analizados los controles que ayudarán al DTIC a mejorar su calidad de la información se procede a la elaboración de las políticas de seguridad que se entregará en la propuesta la misma que consta en la norma vigente ISO 27001:

- Política para el manejo de información clasificada
- Políticas de control de Acceso
- Políticas de intercambio de información
- Política de pantalla y escritorios limpios
- Política de uso aceptable de los activos
- Política del uso de controles criptográficos:

A continuación se realizará una descripción resumida de cada uno de los entregables:

- **Política de seguridad**

El propósito de la misma es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta política se deberá aplicar a en todo el departamento y deberán conocerla todos los trabajadores sin excepción.

Quien maneje y sociabilice esta política serán los directivos del Departamento de Tecnología y Comunicación de la ESPOCH. Véase el Anexo B.

- **Política para el manejo de información clasificada**

Esta política tiene objetivo garantizar que se proteja la información en un nivel adecuado.

Aquí se aplica los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos. Véase el Anexo B.

- **Políticas de control de Acceso**

Esta política tiene como objetivo definir el acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

El alcance de esta política son todos los sistemas, equipos e instalaciones todo lo que sea parte del Departamento. Véase el Anexo C

- **Políticas de intercambio de información**

Esta política tiene como objetivo asegurar la información y el software cuando exista intercambio de información. Este documento aplica a la información y tecnología de la información. Véase el Anexo D.

- **Política de pantalla y escritorios limpios**

Esta política tiene como objetivo establecer reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también las instalaciones y los equipos compartidos. Véase el Anexo E.

- **Política del uso de controles criptográficos**

Esta política tiene como objetivo definir el uso de controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

El Anexo 6 presenta el documento completo

Al crear estas políticas basadas en la Norma INEN-ISO/IEC 27001 se podrá establece una normativa en el Departamento de Tecnología y Comunicación de la ESPOCH. Ya que se encuentra Normado y regularizado. Véase el Anexo F

Propuesta de formatos[1]

Una vez realizado el procedimiento quedará el registro de todos los procesos como se muestra en la tabla.

Tabla 5-3 Formato propuesto.

<<SELLO>>		**TITULO:**	
SERIAL:	FECHA DE EMISIÓN	FECHA DE MODFIFICACION:	APROBACIÓN:
ELABORADO POR:	REVISADO Y APROBADO POR:		NÚMERO DE PÁGINA:
INTRODUCCIÓN: DESCRIPCIÓN:			
I	INSTRUCCIÓN DE TRABAJO		
M	MANUAL		
P	PROCEDIMIENTO		
R	REGISTRO O REPORTE		
L	POLITICA O LINEAMIENTO		

Fuente: (Guevara, 2012)

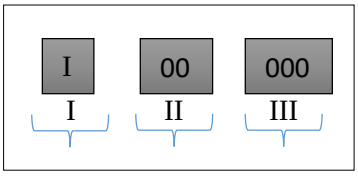


Figura 5.2 Caracteres del Serial propuesto
Fuente: Lucia Guevara E.

El primer carácter nos indica el tipo de documento seleccionaremos cualquiera de estos caracteres como indica la Figura 5.2.

[1] Tesis NORMA ISO 27001 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN IMPLEMENTACIÓN EN LOS PROCESOS MÁS RECURRENTES EN EL DESITEL, pág. 55

Tabla 5-4: Letras de identificación para los documentos

I	INSTRUCCIÓN DE TRABAJO
M	MANUAL
P	PROCEDIMIENTO
R	REGISTRO
L	POLITICA O LINEAMIENTO
R	REPORTE

Fuente: Lucia Guevara. (Guevara, 2012)

El segundo carácter nos indica que área del DTIC genera la documentación:

Opcionalmente el segundo carácter puede ser remplazado por las siglas de área respectivas como se muestra en la Tabla 5.4

Tabla 5-5: Numeración para las áreas

00	Dirección
01	Secretaria
02	Desarrollo
03	Redes
04	DataCenter

Fuente: (Guevara, 2012)

Los próximos tres dígitos son tres caracteres numéricos que representan el orden secuencial en el que se va generando los documentos.

- **Fecha de Emisión:** Nos indicará la fecha en que se ha realizado el documento.
- **Fecha de Modificación:** Nos indicará si ha existido una modificación y en qué fecha.
- **Aprobación:** Indicará si ha sido aprobado o no el documento.
- **Elaborado por:** Indicará los creadores del documento.
- **Revisado y Aprobado por:** Muestra el nombre de quien ha revisado y aprobado en este caso será siempre la Dirección.

- **Número de páginas:** Indicará el número de página para tener una secuencia del documento especificando una de cuantas Ejemplo: 1 de 4
- **Introducción:** Se describirá la metodología a utilizar para definir si está correctamente usado el serial
- **Descripción:** Nos indicará una descripción breve del documento.
- **Instrucción de trabajo:** Se define paso a paso el "como" de una actividad.
- **Formulario:** Para anotar los resultados de cualquier actividad el cual podrá convertirse en registro.
- **Manual:** Es un documento compuesto por cierta extensión en cuanto a sus páginas, especifica y describe el compromiso, las responsabilidades, las autoridades y metodologías del DTIC para cumplir los requisitos de la Norma ISO27001
- **Procedimientos:** Define "quien hace que" y "cuando", Este documento describe la forma específica para llevar a cabo una actividad o proceso contiene 6 partes: propósito, alcance, procedimiento, documentos, definiciones y referencias
- **Registros o reporte:** Sirve para evidenciar o para demostrar a terceros que un requisito está implantado y se ha cumplido, estará detallada la actuación y las personas involucradas y su decisión consta de 4 partes; la detección de incidente, supervisor inmediato, comité de seguridad, Dirección
- **Política o lineamiento:** Sirve para emitir al DTIC que política se ha optado de manera general o por áreas, posee 6 partes alcance, vigencia.
- **Firmas de responsabilidad:** Una vez que se ha realizado el informe el responsable deberá firmar, para quede constancia y se de veracidad al documento.
- **Número de resolución:** En el caso de que se emita un documento una vez realizado consejo politécnico o directivo se deberá colocar el número de la resolución.

Para la creación de las políticas en la Dirección de Tecnología y Comunicación se presenta el siguiente formato:

Tabla 5-6: Ejemplo de una política

(SELLO)	**TITULO:**		
SERIAL: L03001	FECHA DE EMISIÓN:00/12/2000	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR:EQUIPO ISO	REVISADO Y APROBADO POR:		NÚMERO DE PÁGINA:1 de 1
Proceso disciplinario por violación de políticas de seguridad de información Alcance: Vigencia; POLITICA 1.Posibles ocurrencias de incidente de función de nivel de responsabilidad, podrá ser ejemplo: -Llamada verbal de atención -Cuando sea reiterada suspensión laboral -Caso grave se recurrirá al despido			

Fuente: (Guevara, 2012)

5.5. **Definición del Método**

La encuesta permite a las personas que trabajan en el DTIC dar a conocer el estado actual del departamento y si están sujetos a las leyes y normativas vigentes en el Ecuador.

El grupo objetivo que ha sido considerado para el desarrollo del método está compuesto por el personal que trabaja en la Dirección de Tecnología y Comunicación de la Escuela Superior Politécnica de Chimborazo.

Cabe notar que dicha propuesta puede ser sometida en cualquier otro departamento tecnológico el cual el escenario tenga las mismas características.

5.6. **Lineamientos**

Para el desarrollo del Propuesta planteada se plantea lineamientos los cuales permitan alcanzar los objetivos propuestos y encontrar un beneficio para el departamento de tecnología y comunicación de la Escuela Superior Politécnica de Chimborazo.

Los siguientes son lineamientos definidos para el método planteado:

1. Que en el caso de existir una nueva ley esta se pueda adaptar a los controles que se hayan planteado.
2. Que en el método de la propuesta se pueda ser escalable en cuanto a controles y procesos.
3. Que los formatos establecidos puedan ser acoplados a las necesidades de la Dirección de Tecnología y Comunicación de la ESPOCH.

5.7 **Estructura del Método**

En escenario está basado en objetivos, lineamientos definidos para el método propuesto a continuación se presenta su desarrollo.

5.7.1. ***Actividades***

a. Planificación del Proyecto
b. Encuesta para análisis de la situación actual del Departamento
c. Observación de los procesos de seguridad de información que posee el Departamento.
d. Fusión de las leyes y normativa vigentes en el Ecuador
e. Propuesta de aplicación de las políticas de algunos de los principales procesos que realiza el departamento.
f. Encuesta para el análisis de los controles de la política aplicada.
g. Análisis y resultados
h. Conclusiones y recomendaciones

5.7.2 ***Procedimiento***

a. La presentación del proyecto al director del DTIC, con el objetivo de motivar a las Autoridades como personal de la importancia de estar actualizados e implementar las normas y leyes impuestas en el Ecuador para instituciones públicas y privadas.
b. La realización de la encuestas al personal del DTIC será un proceso clave para el levantamiento de información y conocer cómo se encuentra trabajando el

departamento en cuanto a seguridad de información, además que se conocerá los procesos que mantiene el departamento ya que la ISO recomienda un checklist inicial el cual será representado por la encuesta propuesta.

c. Se presentará una propuesta de en base a la situación actual.
d. Se aplicará una política que permita demostrar si existe un cambio.
e. Se realizará una encuesta para conocer si ha existido el mejoramiento de la calidad de seguridad de la información.

5.8 Ventajas y desventajas

La aplicación de la propuesta podría generar ventajas y desventajas, el siguiente tabla se muestran alguna de ellas:

Tabla 5-7 Ventajas y desventajas,

VENTAJAS	DESVENTAJAS
Al levantar la información sobre seguridad del Departamento de Tecnología y Comunicación se podrá dar a conocer como se encuentra el departamento actualmente	El cambio de autoridades del DTIC podrá retrasar el levantamiento de información ya que cada autoridad aplica estrategias para un mejor desarrollo de los procesos, que ya pudieron haberse dado.
Las autoridades del DTIC conocerá las normar y leyes vigentes que rigen en el Ecuador y de esta manera mejorará los procesos o servicios que entrega el departamento.	La información entregada por los trabajadores no siempre se puede constatar ya que los trabajadores saben lo que deben aplicar en sus estaciones de trabajo pero no siempre lo documentan como respaldo de lo acontecido.

Fuente: Lucía Guevara, 2017.

5.9 Repositorio Digital

En base a lo planteado se ve también la necesidad de utilizar un repositorio de información donde esté disponible para los usuarios de DTIC donde puedan acceder a la las políticas y a los formatos cuando se necesiten de esta manera se podrá cumplir la disponibilidad de la información,

Por lo que se presenta como propuesta adicional un repositorio digital el DTIC, el mismo que está en completa libertad de usarlo o pueda ser una guía.

Figura 5-3 Pantalla inicial del repositorio digital
Fuente: Lucía Guevara, 2017

Figura 5-4 Pantalla de descripción del Repositorio digital
Fuente: Lucía Guevara, 2017

Figura 5-5 Opción de descarga de las políticas del DTIC
Fuente: Lucía Guevara, 2017

CONCLUSIONES

- Al analizar las leyes vigentes en el Ecuador se considera que son creadas con el objetivo de que sean cumplidas y así garantizar el buen funcionamiento y manejo de las instituciones públicas o privadas ya que son quienes poseen la información personal de la ciudadanía.
- Al estudiar las leyes existentes se considera importante organizarlas y estandarizarlas para que puedan ser aplicadas a un departamento de tecnologías y comunicación de cualquier institución, es así que el cuadro que se presenta en este trabajo de investigación permite que pueda ser usado en cualquier caso de estudio en el Ecuador.
- La presente propuesta apoya a la Dirección del DTIC en un 60% ya que al evidenciar el estado actual del departamento a través de su FODA, permitirá establecer cuáles son los objetivos y alcances de manera real.
- En el análisis de resultados del estudio en base al escenario inicial del DTIC dio como resultado que no existe ningún tipo de política o manejo de seguridad de información posteriormente al dar una propuesta muestra que así se lograría un incremento de 64,11% en calidad de la seguridad de la información, ya que regularizará los indicadores de seguridad como son la integridad, disponibilidad y confidencialidad.
- La implementación de la propuesta en la política de control de acceso ha permitido mostrar que, de manera empírica los trabajadores usaban su propio conocimiento de lo que no deberían realizar cuantificando esto en un 40% en la seguridad de la información que manejan, al plantear una política basados en controles de la norma ISO y que estén empatadas con leyes del Ecuador, primeramente concientiza a los trabajadores de la obligatoriedad y el compromiso de usarla de esta manera se incrementa al 60% la seguridad de información.
- Se puede evidenciar a través de la implementación de la política de control de acceso que el DTIC mejorará la calidad en la seguridad de la información siempre que exista el compromiso de la Dirección y los trabajadores en su uso constante.

RECOMENDACIONES

- En base al estudio realizado las leyes y normativas del Ecuador pueden ir variando durante el transcurso de los gobiernos, por lo que es importante basarse en una norma estandarizada internacional como la ISO 27001 la cual es la única certificable, es escalable y permite cambios continuos y se adapta fácilmente a las necesidades de un departamento de tecnología y comunicación.
- El uso las políticas planteadas en el presente trabajo de investigación permitirán al DTIC un mejor control en la seguridad de la información el mismo que al estar basado en una norma ISO permitirá hacer referencia a la calidad en el servicio que presta el departamento garantizando a sus usuarios potenciales un tratamiento adecuado a la información que maneja.
- La creación del cuadro de las leyes vigentes en el Ecuador versus los controles que se adaptan a estas leyes no solo beneficiará al caso de estudio presentado sino también a cualquier departamento de tecnología que desea acoplar la ISO 27001 para la creación de su sistema de seguridad de la información.
- Hacer uso de esta investigación para generar nuevos temas de trabajo de tesis de maestrías relacionadas o a su vez continuar con el mismo ya que deja planteada una propuesta de trabajo, la misma que pueda ser implementada o comparada con otra norma para garantizar la seguridad de la información.

BIBLIOGRAFÍA

Normas Tècnicas Ecuatorianas. (1 de mayo de 2014). *http://www.normalizacion.gob.ec.* Recuperado el 4 de agosto de 2015, de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2015/07/nte_inen_iso_27013.pdf

Bitcompany. gob.ec. (7 de mayo de 2013). *www.bitcompany.biz*. Recuperado el 06 de marzo de 2016, de www.bitcompany.biz: http://www.bitcompany.biz/que-es-cobit/#.VyJVLXrorIU

Corporaciòn Nacional de Telecomunicaciones. (19 de mayo de 2015). Obtenido de http://corporativo.cnt.gob.ec/cnt-unica-empresa-publica-en-el-ecuador-que-obtiene-certificacion-iso-27001/

Congreso Nacional del Ecuador. (14 de abril de 2002). *Ley de Comercio Electrnico, Firmas Electronicas y mensajes de Datos*. Recuperado el 26 de marzo de 2016, de Ley de Comercio Electrnico, Firmas Electronicas y mensajes de Datos: http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Lanche Capa Darwin, (6 de enero de 2015). *www.ucuenca.edu.ec.* Recuperado el 2 de agosto de 2015, de http://dspace.ucuenca.edu.ec/bitstream/123456789/22371/1/tesis.pdf

ECONOCOM.com. (20 de septiembre de 2012). *www.itil.oasiatis.es*. Recuperado el 03 de marzo de 2016, de www.itil.oasiatis.es: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Escuela Politecnica del Litoral . (2015). Obtenido de http://rraae.org.ec/Record/0003_2df48696a72d3f968a9a31f89471229b

Contraloria General del Estado Ecuador. (30 de septiembre de 2011). *Normas de control Interno para las Entidades, Organismos del sector Público y de las Personas Juridicas de dercho Privado que dispongan de Recursos Públicos.* Recuperado el 2 de agosto de 2015, de www.contraloria.gob.ec: www.contraloria.gob.ec/pdf.asp?nombredocumento=1774

Fiscalia General del Estado Ecuador. (15 de Abril de 2013). *Fiscalia General del Estado*. Obtenido de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/fiscalias-provinciales/958-fiscal%C3%ADa-investiga-presunto-desv%C3%ADo-de-dinero-del-municipio-de-riobamba.html

Peña Ferney. (19 de MARZO de 2015). *ISO TOOLS*. Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Linares Gabriel. (JUNIO de 2015). Obtenido de http://es.slideshare.net/jonatan0106/distribucion-de-fisher-jicuadrado

Guevara, Lucìa. (2012). *dspace.espoch.edu.ec*. Obtenido de dspace.espoch.edu.ec: http://dspace.espoch.edu.ec/bitstream/123456789/2541/1/18T00517.pdf

Instituto Ecuatoriano de Normalizaciòn. (2016). Obtenido de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Jaramillo, Carlos. Miguel. (03 de julio de 2014). *Normas y Estadares Internacionales.* Recuperado el 01 de agosto de 2015, de www.espe.edu.ec: http://repositorio.espe.edu.ec/bitstream/21000/9022/1/T-ESPE-048282.pdf

Cano Jeymi. (2014). *VI ENCUESTA LATINOAMERICANA DE SEGURIDAD DE LA INFORMACION*. Obtenido de http://blog.segu-info.com.ar/2014/06/resultados-de-la-vi-encuesta.html

Ministerio de telecomunicaciones y de la sociedad de la Informaciòn, Ecuador. (20 de marzo de 2010). *http://www.telecomunicaciones.gob.ec.* Recuperado el 4 de agosto de 2015, de http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf

Agencia Nacional de transito, Ecuador (14 de mayo de 2013). *Ley Organica de Transparencia y Acceso a la Información Pública.* Recuperado el 3 de agosto de 2015, de http://www.ant.gob.ec: http://www.ant.gob.ec/index.php/12-lotaip/249-ley-organica-de-transparencia-y-acceso-a-la-informacion-publica-2013#.VcJz9pMcPIU

OASIATIS.com. (31 de julio de 2013). *Gestión de los servición TI*. Obtenido de http://goo.gl/6jan3b.

Ofiseg,.Consulting, Telde (2014). *http://www.ofisegconsulting.com*. Obtenido de http://www.ofisegconsulting.com/iso27000.htm

Security-Ecuador. (10 de Agosto de 2013). *Security-EC*. Obtenido de http://securityec.com/anonymous-ecuador-ataca-sitios-del-gobierno-ecuatoriano-10-de-agosto-2013/

Secretaria Nacional de la administraciòn Pública, Ecuador. (21 de Enero de 2014). Obtenido de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2015/04/PROYECTO-IMPLEMENTACION-CONTROL-Y-SEGUIMIENTO.pdf

SurAmerica, Noticias. (6 de junio de 2013). *Agencia pública de noticias del Ecuador y SurAmerica*. Obtenido de http://www.andes.info.ec/es/noticias/sistema-informatico-electoral-ecuador-sufrio-ciberataque-pais-primer-mundo.html

Symantec.ec. (2 de junio de 2014). *https://www.symantec.com*. Recuperado el 19 de octubre de 2015, de https://www.symantec.com: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Trendmicro. (12 de febrero de 2012). *http://www.trendmicro.com*. Recuperado el 20 de octubre de 2015, de http://www.trendmicro.com: http://www.trendmicro.com/cloud-

content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf

Universo, Ecuador. (17 de Noviembre de 2014). *El Universo*. Obtenido de http://www.eluniverso.com/noticias/2014/11/17/nota/4226966/ataques-web-podrian-aumentar

Van Bon, Jan. (14 de abril de 2010). *https://books.google.com.ec/.* Recuperado el 2 de agosto de 2015, de https://books.google.com.ec/books?hl=es&lr=lang_es&id=A9pEBAAAQBAJ&oi=fnd&pg=PR5&dq=ITIL&ots=faPYHqkpp_&sig=UJ7BXLKmpjlDHg9a4Yj81MIgoY0#v=onepage&q=ITIL&f=false

Vargas, Francisco. Alejandro. (21 de Noviembre de 2013). *www.uniboyaca.edu.co*. Recuperado el 1 de agosto de 2015, de http://revistasdigitales.uniboyaca.edu.co/index.php/reiv3/article/view/71/73

www.ccia.es. (03 de junio de 2012). *www.ccia.es*. Recuperado el 20 de 03 de 2016, de www.ccia.es: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

ANEXOS

ANEXO A. Encuesta

Encuesta dirigida al personal del Departamento de Tecnología y Comunicación.

ENCUESTA

Fecha: _____

Objetivo.- La encuesta tiene como objeto dar a conocer el estado actual del DTIC además evaluar el conocimiento de los trabajadores del departamento en el tema de seguridad de la información y las leyes que existen en el Ecuador, es parte del tema de titulación "*ESTUDIO DE LAS NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN DE INSTITUCIONES PÚBLICAS: PROPUESTA DE UNA NORMATIVA EN UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR"* de la Maestría en Seguridad Telemática.

Para la resolución de la misma se solicita responder la encuesta con la mayor honestidad la misma que permitirá poder analizar el estado actual del DTIC.

Pregunta N°1 (Normas en vigencia)

¿Usted como Director del DTIC conoce sobre leyes que exige el Gobierno actual sobre seguridad de la información en las Instituciones públicas o privadas en el Ecuador?

◯ SI
◯ NO

Si su respuesta fue **SI** indique cuales:

_____
_____

Pregunta N°2 (Normas en vigencia)

¿Sabe usted si los trabajadores del DTIC tienen conocimiento conoce sobre leyes que exige el Gobierno actual sobre seguridad de la información en las Instituciones públicas o privadas en el Ecuador?

◯ SI
◯ NO
◯ PARCIALMENTE

Si su respuesta fue **SI** indique el nombre de sus trabajadores:

_____
_____

Pregunta N°3 (Normativas en vigencia)

¿Conoce si existen iniciativas que se hayan propuesto los directivos o administrativos del DTIC con respecto a la temática de la seguridad de la información?

◯ SI
◯ NO
◯ PARCIALMENTE

Si su respuesta es sí o poco indique que temática se ha planteado:

_____
_____

Pregunta N°4 (recursos en vigencia)

¿Usted como director o trabajador del DTIC conoce de algún acuerdo de confidencialidad al ingresar a trabajar en el esta área donde se maneje información de la Institución?

- ◯ SI
- ◯ NO

Pregunta N°5 (recursos en vigencia)

¿Usted sabe si el DTIC posee una política de seguridad de la información?

- ◯ SI
- ◯ NO

Pregunta N°6 (integridad)

¿El DTIC maneja procesos que garanticen la seguridad de la información bajo una Norma de calidad de información?

- ◯ SI
- ◯ NO
- ◯ PARCIALMENTE

Si su respuesta fue **SI** indique brevemente el nombre de esos recursos o procesos:

_____
_____

Pregunta N°7 (confidencialidad)

¿Conoce algún reglamento interno del departamento que le indique que tendrá una sanción por divulgar la información del departamento durante su estancia en la misma o fuera de ella?

- ◯ SI
- ◯ NO
- ◯ PARCIALMENTE

Pregunta N°8 (integridad)

¿Cuándo usted recibe información sea física o de una base de datos sabe si se encuentra antes depurada o recibe un documento que le indique en qué estado se encuentra?

◯ SI
◯ NO

Pregunta N°9 (confidencialidad)

¿Usted como trabajador del DTIC registra algún proceso resguarde la información y que no sea de acceso público o a personas que no pertenecen al DTIC?

◯ SI
◯ NO

Pregunta N°10 (disponibilidad)

¿Cuándo existe algún evento en su área de trabajo con respecto a seguridad de la información, posee una bitácora que le permita a usted u otras personas recurrir a ellas para eventos futuros?

◯ SI
◯ NO

Pregunta N°11 (integridad)

¿Esta implementado un algoritmo de seguridad que permita sacar automáticamente los respaldos de la información a su cargo?

◯ SI
◯ NO
Justifique su respuesta:

_____
_____

Pregunta N°12 (confidencialidad)

¿Conoce usted si para acceder a la información se presenta credenciales u oficios al director del DTIC terceras personas cuando necesitan información de un sistema o proceso?

◯ SI
◯ NO
Justifique su respuesta:

_____
_____

Pregunta N°13 (disponibilidad)

¿Al realizar crear o realizar cambios en los sistemas se documenta la información del proceso para conocimiento del Director del DTIC, cualquier auditor o miembro directo del departamento que requiera dicha información?

◯ SI
◯ NO

Justifique su respuesta su procedimiento:

_____
_____

Pregunta N°14 (disponibilidad)

¿Cuándo ha existido un evento de seguridad usted puede acceder a información de manera **inmediata** para que se ayude a superar dicho evento?

- ◯ SI
- ◯ NO
- ◯ PARCIALMENTE

Justifique su respuesta como la hace:

_____
_____

Anexo B. Tabla Chi-Cuadrado (GUAYANA, 2015)

ν \ α	.995	.990	.975	.950	.900	.500	.100	.050	.025	.010	.005
1	.00+	.00+	.00+	.00+	.02	.45	2.71	3.84	5.02	6.63	7.88
2	.01	.02	.05	.10	.21	1.39	4.61	5.99	7.38	9.21	10.60
3	.07	.11	.22	.35	.58	2.37	6.25	7.81	9.35	11.34	12.84
4	.21	.30	.48	.71	1.06	3.36	7.78	9.49	11.14	13.28	14.86
5	.41	.55	.83	1.15	1.61	4.35	9.24	11.07	12.83	15.09	16.75
6	.68	.87	1.24	1.64	2.20	5.35	10.65	12.59	14.45	16.81	18.55
7	.99	1.24	1.69	2.17	2.83	6.35	12.02	14.07	16.01	18.48	20.28
8	1.34	1.65	2.18	2.73	3.49	7.34	13.36	15.5¹	17.53	20.09	21.96
9	1.73	2.09	2.70	3.33	4.17	8.34	14.68	16.92	19.02	21.67	23.59
10	2.16	2.56	3.25	3.94	4.87	9.34	15.99	18.31	20.48	23.21	25.19
11	2.60	3.05	3.82	4.57	5.58	10.34	17.28	19.68	21.92	24.72	26.76
12	3.07	3.57	4.40	5.23	6.30	11.34	18.55	21.03	23.34	26.22	28.30
13	3.57	4.11	5.01	5.89	7.04	12.34	19.81	22.36	24.74	27.69	29.82
14	4.07	4.66	5.63	6.57	7.79	13.34	21.06	23.68	26.12	29.14	31.32
15	4.60	5.23	6.27	7.26	8.55	14.34	22.31	25.00	27.49	30.58	32.80
16	5.14	5.81	6.91	7.96	9.31	15.34	23.54	26.30	28.85	32.00	34.27
17	5.70	6.41	7.56	8.67	10.09	16.34	24.77	27.59	30.19	33.41	35.72
18	6.26	7.01	8.23	9.39	10.87	17.34	25.99	28.87	31.53	34.81	37.16
19	6.84	7.63	8.91	10.12	11.65	18.34	27.20	30.14	32.85	36.19	38.58
20	7.43	8.26	9.59	10.85	12.44	19.34	28.41	31.41	34.17	37.57	40.00
21	8.03	8.90	10.28	11.59	13.24	20.34	29.62	32.67	35.48	38.93	41.40
22	8.64	9.54	10.98	12.34	14.04	21.34	30.81	33.92	36.78	40.29	42.80
23	9.26	10.20	11.69	13.09	14.85	22.34	32.01	35.17	38.08	41.64	44.18
24	9.89	10.86	12.40	13.85	15.66	23.34	33.20	36.42	39.36	42.98	45.56
25	10.52	11.52	13.12	14.61	16.47	24.34	34.28	37.65	40.65	44.31	46.93
26	11.16	12.20	13.84	15.38	17.29	25.34	35.56	38.89	41.92	45.64	48.29
27	11.81	12.88	14.57	16.15	18.11	26.34	36.74	40.11	43.19	46.96	49.65
28	12.46	13.57	15.31	16.93	18.94	27.34	37.92	41.34	44.46	48.28	50.99
29	13.12	14.26	16.05	17.71	19.77	28.34	39.09	42.56	45.72	49.59	52.34
30	13.79	14.95	16.79	18.49	20.60	29.34	40.26	43.77	46.98•	50.89	53.67
40	20.71	22.16	24.43	26.51	29.05	39.34	51.81	55.76	59.34	63.69	66.77
50	27.99	29.71	32.36	34.76	37.69	49.33	63.17	67.50	71.42	76.15	79.49
60	35.53	37.48	40.48	43.19	46.46	59.33	74.40	79.08	83.30	88.38	91.95
70	43.28	45.44	48.76	51.74	55.33	69.33	85.53	90.53	95.02	100.42	104.22
80	51.17	53.54	57.15	60.39	64.28	79.33	96.58	101.88	106.63	112.33	116.32
90	59.20	61.75	65.65	69.13	73.29	89.33	107.57	113.14	118.14	124.12	128.30
100	67.33	70.06	74.22	77.93	82.36	99.33	118.50	124.34	129.56	135.81	140.17

ANEXO C.

Documento Política de Seguridad de información de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE SEGURIDAD DE INFORMACIÓN DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>Serial:
P00001</td><td>Fecha de emisión:24/10/2016</td><td>Fecha de modificación:-</td><td>Aprobación:
SI</td></tr>
<tr><td>Elaborado por:
Maestrante</td><td colspan="2">Revisado y aprobado por:
Ing. Gustavo Hidalgo</td><td>Número de página:
1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Informar a todos los trabajadores que pertenecen al DTIC la política de seguridad de información.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se protegerá los recursos de información del DTIC y la tecnología utilizada para su procesamiento, frente amenazas internas o externas, deliberadas o accidentales con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.</td></tr>
</table>

ANEXO D.

Documento Política de para el manejo de información clasificada de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE PARA EL MANEJO DE INFORMACIÓN CLASIFICADA DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00002</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se protegerá toda información considerada clasificada por el Director o trabajadores ya sea esta verbal, escrita o electrónica ante terceras personas o sin autorización del Director, con el fin de asegurar ante cualquier amenaza o ataque interno o externo que ponga en riesgo el buen funcionamiento del DTCI, además deberá firmar un documento que indique que o divulgará información al salir temporal o definitivamente del DTIC, en caso de comprobar que es así se tomará acciones legales.</td></tr>
</table>

ANEXO E.

Documento Política de claves de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE CLAVES DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00003</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se creará contraseñas para los puestos de trabajo o sistemas que se administren con nivel de seguridad alto mayor a 10 caracteres donde se deberá incluir mayúsculas, minúsculas, números y caracteres especiales, que no sean parte de nombres de familiares o mascotas fácil de obtener en una conversación o fotografías en redes sociales. Las contraseñas se cambiaran en un periodo considerable de tiempo el mismo que deberá ser reportado al Director del DTIC.</td></tr>
</table>

ANEXO F.

Documento Política de control de acceso de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

ANEXO G.

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE CONTROL DE ACCESO DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00004</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 2</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
ACCESO A SISTEMAS:
Será exclusivo del trabajador a cargo, no se podrá permitir el acceso a segundas personas sin previa autorización del Director, con el fin de resguardar la integridad, confidencialidad de la información del sistema.
ACCESO A EQUIPO:
Será exclusivo del trabajador en caso de necesitar acceder a la estación de trabajo deberá ser autorizado por el Director e ingresar con su usuario y contraseña con el fin de resguardar la integridad, confidencialidad de la información.
ACCESO A INSTALACIONES
El acceso de los trabajadores internos deberá ser registrado.
El acceso de personas que no laboren dentro del DTIC deberá ser registrado y no podrán ingresar a las oficinas donde se encuentre información o equipos del DTIC.
ACCESO A INFORMACIÓN DEL DEPARTAMENTO:
La información estará en potestad del Director del DTIC con el fin de asegurar la confidencialidad, disponibilidad e integridad del mismo.</td></tr>
</table>

Documento Política de intercambio de información de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td>  </td><td colspan="3">POLÍTICA DE INTERCAMBIO DE INFORMACIÓN DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00005</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se asegurará toda software que intercambien información ya sea esta interna o externa a la institución con el fin de garantizar la integridad, confiabilidad y confidencialidad</td></tr>
</table>

ANEXO H.

Documento Política de pantalla y escritorio limpio de la Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO DE LA DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00006</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se deberá mantener el escritorio limpio de cualquier código fuente, anotaciones del sistema, claves, cualquier información que pueda ser utilizado para una amenaza o ataque de terceras personas, con fin de garantizar la integridad y confidencialidad de la información, además de salvaguardar la integridad del personal.
Se deberá tener organizada la información en el equipo de trabajo sin colocar nombre a los archivos que indique su procedencia como claves, acceso, información privada entre otros, los mismo deberán estar en carpetas con claves de seguridad.</td></tr>
</table>

ANEXO I.

Documento Política controles criptográficos dela Dirección de Tecnología y Comunicación de la ESPOCH. (Guevara, 2012)

En base a los formatos planteados anteriormente la propuesta de la política de seguridad del DTIC será la siguiente:

<table>
<tr><td> 
</td><td colspan="3">POLÍTICA DE CONTROLES CRIPTOGRÁFICOS DE LA DIRECCIÓNDE TECNOLOGÍA Y COMUNICACIÓN</td></tr>
<tr><td>SERIAL: P00007</td><td>FECHA DE EMISIÓN:24/10/2016</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN: SI</td></tr>
<tr><td>ELABORADO POR: Maestrante</td><td colspan="2">REVISADO Y APROBADO POR: Ing. Gustavo Hidalgo</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DTIC
ALCANCE: Dirigido a todos los trabajadores al ingresar a trabajar en el DTIC, además de socializar periódicamente como recordatorio.
VIGENCIA: A considerar por el Director actual a partir de la fecha de emisión
POLÍTICA:
Se asegurará toda software que intercambien información ya sea esta interna o externa a la institución con el fin de garantizar la integridad, confiabilidad y confidencialidad a través de recurso criptográficos.</td></tr>
</table>